Cuadernos de Globalización con Equidad N° 13

EL FUTURO DIGITAL DEL PERÚ:
COMPROMISOS DE ILUSIÓN Y DESENCANTO

Sofia Scasserra

red GE GLOBALIZACIÓN CON EQUIDAD 15 años
CooperAcción

EL FUTURO DIGITAL DEL PERÚ: COMPROMISOS DE ILUSIÓN Y DESENCANTO

Sofia Scasserra

Red Peruana por una Globalización con Equidad - RedGE

CooperAcción

EL FUTURO DIGITAL DEL PERÚ: COMPROMISOS DE ILUSIÓN Y DESENCANTO

Sofia Scasserra

© Red Peruana por una Globalización con Equidad - RedGE
Jirón Trujillo 678, Magdalena del Mar. Lima - Perú
Teléfono (511) 394 7212.
redge@redge.org.pe / www.redge.org.pe

© CooperAcción
Jirón Trujillo 678, Magdalena del Mar. Lima - Perú
Teléfono (511) 394 7212.
https://cooperaccion.org.pe/

Diseño, diagramación:
Rafael Nova.
Recavarren 1257, Surquillo
Teléfono (51) 990 718 636.

Primera edición digital, abril 2024

Hecho el Depósito Legal en la Biblioteca Nacional del Perú
N° ISBN N° 2024-03740

CONTENIDO

INTRODUCCIÓN

Breve historia de los acuerdos de economía digital

La digitalidad nos envuelve. Si podemos establecer una diferencia entre el milenio anterior y este, es que a partir de la llegada de los 2000, la creciente importancia de la vida ***on line*** fue empujando a las sociedades a tener más bienes y servicios disponibles a través de internet. La pandemia lo exacerbó y hoy parece imposible imaginar una vida sin un teléfono celular en la mano: hoy no solo accedemos al mercado a través de internet, sino que accedemos a derechos, servicios públicos, información, democracia y cultura, entre tantas otras cuestiones.

La digitalidad dejó de ser un lugar de compra venta de productos, y pasó a ser aquel sitio donde nos informamos, estudiamos, trabajamos, accedemos a servicios de salud, accedemos a cultura, por mencionar algunos de sus usos. En este sentido, queda claro que dejó de ser un lugar comercial (si es que alguna vez lo fue) para comenzar a disputar un espacio de derechos humanos y ciudadanos en la web.

Los mercados crecieron, y más aspectos de nuestra vida se mercantilizaron. Los datos recabados de nuestras acciones hicieron que se vuelva valioso (y por ende vendible) qué páginas visitamos, dónde estuvimos, con quiénes hablamos, de qué conversamos, cuáles son nuestros intereses, qué orientación política o religión profesamos, entre muchas otras cuestiones. Todo esto es cuantificado a través de datos que se recolectan por medio de las plataformas que utilizamos a diario. Es la mercantilización de la vida misma lo que está ocurriendo.

Esos datos pueden ser utilizados con fines mercantiles, pero también pueden ser utilizados para el bien común. Se pueden diseñar políticas públicas, establecer derechos económicos, medioambientales, y colectivos para alcanzar mejores derechos laborales con dichos datos. Pero estos objetivos no están en agenda. Así como en su momento las corporaciones se apropiaron del conocimiento, otro bien común, a través de normas de propiedad intelectual, hoy se busca cooptar

los datos a manos de las corporaciones con el mismo fin: obtener poder de mercado, limitar la capacidad regulatoria de los Estados y limitar el accionar de los pueblos en pos del bien común.

A mayor mercantilización de la vida, existe más interés por coartar la capacidad de regulación estatal en pos de establecer nuevos derechos de segunda y tercera generación, saliendo del debate únicamente en torno a la privacidad. Así se debate una arquitectura internacional de normas que buscan ver el manejo de datos y plataformas como meros temas comerciales que nada tienen que ver con los derechos humanos, sino con un tema de propiedad, responsabilidad y privacidad. Básicamente estos son los Acuerdos de Libre Comercio y las normas de comercio internacional suscritas en la Organización Mundial de Comercio: normas que liberalizan y permiten la mercantilización bajo un modelo neoliberal de los diversos bienes y servicios de nuestras economías.

Las negociaciones sobre comercio electrónico en el marco de la Organización Mundial del Comercio (OMC) surgieron a partir del año 1998. Ya el nombre "comercio electrónico" buscaba hacer ver a la negociación como un mero tema comercial. Parecía más que se estaban debatiendo normas estandarizadas sobre cómo comprar y vender en internet, más que una verdadera arquitectura de la economía digital.

En general, las negociaciones sobre comercio electrónico tienen como objetivo establecer un marco regulatorio que permita el libre flujo de datos y de bienes y servicios a través de las fronteras, al mismo tiempo que se protege la privacidad de los consumidores y consumidoras y se busca establecer estándares de seguridad de las transacciones en línea. Esos son los principios generales con los que se manejan las negociaciones, pero como veremos más adelante, esconden bajo un aparente marco de buenas intenciones, una arquitectura global para la privatización de bienes comunes y la creación del Estado "ineficiente" que no sabe diseñar sus propias políticas públicas, vis a vis, corporaciones "inteligentes" que tienen información perfecta y saben lo que es mejor para la sociedad.

El impulso inicial para las negociaciones sobre comercio electrónico en la OMC provino de Estados Unidos, que en la segunda mitad de la década de 1990 comenzó a presionar a otros países para que se discutiera este tema en el marco de la organización.

En la primera reunión del Grupo de Trabajo sobre Comercio Electrónico en 1998, los países miembros adoptaron una declaración conjunta en la que se reconocía la importancia del comercio electrónico y se acordaba iniciar discusiones sobre las implicaciones del comercio electrónico para el comercio internacional.
En los años siguientes, las discusiones se centraron en cuestiones como la facilitación de las transacciones en línea, la protección de la privacidad y la seguridad de los datos, la propiedad intelectual y la interoperabilidad de los sistemas informáticos.

Sin embargo, durante varios años las negociaciones avanzaron lentamente debido a las diferencias entre los países miembros sobre la necesidad de establecer reglas específicas para regular el comercio electrónico. Algunos países argumentaban que era necesario establecer reglas claras para proteger a los consumidores y garantizar un comercio justo, mientras que otros argumentaban que el comercio electrónico debía permanecer libre de regulación.

El primer acuerdo bilateral que incluyó disposiciones específicas sobre comercio electrónico fue el Acuerdo de Libre Comercio de Singapur-Estados Unidos (USSFTA, por sus siglas en inglés), negociado en 2003. Este acuerdo incluyó disposiciones sobre la facilitación del comercio electrónico, la protección de la propiedad intelectual en línea y la eliminación de barreras para el comercio electrónico transfronterizo. Desde entonces, se han negociado varios acuerdos bilaterales y regionales que incluyen disposiciones sobre comercio electrónico.
En 2015, un grupo de países liderados por Estados Unidos lanzó una iniciativa llamada “Comercio Electrónico para Todos” en la que se pedía la eliminación de las barreras al comercio electrónico en el marco de la OMC. Esta iniciativa impulsó las negociaciones sobre comercio electrónico en la OMC, y en los años siguientes se llevaron a cabo varias rondas de negociaciones.

En 2019, un grupo de países liderados por Australia y Japón presentó un proyecto de texto para un acuerdo sobre comercio electrónico en la OMC. El proyecto de texto incluía disposiciones sobre la protección de datos personales, la no discriminación en el comercio electrónico y la facilitación del comercio electrónico transfronterizo. Si bien este proyecto aún no se ha adoptado oficialmente, ha servido como base para las negociaciones en curso sobre comercio electrónico en la OMC.

Hoy día, se ha hecho tan evidente de que la negociación no es únicamente para liberalizar el comercio digital, que se ha modificado el nombre y se habla de negociaciones en torno a la economía digital, en un acto de sincericidio que muestra la verdadera intención: la de construir una arquitectura global liberal en torno a internet.

En resumen, las negociaciones sobre comercio electrónico en la OMC han evolucionado lentamente a lo largo de los años, y han pasado de ser declaraciones de interés a discusiones más concretas sobre la necesidad de establecer reglas para desregular la economía digital.

¿Qué está en juego?

El sistema capitalista se profundiza, se hace más eficiente y expande sus fronteras: encuentra nuevas formas de mercantilización de la vida, nuevas materias primas de explotación y nuevas formas de acumulación. Esto se sabe y se viene estudiando hace décadas. Así, podemos decir que estamos en una nueva fase del sistema capitalista que en muchos sentidos no es muy distinta de las anteriores. Pero en otros sentidos sí lo es.

La tercera revolución industrial trajo consigo un gran cambio en la matriz productiva, al igual que las anteriores: las finanzas y las telecomunicaciones internacionalizaron el mercado y dejaron empresas globalizadas que se movían libremente a través de las fronteras, buscando aprovechamiento de las ventajas comparativas y de la mano de obra barata. En efecto, mientras el capital podía moverse libremente las y los trabajadores migrantes encontraban cada vez más dificultades para ir allí donde la mano de obra es mejor paga. Esto se debió a leyes migratorias locales, así como a normativas de la Organización Mundial de Comercio en materia de exportación de servicios bajo el modo 4, que permite la libre movilidad de profesionales, pero no de trabajos menos calificados. La empresa trasnacional se deslocalizó, terciarizó y se refugió en paraísos fiscales para no pagar impuestos, al calor de unas telecomunicaciones cada vez más eficientes y globales.

¿Qué cambió entonces? ¿no es internet otra forma de telecomunicación? Indudablemente lo es, pero es una forma de telecomunicación que hizo aparecer una nueva materia prima en la economía: los datos.

Si pensamos en la industria 4.0, aparecen imágenes de robots, plataformas, líneas de código de programación y nuevos dispositivos sorprendentes manejados por inteligencia artificial. Pero, ¿es verdaderamente eso la industria 4.0? Hoy día se recolectan datos. Esos datos se procesan a través de algoritmos, que extraen información. Esa información se vende, se comercializa para optimizar procesos y orientar las decisiones a lograr los objetivos comerciales deseados. Esta "inteligencia" de cualquier proceso que se pueda datificar, sea una línea de montaje o un sistema de logística, también se realiza con nuestras acciones. En efecto, la industria digital emula a la industria tradicional en el sentido que sigue

la misma lógica: ingresa una materia prima, heterogénea y disímil, a una fábrica; se procesa, se estandariza, se realiza un control de calidad y se vende de forma masiva en el mercado. Así mismo sucede hoy día con nuestro comportamiento y procesos productivos: ingresan datos, se procesan en una fábrica algorítmica capaz de comprender nuestro comportamiento o formas de producción y sacar conclusiones, se verifica si esa información es real ofreciéndonos incentivos para modificar nuestro comportamiento, y finalmente se vende nuestro perfil a empresas, o el diseño de un sistema logístico más eficiente a medida que tengo capacidad de predecir la producción y el consumo. Para verlo más claro, supongamos con un ejemplo, que una persona ama tomar café en un bar todas las mañanas, las plataformas lo saben a través de nuestra geolocalización, y del procesamiento algorítmico de los datos. Con lo cual nos envían promociones para tomar café en determinado lugar para ver si efectivamente pueden motivar nuestro comportamiento. Luego esa información es vendida en base de datos (¡todas estas personas aman tomar café y si les envías un cupón, irán a tu café a tomarlo!), vendiendo un producto masivo (nuestro comportamiento comprendido en una base de datos) al mercado. Esta industria digital se realizó primero a las y los consumidores, ofreciendo redes sociales, promociones, ***likes*** y descuentos; luego se realizó a los ciudadanos y ciudadanas, buscando motivar el voto en las elecciones de aquellos que tenían un perfil determinado (de ahí devino el escándalo de Cambridge Analytica); y finalmente se realiza a las y los trabajadores a través de la algoritmización de las relaciones del trabajo.

Si miramos la industria digital, existen varias partes de la cadena de producción. Por un lado está la materia prima, los datos. Las herramientas con las que se colectan los datos (medio de producción de la materia prima) son las plataformas digitales. Los algoritmos son la fábrica que procesa la información. Finalmente está el control de calidad y venta, enmarcado en debates en torno a la protección al consumidor y la privacidad. Todos estos elementos, como veremos más adelante, están particularmente incluídos en los acuerdos de comercio electrónico, o economía digital como se les denomina actualmente.

Lo que se está desregulando entonces, es, por un lado, la posibilidad de moldear la industria y de hacer al Estado partícipe de la misma bajo el espíritu de "El estado emprendedor" (Mazzucato, 2014), que muestra que las iniciativas público privadas devienen en mejores inventos, con más escala, y con mayor consideración de los aspectos culturales, permitiendo la participación de diversos actores y, por ende, aumentando el shock de externalidades positivas. Por otro lado, buscan apropiarse de una materia prima que tiene un carácter

no rival y, por ende, común. Los bienes no rivales son aquellos en la economía que, al consumirlos, no se agotan. Como un viaje en transporte público: que un pasajero suba a un tren no significa que otro no pueda hacerlo y le sea igual de útil. Los servicios públicos tienen características de bienes no rivales, como el conocimiento. Los datos cumplen con esta condición, haciendo que su privatización sea en beneficio de unos pocos y en detrimento de muchos. Es decir, existe una nueva materia prima en la economía de la que muchos podrían beneficiarse, pero se está buscando la forma de limitar el acceso a la misma de forma tal de que sean las grandes corporaciones tecnológicas quienes tengan el monopolio de la producción y acceso a la misma.

A su vez, se ha creado una falsa sensación de que internet es un lugar sin límites, que se debe jugar bajo las reglas de las corporaciones, porque son ellas las que tienen el poder en los espacios virtuales. Esto no fue siempre así y de hecho internet, una invención pública, posee fronteras difíciles de ser sorteadas: se pueden limitar contenidos y plataformas, se pueden cobrar impuestos, se pueden poner barreras arancelarias y no arancelarias, pero de hecho sólo las naciones más poderosas como China o EE.UU. lo hacen. La mayoría de los países del mundo no imponen restricciones de contenido, siguiendo el principio de neutralidad en la red, ni cobran impuestos aduaneros por los datos que son extraídos: si algo sabemos en América Latina es que la historia nos ha sacado materia primas de nuestro suelos sin dejar nada a cambio, ni siquiera impuestos para fortalecer al Estado. Hoy día ese mismo extractivismo despiadado se lleva adelante sobre nuestras poblaciones, generando una materia prima gratuita que cotiza en el agregado regional: la ***big data*** latinoamericana. Y así como el poeta alguna vez dijo "tu no puede comprar el viento, tu no puedes comprar el sol, tu no puedes comprar la lluvia, tu no puedes comprar el calor" se debería iniciar un nuevo camino marcado por un "tu no puedes comprar mis gustos, tu no puedes comprar mi ideología, tu no puedes comprar mis amistades, tu no puedes comprar mi geolocalización".

En definitiva, lo que está en juego es una nueva oleada de extractivismo, esta vez digital, que imponga un nuevo sistema colonial, donde los grandes países del norte global se apropien de la "inteligencia" de nuestras sociedades, manejando la industria digital y su producción, y tirando la escalera al desarrollo de las naciones periféricas, imponiendo su cultura, sus formas de producción y sus formas de vida, historia que ya hemos vivido en la región.

Acuerdos firmados por el Perú - Racconto histórico

La historia comercial del Perú muestra un país abierto a negociaciones, con gran entusiasmo por integrar las nuevas agendas que están de moda; sin estudios de impacto profundos que puedan mostrar las implicancias de los acuerdos en la economía peruana. Desde la integración a la Organización Mundial del Comercio (y anteriormente el GATT), fue sumando una serie de acuerdos bilaterales y regionales que fueron introduciendo cláusulas en materia digital, lento pero sin pausa.

Perú firmó el primer tratado de libre comercio con capítulo en materia digital en el año 2006. Este acuerdo que mantiene a la fecha con Estados Unidos, fue el primer acuerdo comercial en Perú de todos los acuerdos que ha firmado, que comienza a sentar las bases de lo que luego fue su historia en materia digital. Dicho acuerdo contenía solo un puñado de cláusulas donde los principios más importantes eran no imponer aranceles de ningún tipo a las transmisiones electrónicas, y la no discriminación de productos digitales. Es decir, Perú en ese acuerdo estaba comprometiéndose con los Estados Unidos a no tener una política preferencial de un producto físico por sobre uno digital (sea un libro, un servicio turístico o un producto bancario) y que sobre la importación/exportación del mismo no cobraría aranceles. El mundo era muy distinto en aquel entonces y si bien lo digital comenzaba a cobrar importancia, jamás se dimensionó en aquel entonces la cantidad exuberante de productos y servicios digitales que consumimos hoy día. En aquel entonces los teléfonos inteligentes apenas comenzaban a salir al mercado y Perú apenas contaba con una red de 2G, siendo la red 3G incipiente y aún no establecida formalmente en el país. Es decir, los productos y servicios digitales eran más un tema del futuro que del presente. No obstante, el acuerdo muestra que EE.UU. ya tenía una clara estrategia de expansión en esa materia dejándose la puerta abierta para ingresar al mercado peruano.

El segundo hito histórico en materia comercial digital se puede trazar con el acuerdo de la Alianza del Pacífico en el año 2010, donde se muestra que los países latinoamericanos integrantes ya poseen una agenda digital en expansión que quieren asentar en la región. Se suman temas a la agenda como la protección al consumidor, la protección de datos personales, y la firma electrónica, entre otros. Asuntos más operativos pero que ya comenzaban a mostrar controversias

en la economía digital y se hacían presentes en negociaciones comerciales a fin de dar una respuesta, buena o mala como veremos más adelante, a temas trascendentales para reforzar los mercados ***online.*** En ese mismo año, el acuerdo comercial con la Unión Europea (UE) introduce el primer artículo de los que denominaremos "contrarios a la industrialización y soberanía digital" de los pueblos: los requerimientos de localización de los datos. Este artículo impide a un país establecer normas respecto a dónde se deben alojar los datos de sus ciudadanos y ciudadanas, perdiendo soberanía y jurisdicción sobre los mismos. A partir del año 2017 con la firma del Tratado Transpacífico (TPP) y el posterior Tratado Integral y Progresista de Asociación Transpacífico (CPTPP), la agenda comercial en materia digital ingresa a Perú con toda su fuerza: se introducen todos los artículos que están actualmente en negociación en acuerdos plurilaterales, conformando una arquitectura digital contraria a los debates vigentes en el Global Digital Compact[1] y en las legislaciones locales en diversos países. En efecto, el mundo se debate cómo regular el futuro asegurándose una agenda digital que no solo incluya a todos, sino que moldee las sociedades de acuerdo a sus derechos y principios, mientras que la agenda comercial en materia digital parece ir en la dirección contraria, conformando una arquitectura liberal que no tiene en cuenta ni estándares éticos, u otros aspectos que no sean meramente económicos, como el medioambiente, la igualdad de género, la inclusión y los derechos laborales, entre otros.

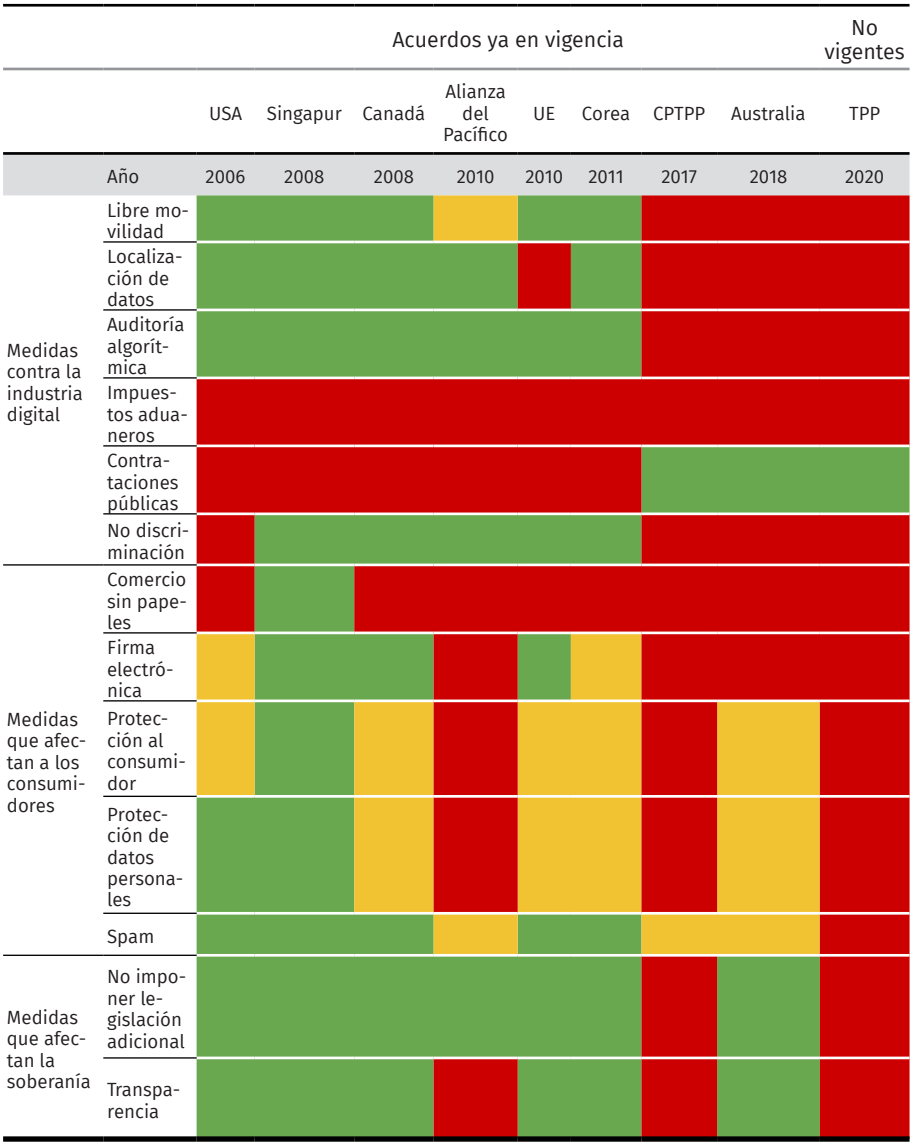
En ese mismo año, se inician las negociaciones en materia digital en la Organización Mundial de Comercio formalmente en la Reunión Ministerial de Buenos Aires, grupo plurilateral del que Perú forma parte.

Así, podríamos resumir la agenda digital comercial de Perú en el cuadro subsiguiente. Los cuadros rojos significan que poseen la cláusula en una versión que afecta a los ciudadanos y ciudadanas del Perú de forma directa, los cuadros amarillos ponen énfasis en la aparición de la temática pero no se ha profundizado en la misma o poseen una versión más laxa de la misma. Finalmente, los cuadros verdes muestran aquellas cláusulas que no aparecen en el acuerdo ni son temas de discusión en los mismos.

1 El Global Digital Compact es una iniciativa de Naciones Unidas que busca algunos principios de gobernanza en internet. Si bien los ejes a tratar y las conclusiones van en una direccion mas saludable que la de los acuerdos de libre comercio, la inicitia posee el vicio de ser "multistakeholder", sentando en la mesa de negociación a las big tech y a la sociedad civil por igual, lo que inclina la balanza en favor de las empresas que son mas poderosas y cuentan con muchos mas recursos.

Cuadro

Principales cláusulas de comercio electrónico de los acuerdos firmados por Perú[2]



2 Las cláusulas contenidas en este cuadro y a lo largo de todo el presente trabajo fueron extraídas de las versiones en español de los acuerdos comerciales firmados por Perú disponibles en la página http://www.acuerdoscomerciales.gob.pe/. Se incluyeron únicamente las cláusulas denominadas de "comercio electrónico" pero no así otras cláusulas en materia digital en apartados como finanzas y telecomunicaciones.

En el cuadro puede apreciarse la evolución de los temas en la agenda. Mientras que en los primeros años se iban introduciendo temas de forma tímida y paulatina, es a partir del año 2017 que se comienzan a comprometer fuertemente diversas agendas que, como veremos más adelante, limitan fuertemente la capacidad regulatoria de Perú y buscan una apertura comercial y un liberalismo que favorezca a las grandes empresas transnacionales tecnológicas.

Claro que uno puede pensar que esto es necesario para la modernización y la inserción digital de Perú, pero esto no es cierto: la digitalidad ha crecido en el mundo y un sinfín de empresas se encuentran en la región sin necesidad de firmar estos acuerdos. De hecho, no es hasta el año 2017 que la agenda se hace presente de forma completa y nadie puede argumentar que previo a ese año no había economía digital en el país. En efecto, no resulta necesario desregular una economía que ya se encuentra desregulada a nivel internacional. La verdadera intención de los acuerdos de libre comercio en materia digital es mantener esa desregulación por siempre, buscando una economía digital que no se plantee una agenda de derechos ni democracia, sino una economía digital con un objetivo económico único: el extractivismo y el colonialismo digital.

¿Qué implican las cláusulas comprometidas?

Las cláusulas que se encuentran en los acuerdos pueden parecer complejas y difíciles de comprender. Es más, se suelen utilizar eufemismos para que hasta parecen razonables y valiosas muchas de ellas... "libre movilidad de datos" (¿puede existir alguien que no quiera que la economía digital fluya?), "transparencia" (como si la opacidad fuera una opción), "protección de datos y al consumidor" (¿es posible que un Estado no quiera proteger estos valores?), entre otras. Lo cierto es que, al mirar la letra chica de los acuerdos, lejos se está de lograr objetivos de política pública que respeten los intereses de los ciudadanos y ciudadanas, sino más bien de las grandes corporaciones tecnológicas. Por ese motivo, iremos explicando una a una las normas o principios generales que envuelven estas cláusulas para que se comprendan los trasfondos de los debates en materia digital.

Cláusulas contra la industria digital local y la regulación

Las siguientes cláusulas podrían considerarse las más peligrosas de los acuerdos en materia digital. En las negociaciones del Perú sólo aparecen a partir del año 2017, pero son las más solicitadas en los acuerdos modernos. Si Perú renegocia con diversos bloques donde ya tiene acuerdos cerrados, es probable que estas cláusulas aparezcan en la negociación, ya que son el corazón de la arquitectura digital y lo que más buscan las empresas hoy día.

Las cláusulas agrupadas aquí conforman un entramado que busca liberar la industria digital de cualquier tipo de regulación. Para comprenderlas, necesitamos saber primero, ¿qué es la industria digital? Si bien esto ya fue mencionado más arriba, nos detendremos aquí en dar una explicación más profunda.

Cuando pensamos en una industria, cualquiera sea, tenemos una materia prima heterogénea y desigual. Esa materia prima ingresa a una fábrica donde se procesa, se transforma en un producto homogéneo y fácilmente vendible en el mercado. Ese producto pasa por diversos controles de calidad para garantizar su homogeneidad y estandarización, para luego salir a la venta de forma masiva. Este proceso podemos verlo en casi cualquier proceso industrial que pensemos, desde la transformación de granos de maíz en aceite, hasta una camiseta

deportiva. Entonces, ¿cómo se construye la industria digital? Pues la materia prima son nuestros datos, disímiles, heterogéneos, privados, individuales. Esos datos se acumulan en un agregado o ***big data*** e "ingresan" en una fábrica procesadora: los algoritmos. Los algoritmos son el sistema por el cual esos datos devienen en información. Se transforman en información estandarizada ("todos estos consumidores toman café en este barrio a esta misma hora", "todos estos ciudadanos piensan igual respecto a una determinada injusticia en la sociedad", "este producto se vende mejor los días de lluvia", etc.) vendible en circuitos industriales dependientes de la era digital. Esta información se verifica, pasa controles de calidad, chequeando si efectivamente es así y motivando ese comportamiento. No es raro que, si mencionamos en un chat de amigos que estamos felices de podernos ir de vacaciones, nos comiencen a llegar promociones y descuentos de escapadas a diversos destinos. Así se verifica y se vende el perfil de forma homogénea y masiva. ¿A quiénes? a empresas interesadas, candidatos políticos, o cualquiera interesado en esa información. Así se genera la verdadera industria digital apropiada por las grandes tecnológicas agrupadas en la sigla GAFAM: Google (ahora Alphabet), Amazon, Facebook (ahora Meta), Apple y Microsoft. Podríamos también sumar a las grandes tecnológicas chinas como Alibaba o Tencent y a nuevos jugadores como Tesla. Sean quienenes sean, son los dueños de la industria digital que se juega con sus reglas y que ponen grandes sumas de dinero en hacer ***lobby*** en pos de que las cláusulas que se describirán a continuación se esparzan cada vez más, configurando una arquitectura desregulada y desprovista de otras intenciones que no sean las económicas.

Esta industria digital también funciona para procesos industriales, donde se extraen datos de las fábricas, se procesa, deviene en información y la misma es utilizada posteriormente para mejorar procesos, predecir la producción y el consumo y mejorar procesos logísticos, entre otros.
Tenemos entonces dos componentes económicos fundamentales: la materia prima, los datos; y la fábrica donde se procesan, los algoritmos. De esos dos componentes, podemos sumar dos medidas de política económica tradicionales que se utilizan en todo el mundo para proteger las industrias nacionales frente a la competencia feroz, defender a los consumidores de abusos y motivar industrias nacientes y, por ende, la industrialización: los aranceles y las compras públicas.

Libre movilidad de datos

La cláusula en cuestión promueve un esquema extractivista de materias primas que ha sido experimentado en tiempos pasados en América Latina. Empresas con capital extranjero llegan al territorio, recolectan datos y los trasladan sin restricción alguna. Este fenómeno podría denominarse extractivismo digital y se refiere al proceso mediante el cual los datos, que representan la materia prima de la inteligencia artificial y otras tecnologías de la nueva revolución industrial, traspasan las fronteras nacionales, lo que conduce a la pérdida de acceso estatal y comunitario a los mismos. Cualquier empresa que inicie operaciones en el territorio en cuestión podría recolectar datos de los consumidores, ciudadanos locales o empresas industriales o de comercio y servicios (o servicios públicos) y llevarlos a otro territorio sin limitaciones. Este hecho es fundamental para comprender que una vez que los datos cruzan la frontera, no se puede exigir acceso o repatriación debido a que el país pierde su jurisdicción sobre ellos. Se trata de un fenómeno equiparable a cualquier bien físico conocido, tal como una obra de arte o un mineral precioso. En otras palabras, una vez que dicho bien cruza la frontera, el país de origen enfrentará grandes dificultades para recuperarlo, si es que alguna vez es posible hacerlo.

Una de las inquietudes fundamentales en relación a la aprobación del flujo transfronterizo o transferencia de datos es la afectación de la privacidad de los ciudadanos y ciudadanas, especialmente en lo que se refiere a datos sensibles como los de salud. En este sentido, países como Australia han implementado leyes rigurosas de privacidad debido a la venta y compra de bancos de datos en la industria de la salud. En el caso del gobierno australiano, su ley de privacidad es más difícil de hacer cumplir si el proveedor de almacenamiento de datos tiene su sede en el extranjero. Por este motivo, el sistema de registros de salud electrónicos de Australia requiere que los datos permanezcan y se procesen en el país (Federal Register of Legislation - Australian Government, 2012). En contraste, la Unión Europea cuenta con el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), que protege la privacidad de los datos de sus ciudadanos (European Parliament, 2016). Sin embargo, se plantea la interrogante de qué sucedería si los datos fueran trasladados a países donde no existen leyes que regulen estas cuestiones. La ley contempla este hecho y otorga jurisdicción extraterritorial para proteger a los ciudadanos europeos. La UE está trabajando en sistemas para garantizar que la ley de protección de datos europea sea aplicable en todo el mundo (European Commission, 2020). A su vez, la GDPR establece que las organizaciones deben informar a los

individuos sobre cualquier transferencia de sus datos personales fuera de la UE y deben obtener su consentimiento explícito para dicha transferencia en ciertas circunstancias. A nivel global, es necesario implementar sistemas de auditoría y control más efectivos para verificar el cumplimiento de la privacidad de los ciudadanos en todo el mundo. No obstante, es difícil exigir lo mismo a países en vías de desarrollo, ya que carecen de los mismos recursos para desarrollar tales sistemas, y la debilidad institucional implica que a menudo no cuentan con leyes sólidas que protejan los datos personales de sus ciudadanos.

Desde una perspectiva de desarrollo económico, la extracción de datos representa una materia prima fundamental para la inteligencia artificial, que una vez transferida fuera del territorio, no retorna. La información contenida en los datos es también relevante para la formulación de políticas públicas efectivas. Si se piensa cuánto valen los datos de una ciudad en términos de movilidad y geolocalización para diagramar nuevas autopistas o sistemas de transporte público, o los datos de los paquetes educativos de Google o Microsoft para pensar políticas educativas, se ve claramente que dejar algún grado de libertar regulatoria en términos de acceso y transferencia de datos, podría resultar muy beneficiosos para un país.

Localización de datos y procesamiento

Esta cláusula está íntimamente relacionada con la anterior, ya que la localización dentro de los bordes de un país, implica limitar la transferencia.

La cadena de valor de los datos como materia prima consta de varias etapas, incluyendo la exportación transfronteriza, el procesamiento y el alojamiento de los datos. Sin embargo, la cláusula que permite la exportación ilimitada de datos se considera una forma de colonialismo digital y dependencia económica. Para evitar esta situación, algunos países han incorporado cláusulas contractuales en sus sistemas de compras públicas que exigen la retención de los datos en el país, a fin de que el Estado tenga acceso a ellos y pueda diseñar políticas públicas y sistemas digitales propios. A pesar de su eficacia en el corto plazo, las cláusulas de localización de datos son resistidas por los grupos de ***lobby*** hegemónicos, que argumentan que los requisitos de localización permiten abusos en el acceso de los Estados a los datos. Por este motivo es que muchas empresas han comenzado a alojar sus datos en paraísos fiscales (Scasserra & Foronda, 2022). A su vez, se argumenta que, si bien protegen a la industria nacional en el corto plazo, al no generar competencia con el exterior, termina yendo en detrimento de

la economía (World Economic Forum, 2020). En conclusión, las mismas empresas aceptan que la localización de datos en el territorio puede proteger la industria nacional, limitando la competencia externa.

Podríamos enumerar varios beneficios por los cuales puede ser estratégico exigir el almacenamiento y procesamiento local:

- El hecho de tener servidores de datos cercanos permite diversas ventajas, como tener sistemas de información más veloces y efectivos. En ausencia de localización cercana, el proceso de búsqueda de datos implica una triangulación que resulta en una demora, aunque imperceptible para la mayoría de los usuarios. Con la llegada del 5G, esta demora se vuelve un factor crítico en aplicaciones como el manejo de autos inteligentes o la realización de cirugías remotas, donde la vida humana puede depender de la rapidez de la información (5G Américas, 2020). Es decir, exigir almacenamiento local puede resultar en mayor seguridad para la población a futuro.

- La localización de datos en el territorio nacional permite que los mismos queden bajo la jurisdicción del país que los produce, lo que eventualmente puede facilitar el acceso a los mismos por razones de seguridad o salud nacional, entre otras. Este enfoque también otorga soberanía sobre los datos, permitiendo que el insumo estratégico quede dentro de los confines del país y de aquellos que los produjeron. En la actualidad, si un gobierno necesita acceder a datos de empresas transnacionales radicadas en los EE.UU. como Google, por ejemplo, debe pedir permiso al Departamento de Estado de los EE.UU. para que a su vez este organismo los solicite a Google y finalmente sean compartidos (Whittaker, 2013).

- Otra ventaja de la localización de datos es la generación de subsistemas económicos de alta tecnología. Un centro de almacenamiento y procesamiento de datos requiere personal altamente capacitado en el ensamblaje y mantenimiento del mismo, producción de hardware y software para operarlo, redes de fibra óptica que lleguen hasta el centro y, en muchos casos, hasta energías renovables para alimentarlos. Muchas empresas han comenzado a invertir en sistemas energéticos autónomos para sus centros de datos debido al riesgo que implica la pérdida de energía como resultado de una falla en el sistema energético nacional, el ahorro de costos que puede traer, además de minimizar el impacto ambiental (Colocation America, 2020).

- A menudo, se lleva a cabo el procesamiento de datos en el mismo lugar donde se almacenan los datos para evitar la triangulación doble, lo que disminuiría la

velocidad en la entrega del producto final. Esto requieren de personal altamente calificado, como ingenieros, programadores y matemáticos (Kumar, 2020).

- Uno de los principales motivos para mantener la localización del almacenamiento y procesamiento de datos es la seguridad, especialmente en cuestiones que podrían afectar la seguridad nacional de un país. Los Estados Unidos, por ejemplo, requieren que todos los proveedores de servicios de computación en la nube que almacenen datos del Departamento de Defensa estén dentro de sus fronteras por motivos de seguridad (Information Technology Industry Council, 2017). Además, mantener la localización permite hacer cumplir la legislación del país y evitar que las disputas legales se resuelvan en cortes internacionales o extranjeras. En Nueva Zelanda, los registros de impuestos deben almacenarse en servidores ubicados en el país, y la falta de cumplimiento es considerado un delito punible con una multa (Inland Revenue, s.f.).

- Este tipo de medidas van contra los denominados "paraísos de datos": centros de almacenaje que a menudo coinciden en locaciones geográficas con los paraísos fiscales, a fin de resguardar la materia prima de la industria digital en lugares con normativas que defienden los intereses de las corporaciones (Scasserra & Foronda, 2022).

- En el ámbito global, se ha observado un creciente aumento en los ingresos generados por el procesamiento y almacenamiento de datos (Taylor, 2022). Se ha comprobado que los ingresos por almacenamiento de datos en un país específico han ido en aumento y que la mayoría de las ganancias se concentran en ciertas regiones geográficas. Según el informe de la Comisión Económica para América Latina y el Caribe (CEPAL) de 2016, el 59,6% de los ingresos por este servicio son obtenidos por Estados Unidos, el 20% por Europa occidental, el 10% por Asia-Pacífico y el resto se distribuye entre África, América Latina y Europa oriental.

Así, se pueden ver los beneficios económicos que trae esta actividad y, por ende, la disputa que genera en torno a dónde se localiza en la cadena global de valor. Es evidente que el negocio del almacenamiento de datos en la nube pública se concentra en ciertas regiones que poseen una fuerte estrategia de extractivismo digital. Además, este aumento en los ingresos no se limita al ámbito estatal, sino que también se extiende a las empresas que ofrecen estos servicios. Por ejemplo, en la actualidad, la empresa Visa ha reportado que el 38% de sus ganancias se derivan del procesamiento de datos (Reiff, 2021).

Auditoría algorítmica

Esta cláusula provoca desigualdad, pobreza, exclusión y competencia desleal.
Para comprender de manera amplia esta cláusula en los acuerdos de libre comercio hay varios conceptos que necesitan ser explicados previamente. Por un lado, ¿qué es un algoritmo? En la economía digital todo se maneja con ellos y es lo que realmente procesa la enorme cantidad de datos que generamos a diario. Los algoritmos son instrucciones que procesan información y devuelven un resultado, sea una maximización u optimización (predicción estadística), un ordenamiento, una decisión o un menú de opciones. Cuando hacemos una búsqueda en Internet, un algoritmo decide qué resultados veremos primero; cuando ingresamos a Netflix, un algoritmo decide qué películas mostrarnos; un algoritmo procesa imágenes médicas e indica cuál es la probabilidad de que determinada mancha sea un tumor; un algoritmo asigna pedidos a repartidores que trabajan en plataformas cuando van por las calles entregando pedidos.

El concepto de sesgo algorítmico acá es clave. Los algoritmos tienen sesgos de fabricación muy importantes que, si bien pueden ser minimizados, es poco probable que sean completamente eliminados. Los sesgos se pueden dar por varias vías:

- Para empezar, los algoritmos se alimentan de datos, pero esos datos son categorizados y separados de manera arbitraria. Desde la categoría sexual binaria hasta la elección de posibilidades de frutas y verduras, las categorías que se eligen para ingresar datos pueden ser sesgadas y dejar grupos enteros de datos sin ser registrados y, por ende, no tenidos en cuenta por un algoritmo.

- A su vez, los datos se cargan con historiales de violencia y discriminación. Por ejemplo, se ha estudiado que las mujeres choferes de UBER en EE.UU. ganan un 7% (Cook et al., 2020) menos que sus colegas hombres, no debido a que manejen peor ni a que sean peores anfitrionas a la hora de llevar un pasajero, sino a que la población tiende a calificarlas más negativamente que a los hombres por aspectos culturales.

- Finalmente, existe un sesgo de programación que es, seguramente, el más importante. La decisión de qué es importante y qué no para un algoritmo es, en definitiva, una decisión humana. Cathy O'Neil tiene un ejemplo muy clarificador (O'Neil, 2016). Ella argumenta que tiene un algoritmo en su cabeza que decide todas las noches qué cocinar para la cena. Las variables que posee es valoración nutricional, elementos que tiene en la heladera, ganas y tiempo de cocinar, lo que comió al mediodía, gustos de la familia, etc. Su

> cabeza procesa eso y decide qué cocinar ese día específico. ¿Qué pasaría si su hijo tomara el control del algoritmo? Seguramente la nutrición pasaría a un segundo plano y los gustos serían predominantes, teniendo como resultado unas papas fritas por sobre un pescado. Aquí se puede ver cómo el sesgo de programación es intrínseco a la persona, empresa, y cultura que programa el algoritmo, ya que decide de forma arbitraria y en base a sus condiciones culturales lo que el algoritmo debe o no debe valorar.

Los sesgos son muchos y tienen impactos enormes sobre las sociedades. Si le sumamos a eso el factor de que la mayoría de los algoritmos que utilizamos a diario son programados en países desarrollados por hombres blancos, de un nivel socioeconómico y educativo determinado, corremos riesgo de que las minorías, disidencias y mujeres jamás sean tenidas en cuenta. En efecto, solamente existen a nivel mundial un 22% de mujeres programadoras. En EE.UU., la mayor economía en la industria, el 67.7% de los programadores son blancos, 19.5% son asiáticos y menos del 13% son personas negras y de otras etnias. Los latinos ni siquiera son contabilizados en las estadísticas (US Data, s.f.).

Ahora bien, ¿por qué es importante todo esto? Porque el artículo claramente prohíbe que se publique el algoritmo y el código fuente. Cabe aclarar que, a los efectos estrictamente técnicos, el algoritmo es la orden dada y el código fuente es la instrucción o el cómo se piensa desarrollar esa orden. Yendo a un ejemplo jurídico, el algoritmo es la ley, el código fuente sería la reglamentación.

En algunos países, como es el caso de Argentina, el software (código fuente y el ejecutable) está protegido bajo la Ley de Propiedad Intelectual, en el marco del derecho de autor. En estos casos, a pesar de existir esa protección para sancionar copias ilegales, por ejemplo, no se impide el acceso a leer el código. Esa prohibición podría darse si el código o algoritmo estuviera protegido por el secreto industrial, como hacen algunas empresas.

En el Perú, el código fuente de un software está protegido por las leyes de derecho de autor, que establecen que cualquier obra literaria, artística o científica, incluyendo el software, está protegida desde su creación, sin necesidad de registro o trámite alguno.

De acuerdo con la Ley de Derecho de Autor peruana (Decreto legislativo, 2003), el titular del derecho de autor sobre un software tiene el derecho exclusivo de autorizar o prohibir la reproducción, distribución, comunicación pública, transformación y

cualquier otro acto de explotación de la obra, incluyendo el código fuente. Además, el autor puede ceder sus derechos a terceros, mediante licencias u otros medios, lo que permite la comercialización y el uso legal del software.

Es importante destacar que, aunque el código fuente de un software está protegido por la ley de derecho de autor, esto no impide la ingeniería inversa o el análisis de su funcionamiento para fines de interoperabilidad o de seguridad informática, siempre y cuando estas actividades se realicen de manera lícita y sin violar los derechos del titular del software.

Lo cierto es que, si no se tiene acceso, no se puede auditar el código para saber qué problemas está teniendo en caso de que algo malo ocurra. La cláusula suele incluir excepciones como en el caso de defensa y seguridad nacional o si hay sospechas de que el algoritmo es contrario a las leyes de competencia del país. La realidad es que es difícil armar un caso que demuestre la necesidad de auditar el algoritmo y que las excepciones no toman en cuenta problemas en la población en general, como el caso de discriminación a trabajadores, trabajadoras o en sistemas de reconocimiento facial, por mencionar algunos. Por otro lado, también cabe aclarar que aun cuando se pueda auditar el código fuente, casi nunca es simple encontrar cuál es el error o identificar el problema que ha surgido. Los algoritmos, en muchos casos a través de Machine Learning, se auto-escriben y terminan siendo ilegibles para los propios programadores. También hay que destacar que en promedio, los programas de código abierto[3] son más fiables que los de código cerrado[4], por lo cual estos traen más beneficios sociales por los motivos antes descritos.

---

3 El concepto de código abierto, que en inglés se conoce como open source, se refiere a un tipo de software que se basa en un modelo de colaboración abierta, es decir que el código fuente se comparte abiertamente porque entiende que existen beneficios prácticos al compartir el código (por ejemplo, al haber más personas que estudian un código y trabajan en mejorarlo o en encontrarle vulnerabilidades, el resultado es un mejor código, por lo tanto, un mejor producto). El código abierto se diferencia del software libre en cuanto a que este último entiende la lógica de compartir el código desde cuestiones morales y filosóficas

4 El código cerrado se llama así en contraposición al código abierto y se refiere al código fuente que no se encuentra disponible para cualquier usuario, es decir no se hace público. Esto es frecuente en empresas de desarrollo que tienen como valor y como recurso competitivo un sistema informático y que lo que hacen es vender licencias de uso de ese sistema, sin habilitar la posibilidad de que ningún competidor pueda estudiar el código y mejorarlo. Acá puede leerse más sobre la diferencia entre ambos tipos de código: Guido Schryen (2009) Security of Open Source and Closed Source Software: An Empirical Comparison of Published Vulnerabilities. Disponible en: https://www.researchgate.net/publication/220891308_Security_of_Open_Source_and_Closed_Source_Software_An_Empirical_Comparison_of_Published_Vulnerabilities

En conclusión, es un problema muy complejo de resolver que la humanidad recién está empezando a enfrentar y que puede tener impactos múltiples en nuestras sociedades generando a futuro discriminación, problemas ambientales, ataques a la democracia y desestabilización económica, entre otros. No parece ser, a simple vista, una buena medida limitar la capacidad estatal ante un problema que recién comenzamos a conocer y que aún no sabemos cómo solucionar. La no divulgación de los algoritmos ha sido problemática hace ya muchos años. Así, aun en los acuerdos de libre comercio, los países han comenzado a poner progresivamente más y más excepciones (Smith, 2017) lo que muestra que dejar ciertos grados de libertad regulatoria, resulta beneficioso frente a un problema que aún se desconoce cómo resolverlo.

El acceso al código fuente puede ser solicitado para casos judiciales por ejemplo para casos de violación de propiedad intelectual de un software, de precisión en los diagnósticos y resultados (por ejemplo, en el caso de un presunto conductor ebrio que quisiera conocer la precisión del sistema de un alcoholímetro). También para saber si el sistema genera o reproduce discriminación en determinadas poblaciones, se puede necesitar acceder al código para estudiarlo y así disminuir las vulnerabilidades al hackeo (por ejemplo, en sistemas de voto electrónico o utilizados en áreas sensibles como puede ser el ámbito de la salud, la seguridad y la administración pública, la infraestructura crítica -como centrales de energía nuclear-, entre otros). Uno de los motivos que pueden tener los gobiernos para requerir acceso al código fuente puede ser para comprobar que se esté cumpliendo con alguna regulación en particular. Un ejemplo de esto es el escándalo de las emisiones de Volkswagen, cuando la empresa de automóviles utilizó el software para superar la prueba de emisiones, aunque, en realidad, estaba contaminando hasta 40 veces más que el límite legal al conducir (Tufekci, 2015).

La UE de hecho, en su aún en negociación, legislación de Inteligencia Artificial (European Commission, s.f.), está estableciendo normas tendientes a auditar aquellos algoritmos que afecten la vida de las personas de forma directa.

Impuestos aduaneros

Si algo vimos durante la pandemia del Covid-19 es que muchas de las cosas que pensamos que jamás iban a ser posibles de digitalizar, lo son. Educación, teletrabajo y telemedicina fueron los grandes cambios, pero otros que venían ganando mercado tímidamente, se aceleraron, como el caso de reuniones y seminarios online, por mencionar algunos. Lo cierto es que a medida que avance

la tecnología, cada vez más proporción de la economía va a poder ser distribuida a través de Internet. De hecho, el proyecto del 5G planea crear ciudades, fábricas y hogares inteligentes, con maquinaria y electrodomésticos que se manejan de manera remota desde otros países (World Economic Forum, s.f.).

Ciudades donde los autobuses no posean choferes y el conductor esté probablemente en un centro de datos en algún territorio alejado y sea un algoritmo. Las impresoras 3D permiten comercializar diseños a través de la web que pueden ser impresos directamente en el país que adquiere el diseño. Esto abre un mundo nuevo en las exportaciones de servicios digitales, desplazando a las exportaciones manufactureras.

En este sentido, prohibir las tasas aduaneras a las transmisiones electrónicas implica no poder cobrar impuestos en frontera por ninguno de estos servicios provistos desde el exterior. Es una desfinanciación del Estado a futuro.

Si bien es cierto que la cláusula no impide cobrar impuestos internos (como impuesto al valor agregado, por ejemplo), sí impide cobrar impuestos aduaneros, lo que deja ver que la intención no es otorgarles menores precios a las y los consumidores, sino que el objetivo es bien distinto. Cuando los impuestos son aduaneros, es el Estado el que los cobra directamente al ingresar al territorio y hacen que los productos nacionales tengan un trato diferenciado de manera indirecta, puesto que no deben pagarlo. Abarata el precio de las mercancías de producción nacional contra las que se producen fuera del territorio. En cambio, los impuestos internos los cobran las empresas directamente al usuario y es esa misma empresa la que es encargada de girar ese dinero al Estado. Esto tiene varios efectos positivos para las empresas trasnacionales. En primer lugar, sólo aquella empresa que posea infraestructura digital lo suficientemente grande para diferenciar los impuestos de cada país en el que opera, podrá ganar mercado. A los competidores pequeños se les hará difícil sostener esa estructura y serán más propensos a cometer errores y, por ende, perder la competencia. En segundo lugar, les da posesión de divisas extra que pueden demorar en el pago, pudiendo producir intereses extra con el manejo de esos fondos. En tercer y último lugar, las normas de trato nacional hacen que, de cobrarles un impuesto interno a las multinacionales, ese impuesto deba ser aplicado también a sus competidores locales. Las economías de escala juegan un papel fundamental ahí donde es mucho más probable que las empresas nacionales no puedan competir a los precios baratos que suelen tener las multinacionales y terminen perdiendo mercado.

En una economía cada vez más digital y globalizada, no poder cobrar impuestos aduaneros a las transmisiones electrónicas es quitarle al Estado su principal fuente de financiación y su capacidad de industrialización digital nacional y soberana, perdiendo empresas tecnológicas nacionales a manos de la competencia internacional.

Esta norma, si bien se está negociando en tratados de libre comercio, ya existe en la OMC hace años a través de la Moratoria de los Derechos de Aduana en las Transmisiones Electrónicas (MDATE). Volveremos a este tema más adelante.

No discriminación contra productos digitales

Básicamente este principio determina que no se puede hacer diferencia entre un producto y otro a la hora de fijar aranceles, subsidios, beneficios impositivos o cualquier otra medida que modifique las condiciones de comercio.

Al incluir los productos digitales en los acuerdos de libre comercio, se está incorporando el Trato nacional y el Acceso a los mercados a todos los productos digitales, a menos que estén expresamente escritos en las excepciones. Así, un producto digital no puede ser tratado de una manera menos favorable que otros productos ni se le pueden restringir los mercados en los que se pueden ofrecer productos digitales o entregables a través de medios digitales.
Esta regulación implica una pérdida de soberanía para tomar decisiones sobre cómo los Estados desean que, de conforme el mercado de bienes y servicios, sobre todo los servicios públicos.

A medida que los servicios digitales avancen, más cantidad de servicios serán ofrecidos por esta vía. La educación es, por ejemplo, sobre todo en el caso de la educación primaria y secundaria, un servicio que típicamente no es transable. Es decir, no se puede exportar servicios educativos de nivel inicial. Muchas veces los Estados protegían estos sectores por ser servicios públicos fundamentales y a fin de conservar soberanía sobre todo y fundamentalmente, dado que es un derecho esencial. Si a partir de la emergencia del Covid-19 la educación cambia y se empieza a brindar a través de plataformas digitales de forma permanente en formato híbrido, ¿ese es un servicio educativo, uno digital, o ambos? ¿Se puede imponer un límite a la utilización de Google Classroom, por ejemplo? Esto es una tendencia creciente en la educación superior donde ya se dictan cursos y carreras de posgrado de forma remota.

Muchos países protegen en la OMC y diversos acuerdos comerciales a sus servicios públicos de las normativas de trato nacional y de acceso a los mercados por temas de interés nacional y soberanía. Pero, al ser un servicio digital, ¿pasa automáticamente a estar afectado por dichas normas impidiendo que un gobierno priorice una plataforma nacional por sobre una foránea?

Estos dilemas se empiezan a plantear en todos los sectores económicos, ya que la incorporación de cibernética es transversal a la economía en su conjunto. Pone en juego los derechos (como la educación y la salud) y la privatización indirecta de los servicios públicos. En efecto, la salud puede ser un servicio público no privatizado, pero si el Estado subcontrata una empresa para que ésta se haga cargo de toda la telemedicina del Estado, entonces esta empresa tendrá los datos y podrá introducir una lógica comercial en el servicio, privatizando de manera indirecta la salud. Esto puede evitarse mediante la firma de un contrato que establezca las reglas mediante las cuales se presta el servicio. Pero, de firmarse este tipo de acuerdo de economía digital, limitará lo que pueda contener ese contrato.

La entrada de los productos digitales a los acuerdos de libre comercio implica la liberalización indirecta de todos los servicios producidos en la economía al presente, de forma indirecta, aun si están protegidos en el acuerdo. No solo eso, sino que también implica liberalizar servicios futuros que aún no han sido creados y que ni siquiera imaginamos.

En el GATT (***General Agreement on Tariffs and Trade***) y el GATS (***General Agreement on Trade in Services***)[5], los gobiernos se tomaron el trabajo de permitir la discriminación de productos cuando se trata de compras públicas. Esto se debe a que muchas veces se usa este recurso para promover productos locales, sobre todo por cuestiones de desarrollo económico o motivos culturales. Si se aplican las normas de Trato Nacional y Nación más Favorecida a los productos digitales sin hacer excepciones, los gobiernos no podrían, por ejemplo, tener preferencias por libros digitales o contenido educativo nacional para estudiantes de escuelas públicas (Smith, 2017).

Contrataciones públicas

Las contrataciones públicas son un instrumento de política pública fundamental. No sólo se utilizan para beneficiar sectores determinados de la sociedad o

5 El GATT y el GATS son los acuerdos de comercio de bienes y servicios de la OMC donde se fijan las reglas comerciales multilaterales que rigen el comercio global.

empresas emergentes en sectores estratégicos, sino que también los socios del Estado y los servicios que contrata el mismo son, en definitiva, la garantía de acceso a derechos fundamentales por parte de la ciudadanía.

En este sentido, las contrataciones públicas son un eje sensible que se debe resguardar cuidadosamente a la hora de realizar compromisos internacionales de acceso a los mercados y trato nacional. Al principio, cuando recién se comenzaban a firmar acuerdos en materia digital en los acuerdos de libre comercio, no se tenía el debido cuidado de salvaguardar estas contrataciones para que estén eximidas de las normas digitales. Esto implica que las normas firmadas, cubren todos los contratos firmados dentro de la economía peruana con empresas del país con el que se firmó el acuerdo en cuestión.

Sin embargo, la creciente importancia de la digitalización hizo ver que de no poner un freno y proteger la contratación pública, muchos servicios protegidos en diversos acuerdo de libre comercio iban a pasar a ser liberalizados. Por eso, se comenzaron a poner cláusulas de excepción.

Para Perú, esas cláusulas de excepción comienzan a introducirse en el año 2017 en el acuerdo CPTPP, luego en el año 2018 con Australia y el último TPP en el 2020. Esto resulta muy beneficioso para Perú, donde los acuerdos más agresivos en materia del Estado no incluyen a los contratos realizados por el estado de forma directa, recobrando algún margen de soberanía y libertad a la hora de proteger a su ciudadanía y garantizar el acceso a servicios públicos de calidad.

Medidas que afectan a las y los consumidores

El siguiente set de medidas, son aquellas que afectan a las y los consumidores y los derechos individuales de la ciudadanía. Derechos de primera generación, que podrían verse vulnerados ante un avance de la agenda digital.

Cabe destacar que estos derechos suelen ser los que más preocupan la agenda de los gobiernos y empresas digitales: en efecto la privacidad, por ejemplo, es sujeto de debates internacionales, regulaciones y financiación tanto por parte de gobiernos como por parte de empresas que bien saben que se no ocuparse de esta temática, pronto se les acabará el negocio.
Si bien la ciudadanía en muchos casos sigue adormecida frente a estos debates diciendo que “no tiene nada que ocultar” y que igualmente las empresas “ya saben quién eres porque libremente les das tus datos ante cualquier suscripción”, esas frases simplifican el debate, que ante nuevos escándalos,

filtraciones y abuso de poder, han dejado en evidencia que en muchos casos se hace un manejo irresponsable, arbitrario y desalmado de los datos, buscando extender la ganancia empresaria a cualquier costo. El fin justifica los medios y en muchos casos los excesos perpetrados para extraer la máxima ganancia de los datos, han sido verdaderamente injustificables y contrarios a derechos humanos fundamentales.

Las empresas saben que, si continúan estos excesos, el propio negocio digital estará más expuesto a regulaciones y, por ende, a menos grados de libertad. Por este motivo, la privacidad, entre otras cuestiones, es un tema de agenda relevante también para las grandes empresas de tecnología.

Autenticación y firmas electrónicas

Esta cláusula establece de forma general que no se pueden imponer restricciones ni limitaciones a las firmas electrónicas. Es decir, si una empresa decide utilizarlas, no se puede reglamentar contra eso. La realidad es que los sistemas informáticos de autenticación y firma electrónica, si bien son bastantes confiables, no están exentos de ataques y hackeos.

Lo cierto es que la fe ciega en los sistemas informáticos, juzgándolos como neutrales, confiables, seguros y veloces, ha hecho que las tecnologías comiencen a estar presentes en los ámbitos más diversos de la sociedad, aun cuando no son recomendados por los especialistas, como el caso del voto electrónico.

La firma electrónica puede no ser segura en muchos casos. Debería existir una vía de escape que permita al Estado regular que determinados contratos y acuerdos no puedan ser efectuados bajo documentos, firmas, o sellos electrónicos. Asimismo, existen diferentes estándares de seguridad.

En informática pueden implementarse medidas sumamente difíciles de romper, como así también estándares laxos fácilmente sorteables. No siempre, pero si generalmente, a mayor seguridad, mayor costo.

Tal y como está redactado este artículo en la mayoría de los acuerdos, uno de los problemas que se presenta es que las partes del acuerdo sean las que decidan qué tecnología de autenticación usarán. Esto se ve claramente en el caso de Visa y Mastercard, dos empresas dominantes que pueden imponerse para establecer los estándares, que implementaron su “software antifraude” en su red comercial

con el propósito declarado de garantizar que el sistema de pago fuera seguro. Sin embargo, la Federación Nacional de Minoristas de EE.UU. calificó el plan como una "casi estafa", y en una impugnación legal se afirmó que "el sistema es menos un sistema para proteger los datos de las tarjetas de las y los clientes que un sistema para obtener ganancias para las empresas de tarjetas a través de multas y sanciones" (Zetter, 2012). De hecho, se ha descubierto que muchas corporaciones son laxas con los datos de las y los consumidores, lo que lleva al robo de identidad y al fraude crediticio (las violaciones de Equifax de febrero y septiembre de 2017 son un ejemplo claro de esto), o a ataques cibernéticos a oleoductos y gasoductos (como le sucedió en abril de 2018 a Energy Services Group en EE.UU. y a Colonial Pipeline en Mayo 2021) (Malik, 2018), y otros problemas que causan daños económicos, a los consumidores y otros daños. Se hace evidente la necesidad de una regulación por parte del Estado -con directivas claras y precisas- y la presencia de una autoridad de aplicación que fije los estándares de seguridad de la tecnología utilizada para la autenticación, incluyendo la posibilidad de definir en qué casos no pueda utilizarse tecnología electrónica y deba recurrirse a otros métodos de autenticación, firmas y sellos.
En un documento de la Red del Tercer Mundo (Smith, 2018) se demuestra que existen fallos sistémicos en los sistemas de ciberseguridad debido a externalidades o asimetrías de información. Estos fallos precisan de regulación efectiva que resuelva el problema, ya que dejar que las propias empresas elijan sus estándares de ciberseguridad ha resultado también problemático debido a que o bien establecen reglas caras difíciles de alcanzar por industrias menores, o los estándares han resultado poco seguros. La regulación de comercio electrónico pone límites a dicha regulación complicando la capacidad del Estado de resolver el problema.

Protección online del consumidor (a)

En principio, la idea es correcta: proteger a las y los consumidores, darles una vía para reclamar, y demandar compensación en caso de que existan problemas. La cuestión aquí es si las agencias de protección al consumidor locales pierden jurisdicción en esta materia. Si bien se las menciona en el artículo diciendo que deben cooperar y que son importantes, no se les da jurisdicción para obrar en caso de que existan casos no resueltos por canales electrónicos. Esto puede ir en detrimento de las y los consumidores que, al no encontrar respuesta de manera directa con la empresa, pueden recurrir a tribunales que no tengan poder para hacer que las empresas cumplan lo que deberían.

Las corporaciones digitales han mostrado una falta de responsabilidad y compromiso en cuanto a garantizar la protección de sus consumidores. Todas las semanas se conocen noticias sobre filtración de datos e información personal y sensible de millones de usuarios y consumidores de todo el mundo de servicios prestados por grandes compañías de tecnología, ya sean proveedoras de servicios de mensajería, redes sociales o de transacciones económicas. Salen a la luz desde contraseñas, números de tarjetas de crédito, fotografías, etc. Además, las y los consumidores han presentado innumerables demandas después de descubrir que sus datos sobre el uso de productos o servicios, desde los auriculares Bose (Graham, 2017) hasta la gestión de correo electrónico (Lohr, 2017) y los juguetes sexuales (Hern, 2017), se vendieron a otras empresas, generalmente sin el conocimiento o consentimiento del consumidor. Un reconocido escándalo internacional fue el de la empresa Facebook, cuando se supo que compartió de manera inapropiada los datos de 87 millones de usuarios con Cambridge Analytica (Lapowsky, 2019) y que podría haber afectado el resultado de las elecciones estadounidenses en 2016.

También existe evidencia de que afectó las elecciones de otros países de América latina como Argentina o Brasil (TelesurHD, 2018). En los casos mencionados se hace evidente el problema al que se enfrentan los consumidores que no logran hacer valer sus derechos ante las corporaciones globales que no atienden sus demandas y la necesidad de que puedan contar con el rol institucional y legal de las agencias de protección de los consumidores locales, que tengan injerencia en esos casos para la protección de consumidores de sus países que quizás no logren resolver los problemas a través de canales electrónicos directos con las compañías.

Medidas contra el spam

Aunque parece una medida contra el spam, en la práctica lo permitirá cuando un consumidor o consumidora ya haya comprado bienes y servicios o cuando la empresa haya "recogido" los datos del consumidor legalmente. Es decir, que, si te diste a conocer en la web como potencial consumidor interesado en determinado producto, automáticamente las empresas están autorizadas a enviarte la cantidad de publicidad que quieran. Esto es así porque las empresas de tecnología venden los datos de los potenciales consumidores a las empresas que proveen estos bienes, con lo cual no es necesario que le hayas dado el dato a una empresa en particular. A partir de que identifican tu perfil de consumidor, todas las empresas que compren dicha información podrán legalmente enviarte publicidad.

Esta situación ya la vivimos hoy en día en Internet todos los usuarios de diversas redes sociales. La infinita cantidad de publicidad que se hace presente en nuestras computadoras ya se ha convertido en inmanejable. Más aún, si hacemos un esfuerzo futurista, a partir de la instalación de la red 5G y los hogares inteligentes, los electrodomésticos pasarán a tener pantallas para sugerirnos compras o avisarnos de fallas o advertencias automáticas. Estos mismos electrodomésticos muy probablemente estén conectados a nuestros teléfonos celulares, enviándonos información a los mismos. Nada impedirá que sea una constante catarata de publicidades en nuestros celulares, en nuestros hogares, cada vez que prendemos un electrodoméstico o nos acercamos a la heladera.

Permitir que los Estados regulen esto a futuro puede defendernos frente a una potencial intoxicación de ofertas, publicidades, y consumismo desenfrenado.

Protección de datos personales y privacidad

Si bien es completamente correcto darle la importancia que se merece la privacidad de los datos personales y no personales, existe una tendencia en diversos acuerdos de libre comercio a permitir analizar los estándares de seguridad y de protección de cada nación basándose en los estándares de otro país. Obviamente, y como suele ocurrir casi siempre, es muy caro y complejo para los países en vías de desarrollo cumplir con determinados estándares, sobre todo los europeos, que le permitan comerciar de igual a igual en la era digital.
La protección de datos y la privacidad se están volviendo vitales en esta nueva revolución industrial y los requerimientos de privacidad que demandan los tiempos que corren no siempre son los que están vigentes en las legislaciones nacionales. Esto no solo exige a los diversos países a actualizar su legislación y adaptarla a la europea, sino además modernizar sistemas e invertir en protección y seguridad con escasos recursos. En definitiva, elevar el estándar es bueno, y exigir una agenda en esa dirección es necesario, lo que hace falta es exigir, pero brindando la ayuda necesaria para llegar a ese estándar deseado.

El artículo declara la importancia de trabajar en el aspecto, pero no asegura compromisos en la materia ni determina cómo ayudar a los países menos desarrollados a tener la capacidad de garantizarlo.

Es decir, no existe un compromiso real en la materia, sino más bien una declaración de interés. Lo que debería suceder es que se exija elevar estándares y se fijen normas mínimas internacionales que garanticen la privacidad y se otorgue a los

países menos desarrollados recursos y ayuda mutua para llegar a esos estándares. Exigir sin dar herramientas puede resultar en una competencia desleal, donde los países que no logren alcanzar las normas establecidas queden fuera de juego.

Esto en el mundo ya se ha visto en otras situaciones, como los estándares medioambientales: son necesarios y positivos, pero implican un alto costo a los países del sur global cuando no fueron ellos los responsables de la contaminación generada en el mundo mayormente. Se les exige alcanzar estándares de emisiones de CO2 cuando las naciones más desarrolladas lograron serlo contaminando sin ningún tipo de control. Hoy los países en vías de desarrollo deben invertir en tecnologías más caras para alcanzar esos estándares internacionales. Eso mismo puede ocurrir con los datos si esta agenda empieza a encauzarse hacia la obligatoriedad. El camino correcto a seguir sería no incluir cláusulas de este tipo en acuerdos de libre comercio y si avanzar en una agenda de cooperación en otros organismos internacionales.

Cabe aclarar que existen normas sobre protección de datos en otros capítulos de los acuerdos de libre comercio, como en finanzas. Pero esos no fueron incluidos en el presente análisis.

El Reglamento General de Protección de Datos de la Unión Europea es un ejemplo claro de regulación en materia de protección de datos personales desde la perspectiva de la protección de la privacidad como un derecho fundamental. En la norma se establece que para que la UE pueda transferir datos personales, su socio comercial debe pasar una “prueba de adecuación” para que los datos estén protegidos (European Commission, 2016). Sin embargo, debido a que Estados Unidos no tiene una regulación única en materia de protección de datos, sino normas locales que difieren de Estado a Estado y entre industrias, la alternativa que existe para que pueda haber intercambios comerciales que involucren datos personales es que la UE permite que EE.UU. incluya en su acuerdo la posibilidad de reconocer que los regímenes voluntarios sean suficientes para cumplir con las disposiciones del acuerdo de libre comercio. Esta es una cuestión que no debería estar sujeta a adjudicación en un acuerdo comercial.

Si se avanzara en este sentido, la decisión iría en contra del régimen de protección de datos y la privacidad de las personas de la UE para poder garantizar el intercambio comercial entre ambas partes. Sin embargo, como indican los antecedentes en materia ambiental, los regímenes voluntarios de cumplimiento corporativo no han logrado los objetivos para los que se implementaron (Laufer, 2003)

Comercio sin papeles

Es evidente que un comercio transfronterizo libre de papeles no sólo coopera con el medio ambiente, sino que también vuelve más ágil un sistema comercial, además de reducir costos y barreras para las empresas. Trabajar en pos de lograr este objetivo es querible a nivel global siendo un beneficio para todos los países. El objetivo a lograr es la digitalización de los flujos de información y requerimientos que son necesarios para que bienes y servicios sean comerciados a través de las fronteras. Sin embargo, el comercio sin papel no es automático, sino que requiere estructuras de gobernanza sólidas y colaboración internacional para garantizar la interoperabilidad de los sistemas (World Economic Forum, 2017).
Sin embargo, el artículo que se refiere a este tema en los acuerdos de libre comercio, obliga a los Estados a poner a disposición medios electrónicos para realizar estos trámites y aceptar la documentación digital como una alternativa válida a la documentación en papel. Dado que la interoperabilidad de los sistemas, los estándares de seguridad diversos, y otros asuntos técnicos, son complejos de migrar y adaptar, la norma puede resultar en un estándar difícil de cumplir, sobre todo para países en vías de desarrollo que no poseen presupuesto disponible para modernizar dichos sistemas.

Un programa conjunto de normalización y recursos necesarios para hacerlo sería un camino más amigable y factible para los países del sur global.

Medidas contrarias a la soberanía

Es común que los acuerdos de libre comercio más recientes incluyan este tipo de normativa. Básicamente el principio de no imponer legislación adicional lleva a poner paños fríos en la capacidad regulatoria del Estado, diciendo que no se impondrá regulación "innecesaria" que entorpezca el comercio electrónico entre países. A su vez, se argumenta en el articulado que se debe participar la opinión de las partes interesadas en un nuevo proceso regulatorio.

Esto es altamente problemático. para empezar, ¿qué se considera innecesario? ¿bajo qué criterio? ¿Quién determina la "necesidad" de una regulación? No se aclara y se presta a controversias.

Por otro lado, se pide facilitar opiniones. En este caso, las partes interesadas son, sobre todo, las empresas afectadas por la regulación, que bajo este acuerdo pasaran a tener "derecho a opinar" y hacer ***lobby*** sobre los reguladores. Es

decir, se busca enfriar la regulación y se busca coartar la soberanía estatal y la capacidad de que un pueblo elija, a través de sus representantes elegidos democráticamente, qué tipo de economía digital quiere tener de puertas adentro de su país.

El programa de comercio electrónico de la OMC y la moratoria

En el ámbito de la Organización Mundial de Comercio hace ya años existe el programa de comercio electrónico. Dicho programa comenzó en el año 1998 (WTO, s.f.).

El único acuerdo vinculante real firmado en dicho momento fue la Moratoria a los Impuestos Aduaneros a las Transmisiones Electrónicas, que básicamente significa que no se cobrarían impuestos por el uso de la tecnología de la información.

Esta moratoria fue negociada por los miembros de la OMC, incluyendo a los Estados Unidos, la Unión Europea, Japón y otros países, y fue una de las medidas tomadas para promover la agenda digital en la OMC. Sin embargo, algunos países expresaron preocupaciones sobre la posibilidad de que la moratoria pudiera afectar negativamente a sus ingresos fiscales y la capacidad de regular el comercio en línea. Por ejemplo, algunos países en desarrollo argumentaron que la moratoria podría desviar los ingresos fiscales que podrían haber sido obtenidos a través de los aranceles y otros impuestos a las transacciones electrónicas. Además, algunos países argumentaron que la moratoria podría debilitar su capacidad para regular el comercio electrónico en línea, lo que podría tener implicaciones para la protección del consumidor y otros objetivos de política pública. Sin embargo, a pesar de estas preocupaciones, se logró un acuerdo que sigue vigente al día de la fecha y se renueva cada reunión ministerial.

Es notable dimensionar que esta moratoria se acordó de forma multilateral en el año 1998, mucho antes de tener dimensión de lo que iba a ser la revolución digital, de que existieran los teléfonos inteligentes y de que las redes sociales modificaran la forma en la que nos comunicamos e informamos.

La moratoria básicamente replica la cláusula de no pagos de impuestos a las transmisiones electrónicas de los acuerdos de libre comercio, pero en el plano multilateral, impidiendo desde el año 1998 que los países en vías de desarrollo y subdesarrollados, importadores netos de servicios digitales, puedan cobrar impuestos aduaneros por los mismos generando una verdadera pérdida fiscal para el sur global.

La inclusión de esa cláusula en los acuerdos de libre comercio tiene como fin lograr que, si alguna vez no se renueva la moratoria, se siga sosteniendo el compromiso a través de la diversidad de TLC que existen.

Si algo es seguro, es que la liberalización digital facilitará las importaciones de contenido digital y no viceversa. Si el comercio digital se expande sin mejorar primero las capacidades productivas y la infraestructura digital (como las mejoras en la infraestructura física y la interconectividad y la adopción de normas aplicables para la privacidad, la protección de datos y los derechos de datos económicos), los países en desarrollo simplemente abrirán sus economías aún más a las importaciones extranjeras (Banga, 2017).

En un documento elaborado por la UNCTAD (United Nations Climate Change Conference) se realizó un ejercicio de simulación que muestra que, si esta moratoria se vuelve permanente, es decir, cero aranceles aduaneros a los productos y transmisiones electrónicas, habrá un aumento adicional de las importaciones de estos productos hacia los países en desarrollo, mientras que las importaciones de los países desarrollados no se verán afectadas. En muchos casos, no todas las importaciones en esta categoría son transmisiones electrónicas, por ejemplo, en el caso de los CD de música, o libros físicos, todavía hay algunas importaciones que no son transferencias electrónicas. A medida que aumenta la digitalización de productos y los consumidores eligen comprar un ***e-book*** o descargarse música a través de plataformas, más de estos productos se incluirán en la categoría de transferencia electrónica. El aumento de las importaciones de este tipo de productos, que actualmente se encuentran en esta categoría, será más alto en términos absolutos para China, seguido por India, Rusia y Brasil (Banga, 2017).

Lo cierto es que la moratoria genera controversias hace años respecto a qué se entiende por transmisión electrónica y si la moratoria cubre solamente a la trasmisión de datos o al contenido de la misma también. La disyuntiva sigue abierta y se debate cada reunión ministerial.

Por otro lado, y más allá de los debates respecto a la moratoria, el programa de comercio electrónico incluía un acuerdo plurilateral que se encuentra actualmente en negociación. En la Reunión Ministerial del año 2017 en Buenos Aires, se firmó una declaración conjunta sobre comercio electrónico (WTO, 2017) que incluye a Perú como país negociador del acuerdo plurilateral. En la misma se compromete a trabajar en un acuerdo conjunto y continuar con el programa

de comercio electrónico iniciado en el año 1998. El borrador del acuerdo en cuestión se filtró (Bilaterals, 2021) y allí puede verse un texto con todas las características de los acuerdos de libre comercio y algunas controversias que no se logran resolver en breve. Lo cierto es que, al negociarse de forma plurilateral, los documentos del mismo no son públicos, por lo que es difícil conocer las intenciones de cada país. Pero si se puede ver que se incluyen muchas de las cláusulas explicadas anteriormente.

Actualmente la negociación sigue en curso y existen presiones para alcanzar un acuerdo de cara a la próxima Reunión Ministerial de la OMC a realizarse en febrero del 2024 en Emiratos Árabes Unidos.

La renegociación con la UE y el modelo que exporta la región: un enfoque centrado en los derechos individuales

El modelo utilizado por la UE para sus negociaciones comerciales en términos de comercio electrónico fue cambiando con el tiempo. Al principio las cláusulas no constituían un capítulo aparte y en muchos casos eran más compromisos de trabajo en la agenda que acuerdos vinculantes detallados. Lo cierto es que la UE no parecía tener una estrategia clara respecto a la economía digital. En el año 2010 el vocabulario utilizado empieza a fijar cada vez más compromisos, hasta el año 2016, donde la agenda cambia radicalmente (Scasserra & Martinez Elebi, 2021) incluyendo artículos altamente problemáticos como la limitación de localización de datos y procesamiento, la libre movilidad de datos y el secreto algorítmico, entre otros.

La UE es especialmente insistente en las políticas de protección de datos, buscando el compromiso de sus socios comerciales para que cumplan las normas internacionales de protección de datos. La cooperación se enmarca cada vez más en términos más concretos e incluye el reconocimiento mutuo de los certificados de firma electrónica, la coordinación sobre la responsabilidad de los proveedores de servicios de Internet, la protección de los consumidores y el comercio sin papel, entre otras. EE.UU., por ejemplo, no es tan claro ni taxativo en este aspecto en los acuerdos que firma a nivel internacional (Burri, 2022). A su vez, EE.UU. busca definir al principio de sus capítulos qué entiende por productos digitales y por transmisiones electrónicas (tema no resuelto en el marco de la OMC). A su vez, muchos de los acuerdos de EE.UU. poseen un sistema de listas negativas, donde todo aquello que no se protege, queda liberado, al contrario del sistema frecuentemente utilizado por la UE de listas positivas.

En este sentido, se podría argumentar que el objetivo de USA es acceder a la venta de la mayor cantidad de productos digitales libres de impuestos dentro del mercado local. Al contrario, la UE posee una estrategia más centrada en proteger los derechos de sus ciudadanos y ciudadanas en términos de privacidad y protección al consumidor, estableciendo una estrategia de extractivismo de datos que le permite generar industrias digitales al interior de su propia economía.

Perú posee un acuerdo con la UE firmado en el año 2012 que incluye pocas cláusulas al respecto. Entre ellas, limitaciones a la localización de datos, comercio sin papeles, no impuestos aduaneros, protección al consumidor y protección de datos personales, mostrando que en ese momento la agenda comercial europea iba avanzando en la dirección marcada. Es de esperarse que, si Perú reabre la negociación con la UE, las demás cláusulas pasen a estar en la agenda de negociación utilizando el formato típico que utilizan para los capítulos de comercio electrónico.

La agenda comercial europea actual incluye las cláusulas de libre movilidad de datos, auditoría algorítmica, y firmas electrónicas por mencionar algunas. También incluye otras igualmente problemáticas que no están incluidas en el presente trabajo porque Perú no las ha firmado aún. A saber:

- La no responsabilidad de los intermediarios, cláusula que exime a las empresas digitales de la responsabilidad que puedan tener por el contenido que circula en sus plataformas; y
- La autorización previa, cláusula que prohíbe la posibilidad de pedir autorización previa de una empresa digital a un estado nacional o municipal para operar en esa región. Es decir, las empresas pueden entrar sin pedir permiso, lo que puede limitar la capacidad de diseñar y programar la economía digital de una ciudad o país. Existen ciudades que han, por ejemplo, prohibido el ingreso de UBER en protección de los taxis tradicionales (Tourism Review, 2019). Esto no podría hacerse si esta cláusula se firmara en acuerdos internacionales.

El Tratado Transpacífico y el programa APEC: la apertura al modelo asiático digital

Perú tiene una historia de búsqueda de socios comerciales mirando hacia el océano pacífico. El vasto océano no parece ser un impedimento para ver como socios estratégicos países alejados, más que a los demás países de la región latinoamericana.

Sea como fuere, se podría marcar un punto histórico donde comienza esta asociación que se irá profundizando a lo largo de los años. Ese momento histórico es la incorporación de Perú al APEC (Foro de Cooperación Asia-Pacifico) en el año 1998. El foro no posee normas comerciales vinculantes, pero busca generar acuerdos por consenso sobre líneas de trabajo en términos de facilitación al comercio e inversiones.

El programa de APEC posee un capítulo digital. En el mismo, se tratan de establecer líneas de trabajo respecto a la interoperabilidad de los sistemas, el acceso universal a internet y el desarrollo de infraestructuras digitales, entre otros. En el documento de trabajo sobre cuestiones digitales se puede ver cómo se sientan las bases de acuerdos comerciales posteriores: se insta a los gobiernos a normalizar la regulación nacional buscando estándares internacionales, facilitar la libre movilidad de datos y el comercio electrónico. El documento busca ser cuidadoso con la forma en la que expresa estas cuestiones, puesto que en APEC existen fuertes jugadores con estrategias digitales completamente distintas, como EE.UU. y China, países que se encuentran en una contienda económica y comercial por el dominio de las redes mundiales y las plataformas que operan en internet. Ambos modelos requieren de condiciones distintas respecto a la neutralidad en la red (que se permite y que no se permite en internet), la responsabilidad de los intermediarios y la localización de datos, por mencionar algunos.

Parecería ser que más que estándares internacionales, APEC busca centrarse en las normas nacionales de cada país, buscando estandarizar la regulación. Existe un documento donde se listan todas las regulaciones pertinentes en materia digital de cada uno de los países miembros, donde Perú listó todas las

normativas nacionales de protección de datos, protección al consumidor, firmas electrónicas, spam, y acceso al dinero electrónico, buscando mostrar el trabajo que ha realizado en esos términos e informando a los demás miembros de sus avances en materia regulatoria.

El programa APEC es entonces, no un acuerdo comercial estándar, sino más bien un foro donde se sientan o se preparan las bases para posteriores acuerdos comerciales en la zona del pacifico, que Perú ha utilizado a posteriori.

La firma del TPP marca un nuevo rumbo en materia comercial en el Perú. No solo se firmó uno de los acuerdos más liberalizadores y agresivos de la historia comercial, sino que se afianza la estructura económica de Perú mirando hacia la región del pacifico. La implementación del acuerdo resulta fallida ya que EE.UU. se retira del acuerdo debido al fuerte descontento que existían en ese momento por la multiplicidad de acuerdos mega regionales que estaba negociando EE.UU. y sus potenciales impactos en la economía norteamericana. En efecto, la sociedad civil norteamericana logró hacerse escuchar y EE.UU. se desvinculó del TPP y del TISA, uno de los acuerdos más liberalizadores de la economía digital que habían existido hasta ese momento.

Al caer el TPP, los países que habían quedado dentro del paraguas del acuerdo, firman el CPTPP quitando algunas de las exigencias que EE.UU. había hecho para unirse al acuerdo, y que muchos de los países se oponían. No obstante, el texto sigue siendo uno de los más liberalizadores en materia digital de los acuerdos existentes a la fecha. Para empezar, toma como estándar en materia de protección de datos personales, las normas menos exigentes o más laxas a nivel nacional (Burri, 2022). Es decir, se asume como estándar internacional lo que todos los países miembros tengan aprobado, y no la norma más protectora de la privacidad de las personas.

Por otro lado, resuelve la controversia de la moratoria a los impuestos aduaneros: el TPP exige que no se puedan imponer barreras aduaneras no solo a la transmisión electrónica (o sea, la importación/exportación de datos) sino también al contenido de la misma. Esto significa no solo liberalizar el extractivismo de datos, sino que también liberaliza sectores que pueden haber sido protegidos pero que a futuro se podrán proveer digitalmente. Por ejemplo, si Perú protegió su sistema educativo para que sea nacional, pero se comienzan a dictar cursos online, Perú no podrá imponer impuestos aduaneros por tomar cursos en el exterior a través de medios electrónicos.

En términos de ciberseguridad, el TPP no hace exigencias de estándares mínimos a los países miembros, sino que expone la importancia de trabajar en esa línea, pero nada más. Este tema es particularmente sensible, ya que la falta de estándares diseñados e implementados por los estados llevan al libre albedrío de las empresas que en muchos casos descuidan estos aspectos, por ser cuestiones que hacen a la calidad de los servicios digitales, pero es inversión que el consumidor no ve hasta que no ocurran los problemas. Es decir, si bien se empieza a tomar más conciencia, es difícil que un consumidor acepte un producto más caro solo porque posee mayores protecciones en materia de ciberseguridad.

En cuanto a las excepciones establecidas en el acuerdo, existen algunas respecto a la localización de datos y procesamiento, pero estas, como ya es costumbre, utilizan palabras ambiguas. Se pueden romper las reglas siempre y cuando sea para alcanzar un objetivo "legítimo" de política pública, sin explicar ni determinar exactamente qué se considera "legítimo". Este tipo de excepciones son raramente utilizadas por los países en los acuerdos comerciales, justamente por esa ambigüedad que lleva a controversias claras cuando hay intereses contrapuestos, teniendo un efecto tranquilizador en materia regulatoria, llevando a los países a no imponer regulación adicional para evitarse problemas, aun cuando fuera necesario.

Respecto al acceso al código fuente, es notable que tanto el CPTPP como el TPP salvaguardan el acceso al mismo cuando éste es para la instalación de infraestructura crítica. Es decir, Perú puede pedir acceso para conocer la forma en la que fue programado un software cuando este es para adquirir o instalar infraestructura vital para el país. Pero tiene extremadamente prohibido hacerlo para cuando este software sirve para la venta de productos masivos. En algunos casos se podría solicitar ese código para verificar que cumpla con leyes a favor de la competencia y libertad de mercados, pero esto está taxativamente prohibido bajo este acuerdo comercial. Lo cierto es que las excepciones a este artículo son variadas en los acuerdos comerciales y han ido creciendo en los últimos años. Existen estudios (Smith, 2017) que muestran cómo estas excepciones van creciendo a lo largo de los años e incluyen cada vez más ítems. El TPP si bien establece una excepción, no resulta en el acuerdo comercial que más excepciones permita.

El acuerdo del CPTPP en materia digital representa una base, un primer paso, para una nueva era de acuerdos comerciales en materia digital con una apertura

comercial indiscriminada, salvaguardando los intereses de las empresas y los inversionistas, por sobre los intereses de los ciudadanos. Las normas duras están más puestas en pos de la liberalización comercial que en pos de la protección de la seguridad, la privacidad y la competencia. Es de esperarse que estos acuerdos sigan avanzando tanto en el ámbito de la OMC como en diversos acuerdos comerciales (como el TISA si es que se revive), configurando una economía abierta para ser territorio donde se dispute la guerra comercial entre EEUU y China por la dominación global de las redes de comunicación y los productos digitales: la industria digital busca tener un claro ganador, y solo dos países tienen hoy dia posibilidad de llegar a lo más alto del podio. Perú, y los demás países del mundo, configuran solamente la cancha donde se disputa el partido.

CONCLUSIONES

¿Qué se juega el Perú en su futuro digital?

La digitalización hace algunas décadas representaba algo novedoso, pero sin demasiada relevancia en la vida de las personas. Poco a poco fue ganando espacio y pasó de ser un tema meramente relacionado con la empleabilidad de la mano de obra, a ser una cuestión esencial para la vida humana.

Lo cierto es que sea como fuere, el mundo apenas comienza a comprender el impacto que la digitalización y la automatización a través de inteligencia artificial tiene en la vida de las sociedades en general y los individuos en particular. Se vive un mundo donde internet y las maravillosas herramientas que supo proporcionar, modifican las formas de vida en esferas tan diversas como la educación, la salud, la democracia, la cultura, la información, y el empleo. Aprender a manejar y producir herramientas digitales no sólo es vital para acceder a empleos de calidad y a cadenas globales de valor, sino que también es vital para acceder a servicios públicos y derechos humanos fundamentales.
Los impactos son muchos, positivos y negativos, se han visto en los últimos años de ambos tipos en la historia de internet. Sistemas automatizados que discriminaban mujeres y se descubrió años más tarde (Dastin, 2018) o herramientas que salieron al mercado para advertir semanas más tarde que destruirán cientos de miles de puestos de trabajo a nivel global (Eloundou et al., 2023). Tanto debate se genera, que se hace imperiosa la regulación. Lo que se debate aquí es si la humanidad quiere una tecnología al servicio de la gente, o poner a las poblaciones al servicio y esclavitud de la tecnología y sus creadores. La regulación es la única capaz de equilibrar una balanza que ya se encuentra favoreciendo claramente a los que poseen los medios de producción, la tecnología y la información para construir industrias digitales.

En este sentido, la regulación posee una característica fundamental: trabaja sobre acontecimientos del pasado. Es común que se diga que la regulación “llega tarde”. Esto es así porque los reguladores actúan frente a problemas reales que existen y tratan de resolverlos, pero en materia digital, estos problemas aún no se conocen en su totalidad. ¿Cómo regular el futuro? ¿Cómo comprender la realidad que se avecina frente a un mundo que cambia tan estrepitosamente?

Es imposible regular lo que se desconoce y la multiplicidad de usos y artefactos tecnológicos que pueden crearse en los años por venir.

En este sentido, los acuerdos comerciales en materia digital no solo ponen un freno a la infinita posibilidad de regulaciones que pueden aparecer, sino que también ven lo digital como un asunto meramente económico, donde lo que se debe resolver es la controversia respecto a cómo se hacen negocios en internet. Y la realidad es que no es así: internet mostró su potencial en términos de acceso a servicios públicos, a poder alcanzar derechos humanos fundamentales, y a darle oportunidades a poblaciones vulnerables y alejadas. Internet es un espacio donde cosas horribles han acontecido, pero también cosas maravillosas, como la inclusión, la comunicación y nuevas oportunidades.

Poder potenciar esas maravillas, y minimizar lo negativo solo es posible con un Estado fuerte que ponga un freno a abusos, haga que los responsables de dichos impactos negativos se hagan cargo y muestren lo que la sociedad peruana desea ser en un espacio digital. Hoy día existe la creencia de que "la culpa es del algoritmo" o "del sistema que no anda". Lo cierto es que detrás de esos sistemas y de esos algoritmos existen responsables de carne y hueso, humanos que han tomado decisiones de inversión y financiamiento y que no siempre tratan de maximizar el medio ambiente, el bienestar de los ciudadanos y los valores democráticos, sino más bien la ganancia empresarial. Se vive un sistema capitalista, no es para sorprenderse, y estos sistemas tienen múltiples impactos, muchos de ellos indeseados, que necesitan ser estudiados y reglamentados para sacar el mayor beneficio social de los mismos, y no solamente la mayor ganancia empresarial.

A su vez, los datos se han vuelto fuente de poder en el desarrollo de políticas públicas, generando estados inteligentes que tengan capacidad de llegar a los que más lo necesitan. Los datos pueden ser utilizados con fines comerciales, pero también pueden ser utilizados para otros fines. Una misma base de datos puede tener múltiples usos: para fines comerciales, para investigación y desarrollo académico, para conocer poblaciones y construir información estadística, para mejorar políticas públicas, para llevar adelante un programa medioambiental, para lograr la igualdad de género, etc. Todos estos fines múltiples hacen que los datos sean bienes no rivales o excluyentes: es decir, que lo utilice alguien no significa que no pueden ser utilizados por otros. En ese sentido, los datos se configuran como bienes comunes (Scasserra & Sai, 2020), bienes que pertenecen

no sólo a aquella empresa que los extrajo, sino a la población que los generó, que mucho provecho puede sacar de ellos. Restricciones a la localización y acceso a los mismos, buscan coartar esto y quitarles ese derecho a poblaciones enteras, privatizando un bien que debería ser de todos los ciudadanos.

Perú ha iniciado un camino hacia la privatización, la liberalización y el entendimiento de las herramientas digitales como un espacio económico para el negocio de pocas empresas tecnológicas. Falta mucho camino por recorrer: aún no ha firmado acuerdos fuertes con los países más poderosos del mundo en materia digital y que más prácticas extractivistas tienen, como China, EE.UU. y la UE. Pero el primer paso está dado en una senda que llevará a restringir su capacidad regulatoria futura cuando haya que minimizar los daños e impactos negativos. La UE se encuentra transitando ese camino regulatorio y aun con todo su presupuesto y especialistas en el tema, ha encontrado sinuosos caminos donde no ha podido lograr una regulación que no se contraponga a estos acuerdos comerciales, suscitando preocupación de parlamentarios y especialistas (James, 2023). Firmar en esta instancia histórica acuerdos que pongan techos regulatorios, no parece ser el mejor camino hacia un futuro incierto, sino que, al contrario, dejar márgenes de maniobra y ser dúctiles parece ser una estrategia acertada en este mundo vertiginoso y cambiante.

El presente digital de Perú en particular y de América latina en general se construye día a día con nuevas herramientas inclusivas y poderosas nuevas oportunidades de negocios. Ese mundo digital creció a pasos agigantados en las últimas décadas de forma completamente desregulada. Argumentar que los acuerdos de libre comercio harán crecer la economía digital es una falacia: lo han hecho sin esos instrumentos. Lo que se debate aquí es si ahora que los gobiernos han descubierto sus aspectos negativos, tendrán la libertad de mitigarlos o no.

Naciones Unidas se encuentra en un proceso de debate respecto al nuevo Pacto Digital Mundial (Naciones Unidas, s.f.) que tiene en cuenta estos aspectos. Sería bueno mirar con mayor detenimiento este tipo de iniciativas más que querer llevar a la esfera comercial algo que trascendió lo meramente económico hace ya mucho tiempo.

BIBLIOGRAFÍA Y REFERENCIAS

Banga, R. (2017). ***Rising Product Digitalisation and Losing Trade Competitiveness Rising Product Digitalisation and Losing Trade Competitiveness***. ResearchGate. https://www.researchgate.net/publication/318469170_Rising_Product_Digitalisation_and_Losing_Trade_Competitiveness_Rising_Product_Digitalisation_and_Losing_Trade_Competitiveness

Bilaterals. (2021). ***Home***. Bilaterals. https://www.bilaterals.org/?wto-plurilateral-ecommerce-draft-45155&lang=en

Burri, M. (2022, July 29). ***The Regulation of Data Flows Through Trade Agreements***. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3028137

CEPAL. (2016). ***Home***. https://www.cepal.org/es/publicaciones/38604-la-nueva-revolucion-digital-la-Internet-consumo-la-Internet-laproduccion
Colocation America. (2020, January 30). ***Renewable Energy and the Future of Data Centers***. Colocation America. https://www.colocationamerica.com/blog/renewable-energy-data-centers

Cook, C., Diamond, R., Hall, J. V., List, J. A., & Oyer, P. (2020). ***The Gender Earnings Gap in the Gig Economy: Evidence from over a Million Rideshare Drivers***. Stanford University. https://web.stanford.edu/~diamondr/UberPayGap.pdf
Dastin, J. (2018, October 10). ***Amazon scraps secret AI recruiting tool that showed bias against women***. Reuters. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

Decreto legislativo. (2003). ***Ley sobre el Derecho de Autor - DECRETO LEGISLATIVO Nº 822 (*)***. Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual. https://www.indecopi.gob.pe/documents/20182/143803/DecretoLegislativo822.pdf

Eloundou, T., Manning, S., Mishkin, P., & Rock, D. (2023, March 17). ***GPTs are GPTs: An early look at the labor market impact potential of large language models***. OpenAI. https://openai.com/research/gpts-are-gpts

European Commission. (2016). ***Home***. https://ec.europa.eu/info/law/law-topic/dataprotection/international-dimension-data-protection/adequacy-decisions_en

European Commission. (2020). ***52020DC0066 - EN - EUR-Lex***. EUR-Lex. https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

European Commission. (s.f.). ***The Artificial Intelligence Act***. The Artificial Intelligence Act |. https://artificialintelligenceact.eu/

European Parliament. (2016). ***EUR-Lex - 32016R0679 - EN - EUR-Lex***. EUR-Lex. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Federal Register of Legislation - Australian Government. (2012). ***Home***. https://www.legislation.gov.au/Details/C2012A00063

5G Americas. (2020). ***Global 5G: Rise of a Transformational Technology***. 5G Americas. https://www.5gamericas.org/global-5g-rise-of-a-transformational-technology/

Graham, J. (2017, April 20). ***Bose is accused of recording, selling audio information***. Boston Herald. https://www.bostonherald.com/2017/04/20/bose-is-accused-of-recording-selling-audio-information/

Hern, A. (2017, March 14). ***Vibrator maker ordered to pay out C$4m for tracking users' sexual activity***. The Guardian. https://www.theguardian.com/technology/2017/mar/14/we-vibe-vibrator-tracking-users-sexual-habits

Information Technology Industry Council. (2017, January 19). ***Data Localization Snapshot***. Data Localization Snapshot Current as of January 19, 2017 Active Measures. https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf

Inland Revenue. (s.f.). ***Home***. http://www.ird.govt.nz/technical-tax/revenue-alerts/revenue-alertra1002.html

James, D. (2023, March 28). ***EU Digital Trade Rules: Undermining attempts to rein in Big Tech.*** https://left.eu/issues/publications/eu-digital-trade-rules-undermining-attempts-to-rein-in-big-tech/

Kumar, S. (2020, August 4). ***Are Data Centres Helping The Economy? TechNative.*** https://technative.io/how-data-centres-are-helping-the-economies/

Lapowsky, I. (2019, March 17). ***How Cambridge Analytica Sparked the Great Privacy*** Awakening. WIRED. https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/

Laufer, W. S. (2003). ***Social Accountability and Corporate Greenwashing. ResearchGate.*** https://www.researchgate.net/publication/226631106_Social_Accountability_and_Corporate_Greenwashing

Lohr, S. (2017, April 24). ***Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data*** (Published 2017). The New York Times. https://www.nytimes.com/2017/04/24/technology/personal-data-firm-slice-unroll-me-backlash-uber.html

Malik, N. S. (2018). Home. https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hotseat

Mazzucato, M. (2014). ***El Estado emprendedor: mitos del sector público frente al privado.*** RBA.

Naciones Unidas. (s.f.). ***Pacto Digital Mundial |*** Oficina del Enviado del Secretario General para la Tecnología. https://www.un.org/techenvoy/es/global-digital-compact

O'Neil, C. (2016). ***Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.*** Crown.

Reiff, N. (2021). ***How Visa Makes Money: Data Processing, Service, and International Transactions.*** Investopedia. https://www.investopedia.com/how-visa-makes-money-4799098

Scasserra, S., & Foronda, A. (2022, November 23). ***Un paraiso de datos. Transnational Institute.*** https://www.tni.org/es/publicaci%C3%B3n/un-paraiso-de-datos

Scasserra, S., & Martinez Elebi, C. (2021, October 7). Colonialismo digital. Transnational Institute. https://www.tni.org/es/publicaci%C3%B3n/colonialismo-digital

Scasserra, S., & Sai, L. (2020). tapa 56_Maquetación 1. Bibliothek der Friedrich-Ebert-Stiftung. https://library.fes.de/pdf-files/bueros/argentinien/16371.pdf

Smith, S. R. (2017, December 10). S*ome of the implications of ecommerce proposals for government procurement - MC11 briefing paper* Introduction Liberalisation. Our World Is Not For Sale. https://ourworldisnotforsale.net/2017/TWN_Procurement.pdf

Smith, S. R. (2017, December 10). ***Some preliminary implications of WTO source code proposal Introduction.*** Third World Network (TWN). https://www.twn.my/MC11/briefings/BP4.pdf

Smith, S. R. (2018). ***Third World Network Preliminary Note: Electronic authentication: some implications***. Third World Network (TWN). https://www.twn.my/announcement/TWN_esignatures2018-9.pdf

Taylor, P. (2022, August 26). ***Big data and business analytics revenue 2022***. Statista. https://www.statista.com/statistics/551501/worldwide-big-data-business-analytics-revenue/

TelesurHD. (2018). ***Home.*** https://www.telesurenglish.net/%20analysis/Cambridge-Analytica-in-Latin-America-What-We-Know-So-far-20180322-0028.html

Tourism Review. (2019, April 22). ***Cities That Banned Uber – Fighting the Impact on Economy |*** .TR. Tourism Review. https://www.tourism-review.com/many-cities-around-the-world-banned-uber-news11032

Tufekci, Z. (2015, September 23). Opinion | ***Volkswagen and the Era of Cheating Software*** (Published 2015). The New York Times. https://www.nytimes.com/2015/09/24/opinion/volkswagen-and-the-era-of-cheating-software.html

US Data. (s.f.). Home. https://datausa.io/profile/soc/151251

Whittaker, Z. (2013, January 28). ***What Google does when a government requests your data.*** ZDNET. https://www.zdnet.com/article/what-google-does-when-a-government-requests-your-data/

World Economic Forum. (s.f.). ***Home.*** https://www.weforum.org/projects/5g-global-accelerator

World Economic Forum. (2017, November 2). ***World Economic Forum.*** World Economic Forum. https://www.weforum.org/whitepapers/paperless-trading-how-does-it-impact-the-trade-system/

World Economic Forum. (2020, June 9). ***Where data is stored could impact privacy, commerce and even national security.*** The World Economic Forum. https://www.weforum.org/agenda/2020/06/where-data-is-stored-could-impact-privacy-commerce-and-even-national-security-here-s-why/

WTO. (s.f.). WTO | E***lectronic commerce. World Trade Organization.*** https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm

WTO. (2017). OMC | ***Comercio Electrónico. World Trade Organization***. https://www.wto.org/spanish/tratop_s/ecom_s/joint_statement_s.htm

Zetter, K. (2012, January 11). ***Rare Legal Fight Takes On Credit Card Company Security Standards and Fines.*** WIRED. https://www.wired.com/2012/01/pci-lawsuit/


red GE
GLOBALIZACIÓN CON EQUIDAD
15 años