DOI: https://doi.org/10.24215/24689912e019

DATOS PERSONALES: SEGURIDAD NACIONAL Y CONCERTACIÓN INTERNACIONAL. LA DISYUNTIVA LATINOAMERICANA

PERSONAL DATA: NATIONAL SECURITY AND INTERNATIONAL AGREEMENTS. THE LATIN AMERICAN OPTION

Marcelo Halperin

RESUMEN
Conmovieron a la prensa internacional las restricciones adoptadas por el gobierno estadounidense, primero para impedir compras gubernamentales (Ley de Autorización de Defensa Nacional 2019) y, más recientemente, para evitar la actualización de sistemas operativos de equipos de telecomunicaciones suministrados por empresas chinas (Orden Ejecutiva del Presidente, del 16 de mayo de 2019). Pero rápidamente se advirtió que las últimas medidas podían resultar no sólo ineficaces sino, peor aún, producirían efectos adversos. La amenaza que representa el desarrollo de redes y sistemas de alta velocidad para la manipulación de datos y, por extensión, para la seguridad nacional de Estados Unidos (EUA), ya no podría neutralizarse con medidas comerciales ni mediante las reglas de propiedad intelectual. En este sentido, la modalidad de código abierto en las patentes de sistemas operativos para dispositivos electrónicos, pone en evidencia que los estatutos de propiedad intelectual están flexibilizándose y adaptándose a muy aceleradas sustituciones tecnológicas, las cuales, en el sector de las tecnologías de la información y las comunicaciones (TIC) apuntan a la captura y manipulación de datos personales con una voracidad inédita.

En este contexto y con motivo del flujo electrónico de datos personales desde la Unión Europea (UE) hacia EUA y ante la dificultad para armonizar sus normas, en los últimos años se habilitó un "Escudo de Privacidad" con el objeto de garantizar los derechos de los usuarios y compatibilizar la actividad de empresas tecnológicas con los principios de interés público en ambos lados del Atlántico. Este régimen podría ser un valioso antecedente en el diseño de un acuerdo internacional de carácter multilateral destinado a reglar la conectividad global.

PALABRAS CLAVE
Datos personales – seguridad nacional – escudo de privacidad – conectividad globlal

ABSTRACT
The restrictions adopted by the US government shocked the international press, first to prevent government purchases (National Defense Authorization Act for Fiscal Year 2019 (NDAA) Sec.889), and more recently to prevent the updating of telecommunication equipment operating systems produced by Chinese companies (Executive Order issued by President Trump on May 16, 2019). But it was quickly noticed that the latest measures could be not only ineffective but, worse still, would lead to adverse effects. The threat posed by the development of high-speed networks and systems for the manipulation of data and, by extension, for the national security of the United States (USA), could no longer be neutralized by trade measures or by intellectual property rules. In this sense, the open source modality in the patents of operating systems for electronic devices, shows that the intellectual property statutes are becoming more flexible and adapting to very fast technological substitutions which, in the information & technology sector, point to capture and manipulate personal data with un-precedent voracity.

In this context and due to the electronic flow of personal data from the European Union (EU) to the USA and faced with the difficulty for a regulatory convergence, a "Privacy Shield" was set up in order to guarantee the rights of the users and make the activity of companies compatible with the principles of public interest on both sides of the Atlantic. This could be a valuable precedent for the design of an international agreement of a multilateral nature aimed at regulating global connectivity.

DOI: https://doi.org/10.24215/24689912e019

KEY WORDS
Personal Data – National Security – Privacy Shield – Global Connectivity

DOI: https://doi.org/10.24215/24689912e019

INTRODUCCIÓN

Merecería una segunda lectura la medida del gobierno de Estados Unidos de América (EUA) por la cual se decidió imponer restricciones comerciales a fin de neutralizar actividades contrarias a la seguridad nacional y que, en mayo de 2019, salió a la palestra con motivo del caso de la empresa china HUAWEI. La disposición aludida consistió en una Orden Ejecutiva dictada por el Presidente el día 16 de mayo, por la cual se prohibió a las empresas estadounidenses utilizar dispositivos elaborados por compañías cuyas actividades pudieran hacer suponer un riesgo para la seguridad nacional. De modo que la fijación de restricciones comerciales excedió el caso de esta sola empresa, proveedora de teléfonos celulares inteligentes (*smartphones*) y con una participación significativa en el mercado.

La Orden Ejecutiva del Presidente norteamericano estuvo anticipada e inspirada por la Ley de Autorización de Defensa Nacional de 2019 (*National Defense Authorization Actfor Fiscal Year 2019, NDAA*) cuya Sección 889 autorizó a las autoridades de agencias ejecutivas del Estado federal a imponer, en determinadas circunstancias, restricciones para contratar adquisiciones o prestaciones o autorizar préstamos, concesiones o subsidios destinados a la adquisición u obtención de los elementos descritos en los siguientes términos, tan amplios como minuciosos: *"any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component or any system, or as critical technology as part of any system"*[1].

Las medidas, según dicha Ley, pueden ser aplicadas en atención a objetivos de seguridad nacional, para impedir la adquisición por las reparticiones públicas federales de tales bienes producidos o provistos por entidades respecto de las cuales las autoridades competentes estimen razonablemente que son propiedad de un Estado extranjero, o están controladas por él o bien vinculadas de algún modo con un Estado extranjero.[2] Pero además, algunas de estas empresas ya están definidas por la propia Ley, como es el caso de HUAWEI TECHNOLOGIES COMPANY y ZTE

[1] Ley citada, Sec. 898 *"Prohibition on certain telecommunications and video surveillance services or equipment",* (a) (A).
[2] "The term "covered telecommunications equipment or services" means any of the following: […] Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonable believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country" (Sec. 898 (f) *Definitions*, 3 D).

DOI: https://doi.org/10.24215/24689912e019

CORPORATION, incluyendo a cualquiera de sus subsidiarias o afiliadas[3] contra las cuales pueden adoptarse las medidas de referencia, pero en estos dos casos sin hacer alusión a la necesidad de contar con la presunción sobre su vínculo con un Estado extranjero. Por lo demás, el concepto de "Estado extranjero" *("foreign country"*) "significa" *("theterm "covered foreign country means"*), lisa y llanamente: REPÚBLICA POPULAR CHINA.[4]

Más allá del soporte legal que pudiera justificar formalmente la decisión presidencial, convendría detenerse sobre las motivaciones políticas que indujeron la elaboración de una nómina de empresas extranjeras, en principio chinas, a las que se impondrían las restricciones comerciales, ya no sólo en el ámbito de las contrataciones públicas sino directamente para operar en el mercado estadounidense, según el criterio del Departamento de Seguridad Nacional y luego del Departamento de Comercio de EUA. Entre las presuntas amenazas resalta una supuesta capacidad –actual o potencial- para la apropiación y consiguiente manipulación de datos –incluyendo los datos personales- mediante el control de redes de alta velocidad, que se suma a la presunción, por las autoridades estadounidenses, de sus vinculaciones con el Estado extranjero (CHINA) donde se asienta la respectiva matriz. De ahí la estrecha relación entre la Orden Ejecutiva y la Ley de Defensa Nacional. Desde la perspectiva del gobierno de EUA, inicialmente se consideró verosímil la sospecha sobre una amenaza de HUAWEI a la seguridad nacional.[5] De ahí las prontas reacciones empresariales para privar a esa firma de distintos insumos tecnológicos.[6]

[3] Conf. (f) *Definitions*, 3 A.
[4] *"The term "covered foreign country" means the People's Republic of China"* (Sec. 898 (f) Definitions, (2)).
[5] La posibilidad de un mayor acceso a los datos personales de residentes en EUA está asociada a un compromiso para la seguridad nacional en la medida que HUAWEI viene desarrollando la tecnología 5G, que permitirá incrementar drásticamente la velocidad de las conexiones reduciendo la latencia (tiempo de respuesta que tarda un dispositivo para ejecutar la orden desde el momento que es emitida). Estas cualidades permitirán desarrollar el control de actividades por control remoto ("internet de las cosas") y, por extensión, facilitarán el espionaje.
[6] Sin embargo y, atendiendo a la necesidad de proteger a los usuarios de dispositivos producidos por HUAWEI, el 20 de mayo de 2019 el Departamento de Comercio de EUA estableció una licencia temporal, hasta el 19 de agosto del mismo año, a fin de garantizar a HUAWEI el mantenimiento de redes existentes y el acceso a las actualizaciones del software para sus teléfonos móviles en uso. La misma Ley de Autorización de Defensa Nacional de 2019, en la Sección 889 comentada más arriba, contempla expresamente la posibilidad de otorgamiento de un *"waiver"* a las entidades susceptibles de ser sancionadas (Sec. 889, (d)).

DOI: https://doi.org/10.24215/24689912e019

I. ¿POR QUÉ LAS GUERRAS COMERCIALES YA NO PUEDEN DIRIMIRSE SOLO COMERCIALMENTE?

La sanción a la empresa HUAWEI partió de un doble supuesto: la seguridad nacional estaría jaqueada por una intromisión informática destinada a la captación y manipulación de datos, que a su vez podrían ser utilizados por un Estado extranjero (hipótesis de espionaje). Esta última suposición es susceptible de análisis, debate y hasta cuestionamiento jurisdiccional desde el punto de vista de las obligaciones y derechos de los Estados en el marco del sistema político internacional. Así lo interpretó rápidamente la misma empresa HUAWEI, que presentó una demanda por inconstitucionalidad de la Ley de Defensa Nacional de 2019.[7]

Pero dejando a un lado por un momento la hipótesis acerca del espionaje, cabe advertir que un cercenamiento de las actividades comerciales en el sector de las tecnologías de la información y las comunicaciones (TIC), suele poner sobre la palestra una colisión entre dos valores o bienes jurídicos arraigados en la posmodernidad: el derecho al acceso a la información frente al derecho a la protección de los datos personales. Si bien el derecho al acceso a la información era concebido hasta hace pocos años como derecho "individual" y hasta "universal"[8], la mercantilización a gran escala de las TIC convirtió a los datos personales en otra cosa, pues pasaron a ser objetos preciados en tanto susceptibles de capitalización (acumulación y reproducción) por las empresas transnacionales (ETN). Por otro lado, también es conocida la dificultad para deslindar, en el caso del sistema económico e institucional chino, a las empresas públicas de las empresas privadas, hasta el punto que el Sistema de Solución de Diferencias de la OMC ha tropezado con un impedimento insalvable para sancionar al Estado chino por la adopción de subvenciones ilícitas cuando resulten de prácticas propias de empresas estatales pero

[7] En el marco de este litigio, el 28 de mayo de 2019 los letrados presentaron ante una Corte Federal del Distrito Este de Texas una petición para la declaración de inconstitucionalidad de la Ley de Autorización de Defensa Nacional de 2019.

[8] "El objetivo de la universalización del acceso a banda ancha tiene la misma importancia para el desarrollo con igualdad que tuvo el desarrollo de las redes de energía eléctrica, caminos y transporte para el avance de la actividad industrial en el siglo pasado. Es un servicio indispensable que ofrece oportunidades de progreso económico y mayor igualdad y participación. Por ello el acceso a Internet de banda ancha debe considerarse un derecho de los ciudadanos de América Latina y el Caribe" (CEPAL: "Las TIC para el crecimiento y la igualdad, renovando las estrategias de la sociedad de la información", documento editado en noviembre de 2010 (LC/G.2464), p. 109).

DOI: https://doi.org/10.24215/24689912e019

equívocamente presentadas como "no gubernamentales".[9] En este aspecto conviene recordar que ambas cuestiones, esto es, **por un lado la capitalización de bienes intangibles tan asociados a la privacidad como son los datos personales y, por otro lado, la creciente opacidad de la frontera conceptual entre lo público y lo privado, son indicadores de una transformación que parece irreversible dentro de las condiciones de producción prevalecientes a nivel global.**

Ahora bien, la novedad del debate abierto en los medios masivos estriba en un hallazgo: la ineficacia del uso de restricciones comerciales para neutralizar el impacto informático de los equipamientos a través de los cuales las firmas como HUAWEI podrían acopiar, manipular y comercializar datos personales. Como es sabido, el objetivo de las prohibiciones comerciales para el acceso al sistema operativo utilizado por los dispositivos de HUAWEI (ANDROID, sistema operativo desarrollado por GOOGLE), consistiría en inducir un rápido proceso de obsolescencia para dichos dispositivos. En tal sentido, no debería presumirse que la eficacia de tales medidas restrictivas estaría amparada por el rigor del derecho de la propiedad intelectual, en este caso referido al software requerido para la actualización de los sistemas operativos. Contrariamente, se trata de un software conocido como de "código abierto" (*open source*), es decir, dispuesto para recibir aportes enriquecedores de usuarios y programadores, aunque sin la posibilidad de instalar en los mismos dispositivos móviles dichas versiones modificadas. A todo evento, rápidamente se difundieron versiones acerca de los proyectos que tendría HUAWEI para reutilizar los códigos

[9] En el Sistema de Solución de Diferencias de la OMC resultó aleccionador el informe del Órgano de Apelación dentro del caso DS 437 "ESTADOS UNIDOS. Medidas en materia de derechos compensatorios sobre determinados productos procedentes de China". Finalmente no se hizo lugar a los derechos compensatorios aplicados por Estados Unidos contra importaciones originarias de China cuyos insumos habían sido adquiridos en origen mediante condiciones ventajosas a empresas de propiedad estatal. El Órgano de Apelación determinó que los beneficios supuestamente otorgados por el Estado chino debían ser objeto de prueba por el Estado Miembro que los cuestionaba (a la sazón, EUA) en los términos del artículo 14 apartado d) y artículo 1.1.b) del Acuerdo sobre Subvenciones y Medidas Compensatorias. Al efecto, correspondía tomar como referencia los precios que reflejaran las condiciones reinantes en el mercado del país de suministro, más allá de las constataciones acerca de lo que debía ser considerado estrictamente como "gobierno" u "organismo público" en el marco del Acuerdo. Este contundente informe fue adoptado por el Órgano de Solución de Diferencias el 16 de enero de 2015. El tema relativo al carácter "público" de las empresas chinas involucradas, ya había sido materia de análisis en el Grupo Especial, cuando los árbitros, interpretando el sentido que debía asignarse al concepto de "organismo público" en el Acuerdo sobre Subvenciones y Medidas Compensatorias, hicieron hincapié en que "organismo público" no es sinónimo de "empresa de propiedad estatal". El informe de esta primera instancia se había distribuido el 14 de julio de 2014. Las inquietudes despertadas por este tipo de controversia fueron expuestas entonces por Pedro da Motta Veiga: "Los subsidios chinos absueltos" (en portugués), diario O Estado de S. Paulo, sección Economía, 16 de mayo de 2011.

DOI: https://doi.org/10.24215/24689912e019

abiertos de ANDROID y así poder desarrollar una versión alternativa (bifurcada o "*fork*") de ANDROID, para estar en condiciones de seguir actualizando los sistemas operativos y las aplicaciones (*Apps*) demandadas por sus clientes. Más aún, al disponer de un sistema operativo propio y considerando la presencia de HUAWEI en el mercado estadounidense y mundial, esta empresa podría vender el nuevo sistema operativo a otras firmas productoras de teléfonos inteligentes desplazando al proveedor estadounidense de ese mercado y así perseverando en su capacidad de penetración para la captura de datos personales.

Pero las restricciones comerciales unilaterales resultan inoperantes y contraindicadas no solo en virtud de los códigos abiertos en los protocolos que conforman las patentes de invención, sino también porque las retaliaciones chinas podrían ser devastadoras, en atención a que este último país es el mayor productor mundial y abastecedor principal de EUA de materias primas indispensables para la producción de dispositivos e insumos en el rubro de las TIC. Se trata de los minerales y elementos conocidos como "tierras raras" en atención a que difícilmente se presentan en la naturaleza en estado de pureza.[10] No sorprendió entonces que el 29 de mayo de 2019 el gobierno chino hiciera circular informalmente insinuaciones acerca de una posible imposición de nuevas restricciones a dichas exportaciones estratégicas a EUA. De todos modos, esta reticencia china no es novedosa, porque si bien al suscribir el Protocolo de Adhesión a la OMC se había comprometido a no adoptar restricciones a sus exportaciones (salvo contadas excepciones), luego adoptó restricciones para distintas "tierras raras" argumentando que lo hacía con el fin de conservar recursos naturales agotables y reducir la contaminación ambiental generada por la actividad minera, buscando así el amparo normativo del artículo XX apartado g) del GATT. Ello dio lugar a que se incoaran litigios dentro del Sistema de Solución de Diferencias de la OMC, a instancias de EUA, la UE y JAPÓN. Los pronunciamientos del Órgano de Apelación confirmaron lo decidido por el Grupo Especial[11] en el sentido de advertir que la

[10] Estos elementos están presentes en distintos láseres; electrodos de baterías; lentes de cámara; motores eléctricos; condensadores de cerámica; memorias de computadoras; agentes de contraste para equipamiento médico; aditivos; imanes; fibra óptica, etc.
[11] En la reunión del 23 de julio de 2012 el Órgano de Solución de Diferencias estableció un solo Grupo Especial (conforme el Entendimiento sobre Solución de Diferencias, artículo 9 párrafo 1) para dirimir en primera instancia las tres controversias que se habían abierto.

DOI: https://doi.org/10.24215/24689912e019

invocación conservacionista china encubría medidas destinadas a controlar el mercado internacional con respecto a esos mismos recursos naturales.[12]

En conclusión, el intento de EUA para neutralizar a empresas como HUAWEI mediante restricciones comerciales, tendría efectos contraproducentes que al parecer no habían sido debidamente ponderados en un primer momento.

II. ¿COEXISTENCIA DE LAS ETN? EMPRESAS TRANSNACIONALES Y LOS ESTADOS NACIONALES: ¿CAMBIO DE ROLES?

Dentro del panorama indicado, han de comprenderse las políticas empecinadas de los Estados nacionales para poner coto, ya no a las tradicionales estrategias empresariales montadas sobre la propiedad intelectual, sino para enfrentar de algún modo a las estrategias empresariales que, sin respaldos registrales apuntan al acaparamiento y depredación desenfrenada de los mercados.

La experiencia en el caso HUAWEI parece demostrar dos cosas. Ante todo, que por la vía de las restricciones comerciales adoptadas de manera unilateral por los Estados nacionales, difícilmente puedan encauzarse semejantes porfías. Luego, que **urge algún tipo de intervención intergubernamental frente al "derrame" de conocimientos que en sí mismo constituye un potencial capital reproductivo difícilmente mensurable. En tal sentido, ha de advertirse que el desarrollo y control de redes de alta velocidad, además de perforar la intimidad de las personas puede tener directa incidencia política y militar.**

Así, debido al vértigo impreso a dichos procesos de conocimiento y al rebasamiento de los estatutos de la propiedad intelectual, se proyecta un halo de imprevisibilidad y consiguiente indefensión sobre sociedades y economías dependientes de tecnologías que van siendo arrasadas una tras otra y a un ritmo que se insinúa como políticamente incontrolable. He aquí una nueva paradoja en la economía global: la incipiente dilución de los estatutos de la propiedad intelectual puede tener efectos adversos aún más lacerantes que la odiosa monopolización del conocimiento. En este punto, con motivo de la lucha despiadada por la conquista de mercados y que incluye como uno de los rubros más apetecibles la captación y mercantilización de datos personales, reaparecen en escena los Estados nacionales con sus armas tradicionales: las

[12] En los tres litigios, el Órgano de Apelación se expidió el 7 de agosto de 2014. Los casos fueron formalizados a través de los expedientes WT/DS 431 (a instancias de EUA); WT/DS432 (a instancias de la UE); y WT/DS433 (a instancias de Japón).

DOI: https://doi.org/10.24215/24689912e019

restricciones comerciales. En particular, el gobierno de EUA decidió intervenir de manera ruda e improvisada, como lo muestra el caso HUAWEI, no sólo con el objeto de impedir una depredación de su propio mercado sino también aduciendo motivos estratégicos vinculados a la seguridad nacional.

De tal modo, **la voracidad para la apropiación y manipulación de datos personales se manifiesta por un lado como resultado del desarrollo frenético de tecnologías, las que al no poder ser encauzadas por las restricciones de la propiedad intelectual, perforan sin pausa ni límites la intimidad de las personas. Al multiplicarse y desagregarse los datos y las informaciones obtenidas mediante procesos informáticos dotados de creciente velocidad y precisión, pueden realimentarse los dispositivos destinados a exacerbar la dependencia compulsiva de los mismos usuarios y consumidores, cautivos del insaciable deseo que se les continúa inyectando**.[13]

Pero lo cierto es que la intervención unilateral del gobierno de EUA en el caso HUAWEI resultó fallida y, por tal motivo, prontamente el propio Presidente reconoció públicamente que el problema podía encuadrarse bajo un acuerdo intergubernamental EUA-CHINA y que a la sazón ya se estaba negociando.[14]

III. REACOMODAMIENTO DE PIEZAS EN EL TABLERO DE LA CONTIENDA SISTÉMICA

A propósito de la búsqueda de acuerdos intergubernamentales en las TIC, no se puede pasar por alto que en materia de protección de los datos personales está en vigencia un mecanismo extraordinariamente versátil y en el que confluyen Estados nacionales y ETN: el que proporciona reglas (aunque son llamadas "principios") para los datos personales transmitidos desde el territorio de la UNIÓN EUROPEA (UE) al territorio de EUA. Se trata del *"Privacy Shield"* ("escudo de la privacidad" y, en una traducción quizás más ilustrativa si se atiende a la acepción inglesa, "escudo de la intimidad"). Este curioso mecanismo, como algunos otros en el pasado, ha sido el producto del pragmatismo por necesidades compartidas antes que una estrategia pergeñada en círculos áulicos. Surgió debido a las diferencias que hay entre los regímenes de EUA por un lado y la UE por otro lado, a propósito de la protección de

[13] A.L. Fitzsimons: "¿Qué es el "fetichismo de la mercancía"? Un análisis textual de la sección cuarta del capítulo primero de El Capital de Marx", en Economía Crítica número 21, primer semestre, año 2016, pp. 43-58.
[14] La referencia corresponde a una intervención del Presidente Trump y reproducida por la prensa internacional el 23 de mayo de 2019.

DOI: https://doi.org/10.24215/24689912e019

los datos personales. Ellas habían generado un clima de inseguridad jurídica para las ETN que como es obvio no pueden prescindir, en la economía global, de las redes a través de las cuales fluye la información y las comunicaciones. En particular y, debido al mayor rigor en los márgenes de protección previstos por las regulaciones de la UE respecto de las vigentes en EUA, esa inseguridad se acrecentaba con motivo de las transmisiones y manipulación de datos personales que se dirigen desde la UE hacia EUA.[15] Aquí conviene recordar que las diferencias regulatorias vigentes en ambas márgenes del Atlántico últimamente se han agudizado, en virtud de la normativa establecida por la UE: "*The EU General Data Protection Regulation* (GDPR o bien, en español RGPD)".[16]

Atendiendo a que había entrado en *statu-quo* el proceso de convergencia bilateral destinado a formalizar un Acuerdo Transatlántico sobre Comercio e Inversión ("Transatlantic Trade and Investment Partnership", TTIP),[17] la fórmula "*PrivacyShield*" se impuso como necesidad, supuestamente "transitoria" (hasta tanto se perfeccione aquel Acuerdo intergubernamental), para poder así articular los intereses "privados" de las ETN y los cuales están enraizados en la dinámica de la economía global con los intereses "públicos" que, para su propia preservación, no pueden circunscribirse a la

[15] Desde 2000 los flujos transatlánticos de datos habían estado amparados por el régimen "*Safe Harbour*" ("Puerto Seguro"), hasta que la Corte de la UE, en el caso promovido por el ciudadano austríaco Max Schrems contra Facebook ante tribunales irlandeses en 2011, finalmente determinó en 2015 que la Decisión de la Comisión Europea que había consagrado aquel régimen debía reputarse inválida.

[16] Entró en vigencia el 24 de mayo de 2016 pero es de obligatorio cumplimiento a partir del 25 de mayo de 208. Véase: https://www.eugdpr.org. Este ordenamiento prohíbe la transferencia de datos personales fuera de la UE, a menos que el país importador brinde una protección adecuada (similar a la de la UE) sobre la privacidad o bien se cumplan determinadas condiciones relativas al consentimiento requerido. De modo que, como en otras materias, la normativa comunitaria manifiesta una pretensión de extra-territorialidad, que ante todo queda en evidencia por la reivindicación de atribuciones para evaluar a Estados extra-comunitarios según sea su adecuación a un nivel considerado como aceptable en materia de protección de datos personales. En tal sentido, el régimen de la UE contempla dos figuras arquetípicas: (i) el "derecho al olvido", esto es, el derecho de cualquier individuo para obtener la eliminación de toda información digital sobre su persona que le resulte lesivo; y (ii) el derecho a la portabilidad de los datos personales, es decir, el derecho a obtener de una empresa la información completa disponible en esa empresa sobre la persona del solicitante. La protección comunitaria se extiende a la información personal de los residentes en la UE que fuera capturada por empresas en cualquier lugar, tengan o no dichas empresas actividades dentro del territorio comunitario.

[17] Para un seguimiento de dichas negociaciones, que habían alentado interpretaciones optimistas entre 2013 y 2016, véase www.ustr.gov/ttip.

DOI: https://doi.org/10.24215/24689912e019

actividad jurisdiccional destinada a reparar "*ex post"* los daños ocasionados por la difusión indebida de datos personales.[18]

Elaborados con el fin de prevenir y neutralizar la manipulación lesiva de datos personales con motivo de su transmisión desde la UE hacia EUA, los denominados "Principios" (*Principles*) y los Principios Suplementarios ("*Supplemental Principles"*), son en realidad disposiciones a las que deben atenerse las empresas que voluntariamente adhieran (mediante certificaciones renovables anualmente) al *PrivacyShield*. Se trata de una adhesión con efectos vinculantes, porque obliga a las empresas con actividad en EUA, una vez adheridas al régimen, a cumplir sus disposiciones entre las cuales figura la obligación de notificar a los particulares, atender reclamos y atenerse a los laudos arbitrales que resulten de controversias también planteadas por particulares frente al incumplimiento de aquellas mismas disposiciones. Se trata de reglas emitidas por el Departamento de Comercio (*Department of Commerce*), aclarándose en el resumen introductorio *("Overview"*) del *"PrivacyShield Framework"* que dichos Principios fueron desarrollados "en consulta" con la Comisión Europea, la industria y otras partes interesadas *("stakeholders")*. De modo que las más de tres mil empresas adherentes y que componen la nómina (the*"PrivacyShieldList"*), en tanto tales contraen obligaciones simultáneamente con el Estado norteamericano[19] y los particulares, quienes a su vez, más allá de mantener la indemnidad de los derechos personales frente al propio Estado de residencia, pueden dirigir a las empresas directamente sus solicitudes, reclamos y litigar con ellas en foros arbitrales.[20]

Para un botón de muestra sobre los alcances del derecho reconocido a los particulares ante las empresas adheridas, basta con recordar la vigencia de la facultad para impedir, lisa y llanamente, la difusión de informaciones *("optout"*):

[18] El nuevo estatuto resultó de unas tratativas entre autoridades de EUA y la UE que insumieron dos años de labor. En febrero de 2016, urgidos por el vacío dejado por la pérdida de legitimidad del "*SafeHarbour*", los gobiernos anunciaron entonces haber arribado a un acuerdo para instituir el "*Privacy Shield*". A fin de ponderar las dudas y expectativas planteadas en aquel momento, véase el comentario titulado "EU, US Clinch Political Deal in "Safe Harbour" Talks", International Centre for Trade and Sustainable Development (Bridges), volumen 20 number 4, February 4, 2016.

[19] Para las empresas que sean removidas de la nómina debido a sus incumplimientos, las sanciones alcanzan también a la exclusión de beneficios resultantes de previsiones adoptadas por la UE, pues *"*such organizations are no longeren titledtobenefit from the European Commission'sadequacy decision that wouldenablethose organizationstoreceive personal information from the EU*"*

[20] Estas facultades están regladas por el Principio 7 ("Recourse, Enforcement and Liability") y el Principio Suplementario 11 ("Dispute Resolution and Enforcement").

DOI: https://doi.org/10.24215/24689912e019

> *"2.CHOICEa. An organization must offer individuals the opportunity to choose (opt ut) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose (s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice*".[21]

Pero en materia de TIC nunca está dicha la última palabra. Mientras estatutos como *Privacy Shield* procuran un alineamiento al más alto estándar posible de las empresas que en EUA trabajan con información originaria de la UE, las condiciones políticas, económicas y sociales presionan dentro de la propia UE para relajar el nivel de protección. En tal sentido, merecen citarse algunos ejemplos aleccionadores:

(i) A principios de 2019 se difundió un dictamen del abogado general" de la UE – funcionario que presenta sus dictámenes ante el Tribunal de Justicia-, quien consideró que no se debía exigir a la empresa GOOGLE, en su calidad de motor de búsqueda, que borrara, bloqueara o suprimiera ilimitadamente desde el punto de vista geográfico, los vínculos relativos a los datos personales de un usuario. Al respecto, la empresa había pretendido (en principio sin éxito ante la Comisión Nacional de Informática y Libertades de Francia), limitar el bloqueo que se le había solicitado, circunscribiéndolo al ámbito de los vínculos accesibles para su buscador en la UE, procurando de ese modo que la información no pudiera ser accesible desde dispositivos a los que pudieran tener acceso individuos del entorno del sujeto afectado. Siguiendo la misma línea se pronunció el "abogado general", agregando que si se extendiera el borrado a todo el mundo, podría darse lugar a que determinados Estados extra-comunitarios eventualmente pudieran imponer restricciones similares para contenidos de información a los que internautas de la propia UE pretendieran acceder.

(ii) Otro ejemplo significativo sobre la progresiva relajación del rigor normativo adjudicado a la UE para la protección de los datos personales, consiste en circunscribir ese rigor para las actividades "comerciales" y excluir las "políticas", a propósito de la manipulación de datos personales con el propósito de sesgar la propaganda electoral según el perfil de los

[21] Principle number 2. CHOICE. Podría considerarse a esta norma como versión del denominado "derecho al olvido" vigente en la UE.

DOI: https://doi.org/10.24215/24689912e019

destinatarios. Al respecto, el considerando número 56 del Reglamento UE 2016/679 (RGPD) que autoriza a los partidos políticos a utilizar datos personales en actividades de proselitismo electoral *"*siempre que se ofrezcan garantías adecuadas": "Si en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un estado miembro que los partidos políticos recopilen datos personales sobre opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas*"*. El criterio fijado por dicho considerando 56 ha sido puesto a prueba en España, con motivo de la modificación de la Ley Orgánica del Régimen Electoral. Sus fundamentos no pudieron ser más atinados: *"*adecuar el reglamento a las especificidades nacionales y establecer salvaguardas para impedir casos como el que vincula a Cambridge Analytica con el uso ilícito de datos de cincuenta millones de usuarios de Facebook para mercadotecnia electoral*"*. Sin embargo, en la citada modificación fueron borradas las referencias al Considerando 56 y la nueva redacción del artículo 58 bis de la Ley española replantea dudas acerca del cumplimiento de aquellas *"garantías"*. En tal sentido, según la presunción legal, los datos personales quedarían suficientemente protegidos si, en el envío de propaganda por medios electrónicos no se revelara la ideología política del receptor aunque su detección, a través de las páginas web y otras fuentes de acceso público, sea el determinante del contenido personalizado de la misma propaganda.[22]

(iii) Un tercer ejemplo relativo al ablandamiento de las exigencias comunitarias en la materia está impuesto por la necesidad de combatir la delincuencia. Difícilmente pueda objetarse una mayor flexibilidad para la reducción de las actividades delictivas en el territorio comunitario. Pero la novedad es que, ante la consulta prejudicial de la Audiencia Provincial de Tarragona, España, el Tribunal de Justicia de la UE se pronunció el 2 de octubre de 2018 a propósito de la posibilidad de acceder a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas para prevenir, investigar, descubrir y perseguir "delitos" en general y sin necesidad de su calificación como delitos "graves". En su

[22] Véase Olga Guidotti Simon: "Partidos Políticos, Redes sociales, Mercadotecnia Electoral y Privacidad", en Legaltoday, 7 de diciembre de 2018 (www.legaltoday.com/practica-juridica/).

DOI: https://doi.org/10.24215/24689912e019

sentencia, el Tribunal comunitario señaló la legitimidad del relevamiento de datos con la sola condición de no revelar detalles de la "vida privada" de los sujetos investigados.[23] Pero el mismo Tribunal puso de relieve que aquí se trató del simple robo de un teléfono celular y que la tesitura debe ser diferente y corresponde investigar la vida privada de las personas cuando se trate de neutralizar e incluso prevenir la comisión de delitos graves.[24]

En síntesis, los ejemplos expuestos ilustran sobre los efectos adversos que tendría una protección exacerbada de los datos personales, habida cuenta de inconvenientes tales como: posibles retaliaciones que limitarían el acceso a la información; afectación del proselitismo político partidario en esta era cibernética; y desventaja para las fuerzas de seguridad en la lucha contra el delito. De ahí que la hermenéutica y la jurisprudencia europea vayan matizando el rigor regulatorio.

IV. OPCIONES LATINOAMERICANAS

Como es sabido, los países de la región suelen ser "tomadores" y difícilmente "formadores" de los precios de las materias primas que constituyen el grueso de su oferta exportable. Pero también son "tomadores" ya no de precios sino de las tecnologías que requieren para promover el desarrollo y, en particular, de las TIC.

A propósito de las TIC, en América Latina se deben afrontar dificultades parecidas a las observadas en otras regiones, a saber:

a) Las oleadas de innovación tecnológica que van sustituyendo aceleradamente productos, servicios y procesos, tienen un efecto secundario especialmente adverso sobre las economías y las sociedades periféricas. En este sentido, la

[23] Sobre el fondo del asunto, el Tribunal determinó que: *"*esta solicitud no tiene más objeto que el acceso a los números de teléfono correspondientes a las tarjetas SIM así como a los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y, en su caso, la dirección […] Por tanto, los datos a que se refiere la solicitud de acceso controvertida en el litigio principal solo permiten vincular, durante un período determinado, la tarjeta o tarjetas SIM activadas con el teléfono móvil sustraído y los datos personales o de filiación de los titulares de estas tarjetas SIM […] Por tanto, dichos datos no permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados*"* (numerales 59 y 60 del fallo emitido por el Tribunal de Justicia (Gran Sala), en el asunto C-207/16 y publicado por https://curia.europa.eu/jcms/jcms/index.html)

[24] *"*El Tribunal de Justicia ha declarado que, en materia de prevención, investigación, descubrimiento y persecución de delitos, solo la lucha contra la delincuencia grave puede justificar un acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas que, considerados en conjunto, permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos han sido conservados*"* (numeral 54 del fallo citado supra.).

DOI: https://doi.org/10.24215/24689912e019

difusión de dispositivos electrónicos opera como una cabecera de playa para la recopilación y manipulación de datos personales a gran escala y, por lo tanto, como llave maestra para la penetración progresiva de productos y servicios difícilmente asimilables por la población-objetivo de dichas ofertas.[25]

b) A fin de diversificar sus exportaciones al resto del mundo, tanto las ETN con filiales en los países latinoamericanos como las empresas locales grandes, medianas y pequeñas, necesitan acceder a bancos de datos que incluyen los datos personales de potenciales demandantes extra-regionales de distintos productos y servicios. Y a mayor especificidad o selectividad de dicha demanda potencial, se requieren informaciones y datos más voluminosos y desagregados.

Ahora bien, **las informaciones y los datos indispensables para orientar exportaciones latinoamericanas no tradicionales al resto del mundo, son suministrados por las mismas ETN que capturan las informaciones y datos,**

[25] Distintos productos digitales tienen precios cada vez más bajos a la vez que disminuyen los requerimientos de capacitación (alfabetización digital) hasta el punto que hoy día un semi-analfabeto analógico puede utilizar teléfonos inteligentes. Ingresamos entonces en la fase de una globalización que procura ser cada vez más "amigable". Pero inevitablemente los conflictos sociales afloran con motivo del control y la manipulación de las fuentes de goce. El sujeto marginal que aprende a manipular estos artefactos, ya sea para ensimismarse con las imágenes o con la música; o bien cuando los emplea para desempeñar cualquiera de las tareas serviles que le son encomendadas, ¡también está globalizado! En este aspecto, el uso de dichos artefactos en condiciones de pobreza estructural presenta dos rasgos que merecerían especial atención. El primero es el del consumo conspicuo pero con características folklóricas, o sea la emulación del consumo atribuido a los estratos dominantes pero bajo formas esquemáticas y simplificadas. Esta destreza limitada de todos modos resulta suficiente para su aplicación a los quehaceres de supervivencia (esencialmente sólo se trata de recibir instrucciones, informar su cumplimiento y concertar encuentros). El segundo rasgo es el de la imposibilidad de acceder a las ofertas que presentan las pantallas dentro de la realidad cotidiana de quien las recibe. Cada dispositivo empieza a parecerse a un fruto envenenado. El resultado es conocido: la elevación de los estándares de bienestar prometido por las TIC está teniendo un efecto contraproducente en el sentido de profundizar las disparidades económicas y sociales. Ello se aprecia en países periféricos como los latinoamericanos, cuyos mercados se han internacionalizado hasta el punto de someter los hábitos y expectativas de las poblaciones a estándares que sus sistemas económicos y sociales no pueden equiparar desde el punto de vista de las actividades productivas ni sostener desde el punto de vista del consumo. Véase un mayor desarrollo de estas ideas en el trabajo del autor: "Consecuencias del despoblamiento rural y la desorganización social en América Latina", en el libro *Latinoamérica: inserción global e integración regional*, bajo la dirección y edición de Noemí Mellado, editorial Lerner, Córdoba, Argentina, 2016.

DOI: https://doi.org/10.24215/24689912e019

incluyendo datos personales, que realimentan la penetración masiva de productos digitales en la región. Si, como se ha indicado más arriba, los estatutos rigurosos de protección de datos personales adoptados en países desarrollados, como es el caso emblemático de la UE, deben ir flexibilizándose bajo la presión de la dinámica propia de la economía global (*PrivacyShield* e interpretaciones extensivas del RGPD dentro del propio territorio comunitario), ¿qué tipo de solución cabría para las economías y sociedades periféricas?

La cuestión latinoamericana que debería resolverse jurídicamente, consistiría entonces en compatibilizar el objetivo de captar y promover las TIC en el frente interno minimizando sus efectos sociales adversos, con el objetivo externo, esto es, valerse de las TIC para mejorar los términos de la inserción internacional de sus economías. ¿Cómo hacerlo? Las legislaciones nacionales relativas a protección de datos, incluyendo los datos personales, parecen insuficientes en la medida que se trata de una materia inserta en las relaciones económicas internacionales. De modo que, más allá de las disposiciones legales que han ido adoptando los distintos países latinoamericanos unilateralmente y tomando como un modelo de orientación a las disposiciones de la UE, se insinúa una vía que corre paralelamente a ella: la de los tratados de libre comercio de última generación (TLC) con países extra-regionales. Aquí van apareciendo previsiones que insinúan cuál sería el futuro ámbito de concertación internacional en la materia.

Con respecto a los ordenamientos jurídicos internos, en América Latina los constitucionalistas, legisladores y doctrinarios, al abocarse al tema tuvieron y siguen teniendo la sensata preocupación de proteger los datos personales de sus residentes.

Este papel de resguardo está cubierto, en primer lugar por preceptos constitucionales que lo prevén asertivamente y en determinados ordenamientos fijando el recurso jurisdiccional de "*habeas data*".[26] Luego, se presentan disposiciones legales que, al regular distintas materias, ofrecen directa o indirectamente algún marco de protección.

[26] Entre los Estados latinoamericanos cuyas cláusulas constitucionales contemplan el derecho a la protección de datos personales, una investigación realizada en 2012 registró los casos de México, Panamá, Perú y Venezuela, en tanto el recurso de *habeas data* se detectó en disposiciones constitucionales de Bolivia, Panamá, Perú, Colombia, Brasil, Ecuador y Honduras. En tal sentido, véase: Ma. De Lourdes Zamudio Salinas: "El marco normativo latinoamericano y la ley de protección de datos personales del Perú", en Revista Internacional de Protección de Datos Personales, Universidad de Los Andes, Colombia, número 1, julio-diciembre 2012.

DOI: https://doi.org/10.24215/24689912e019

Más específicamente, los países de la región citados a renglón seguido han sancionado leyes de protección de datos personales, que incluyen el establecimiento de organismos de aplicación y procedimientos administrativos con el objeto de asegurar el cumplimiento de sus normas: ARGENTINA; BRASIL; COSTA RICA; MÉXICO; NICARAGUA; PERÚ; REPÚBLICA DOMINICANA; y URUGUAY.[27] Por otro lado, CHILE dispone de una ley alusiva pero cuyas disposiciones han sido consideradas como de carácter programático.[28]

En los TLC celebrados por países latinoamericanos con países extra-regionales, resaltan algunas diferencias metodológicas, pero no tanto en lo que se refiere al contenido de las reglas para la protección de los datos personales, en particular si se comparan los vínculos formalizados por países de la región con dos contra-Partes: la UE y CHINA.

En el caso de los TLC con la UE, aparece una y otra vez la preocupación por evitar que, al invocar la protección de los datos personales, encubiertamente se procure obstaculizar el comercio de servicios. Así surge con claridad al menos en el TLC CENTROAMÉRICA-UE y en el TLC COLOMBIA, PERÚ y ECUADOR-UE.

Con respecto al TLC CENTROAMÉRICA-UE,[29] dentro de la Sección dedicada a los servicios de telecomunicaciones, el artículo 192 relativo a confidencialidad de la información, establece que:

> Cada Parte, de conformidad con su legislación respectiva, asegurará la confidencialidad de las telecomunicaciones y de los datos de tráfico relacionados por medio de una red pública de telecomunicaciones y servicios de telecomunicaciones disponibles al público, sin perjuicio del requisito de que tales

[27] En Argentina, es la Ley 25326 del año 2000, reglamentada por Decreto 1558/2001; en Brasil la Ley General de Protección de Datos entró en vigencia en julio de 2018; en Costa Rica, es la Ley 8969 (2011); en México la Ley Federal de Protección de Datos Personales en posesión de los particulares fue sancionada en 2010 y reglamentada en diciembre de 2011; en Nicaragua se trata de la ley 787 de 2012; En Perú la Ley 29733 data de 2011; en Uruguay la Ley 18331 del año 2008 fue reglamentada por Decreto 414/2009.

[28] Se trata de la Ley 19628 de 1999 sobre protección de la vida privada. De las legislaciones nacionales mencionadas en el texto, dan cuenta el artículo de Ma. De Lourdes Zamudio Salinas indicado más arriba, así como el más reciente de Bojalil, Paulina; Egan, Michael; y Vela-Treviño, Carlos: "Despuntan las reformas en materia de protección de datos en América Latina" publicada el 12 de febrero de 2019 en el sitio web del Banco Interamericano de Desarrollo (BID): https://blogs.iadb.org

[29] El Acuerdo de Asociación Centroamérica-UE es de aplicación provisional: para Costa Rica y El Salvador desde el 1 de octubre de 2013; para Guatemala desde el 1 de diciembre de 2013; y para Honduras, Nicaragua y Panamá desde el 1 de agosto de 2013.

DOI: https://doi.org/10.24215/24689912e019

> medidas no se apliquen de manera que constituyan un medio de discriminación arbitrario o injustificable, o bien una restricción encubierta al comercio de servicios.

La misma tesitura informa el TLC que por ahora vincula a tres de los países de la Comunidad Andina con la UE.[30] Al igual que en el caso anterior, dentro de la Sección de telecomunicaciones, el artículo 149, a propósito de la confidencialidad de la información, dispone: *"*Cada Parte garantizará la confidencialidad de las telecomunicaciones y los datos de tráfico relacionados a través de redes y servicios de telecomunicaciones públicamente disponibles, sin que con ello se restrinja el comercio de servicios*"*. Y en el capítulo sobre Comercio Electrónico, el artículo 164 titulado *"*Protección de datos personales" expresa livianamente: *"*En la medida de lo posible, las Partes procurarán, dentro de sus competencias respectivas, desarrollar o mantener, según sea el caso, la normativa relacionada con la protección de datos personales*"*.

A tenor de semejante normativa, queda en claro que la UE adopta, para sus relaciones comerciales pautadas en estos TLC con países latinoamericanos, un criterio de flexibilidad que, como se sugirió más arriba, se compadece ya no con su legislación interna sino con las imposiciones de la economía global. Pero confrontando estas escuetas y difusas cláusulas de los TLC frente a un régimen exhaustivo como es el *PrivacyShield,* habría que preguntarse si, debido al progresivo incremento y agudización de la conectividad transoceánica, las expresiones contenidas en los TLC con países latinoamericanos no serían inapropiadas y por lo tanto generadoras de conflictos de difícil resolución. En efecto, frases tales como "discriminación arbitraria o injustificable, o […] una restricción encubierta al comercio de servicios*",* o bien *"en la medida de lo posible"* sugieren que para compatibilizar el valor asignado a la protección de los datos con el valor también asignado al acceso a la información, los países latinoamericanos más temprano que tarde necesitarán articular sus economías digitales con los países desarrollados valiéndose de compromisos más

[30] El Acuerdo Comercial entre Colombia, Perú, Ecuador y la UE rige para Colombia desde el 1 de agosto de 2013, para Perú desde el 1 de marzo de 2013 y, en el caso de Ecuador, es de aplicación provisional desde el 1 de enero de 2017. Bolivia, también país miembro de la Comunidad Andina, envió en marzo de 2019 una Comisión a Bruselas para progresar en las tratativas destinadas a suscribir un acuerdo comercial a través del cual, según expuso el canciller boliviano en conferencia de prensa (registrada por www.cancilleria.gob.bo), "Bolivia estaría contribuyendo a que toda la Comunidad Andina cierre un acuerdo definitivo con la Unión Europea, un acuerdo de dos bloques, y ese acuerdo permitirá también fortalecer toda la alianza de la Comunidad Andina con la Unión Europea".

DOI: https://doi.org/10.24215/24689912e019

pormenorizados. Y para ello parecería que ante las notorias asimetrías existentes, la negociación bilateral no sería la más adecuada, sino que debería contarse con un marco de alcance plurilateral o, más aún, multilateral. Y en este aspecto aquel "*Privacy Shield*" podría ser considerado como un antecedente de gran utilidad.

El TLC entre PERÚ y CHINA[31] presenta cláusulas de contenido equivalente pero no exclusivamente alusivas a la economía digital. En el capítulo 13 relativo a *Transparencia*, el artículo 168 dispone que: *"*Nada en este Tratado obligará a una Parte a revelar información confidencial cuyo develamiento pueda impedir el cumplimiento de la ley, o de algún otro modo ser contrario al interés público o perjudicar los intereses comerciales legítimos de cualquier operador económico". Y en el mismo sentido, dentro del capítulo 16 sobre Excepciones, el artículo 195, titulado "Divulgación de Información" señala:

> Nada en este Tratado se interpretará en el sentido de exigir a una de las Partes proporcionar o permitir el acceso a información confidencial, cuya divulgación impediría el cumplimiento de la Constitución, de las leyes o sea de algún otro modo contrario al interés público, o que pueda perjudicar los intereses comerciales legítimos de empresas particulares, públicas o privadas.

Las mismas reservas expuestas por el autor con relación a los TLC de países latinoamericanos frente a la UE pueden reproducirse con motivo de este último TLC que liga las economías de PERÚ y CHINA. En efecto, ¿cuáles serían los *intereses comerciales legítimos* que podrían justificar un acceso a información confidencial? ¿No serían necesarias mayores precisiones? Y, en tal caso, ante la eventualidad de una controversia ¿no convendría para los países de menor desarrollo económico relativo disponer de criterios respaldados multilateralmente?

Por último, se advierte otra variante metodológica en el TLC modernizado que rige para CHILE y CHINA desde el 1 de marzo de 2019.[32] Al incluir un capítulo relativo a Comercio Electrónico, se incluyen en el mismo dos disposiciones específicamente referidas a la protección del consumidor en línea (artículo 54) y a la protección de datos personales en línea (artículo 55):

[31] Este Tratado de Libre Comercio está en vigencia desde el 1 de marzo de 2010.
[32] Se denomina "Protocolo de Modificación del Tratado de Libre Comercio y del Acuerdo Complementario sobre Comercio de Servicios entre el Gobierno de la República de Chile y el Gobierno de la República Popular China". El Tratado, en su versión inicial, regía desde el 1 de octubre de 2006.

DOI: https://doi.org/10.24215/24689912e019

Según el primero de dichos artículos, *"*cada Parte deberá, en la medida de lo posible y de una manera considerada apropiada, adoptar o mantener medidas que otorguen protección a los consumidores que utilicen el comercio electrónico, que sean a lo menos equivalentes a las medidas que otorguen protección a los consumidores de otras formas de comercio*"*. A continuación, el artículo 55 expresa: *"*Reconociendo la importancia de proteger la información personal en el comercio electrónico, cada Parte deberá adoptar o mantener una normativa interna y otras medidas que garanticen la protección de la información personal de los usuarios del comercio electrónico*"*. Estas últimas previsiones no disipan las dudas, empezando por la asignación a cada una de las Partes de las atribuciones regulatorias para preservar la confidencialidad, cuando es notorio que a través del comercio electrónico precisamente los datos e informaciones personales salen a la luz en las dos terminales de la red. Otra vez entonces aflora la necesidad de una convergencia regulatoria. Por lo demás, ambas disposiciones quedan en el marco de las buenas intenciones, porque a tenor del artículo 58, los citados artículos 54 y 55 figuran entre los que no pueden ser invocados por las Partes para recurrir al capítulo X sobre Solución de Controversias.

V. CONCLUSIONES

La embestida política del gobierno estadounidense contra empresas chinas del sector de las TIC, empezando por HUAWEI, se manifestó inicialmente a modo de restricciones comerciales para la explotación del mercado interno, al privar a sus dispositivos electrónicos de los sistemas –de origen norteamericano- indispensables para las actualizaciones y el funcionamiento de aplicaciones complementarias. Dichas medidas fueron expresamente justificadas por la capacidad actual o potencial (imputada inicialmente a HUAWEI pero extensible a otras empresas de origen chino), para la apropiación y consiguiente manipulación de datos, no sólo personales, mediante el control de redes de alta velocidad. Ante la constatación de estas destrezas fue activado el estado de alerta considerando además las vinculaciones de las empresas chinas con el Estado donde se asientan sus matrices. De ahí la invocación a la seguridad nacional.

Semejantes imputaciones tienen un principio de verosimilitud en al menos dos aspectos esenciales. En primer lugar, es evidente que las TIC ofrecen recursos cada vez más sofisticados para inducir y realimentar las preferencias de consumidores y usuarios, valiéndose precisamente del acceso a los datos personales y operando casi

DOI: https://doi.org/10.24215/24689912e019

en tiempo real. De modo que el control y manipulación de dichos datos representa la posibilidad de acumular y reproducir un capital altamente apreciado por las ETN. Este es el primer paso para la captura y aun para el eventual acaparamiento y depredación de mercados. En segundo lugar, resulta notoria la dificultad para deslindar, en el caso del sistema económico e institucional chino, a las empresas públicas de las empresas privadas, hasta el punto que el Sistema de Solución de Diferencias de la OMC ha tropezado con un impedimento insalvable para sancionar al Estado chino por la adopción de subvenciones ilícitas cuando resultan de prácticas propias de empresas estatales pero equívocamente presentadas como “no gubernamentales”.

Sin embargo, las pretendidas restricciones comerciales urdidas por el gobierno de EUA parecen ineficaces y hasta resultarían contraproducentes. En tal sentido, HUAWEI insinuó una estrategia para desarrollar su propio sistema operativo, desplazando así al proveedor estadounidense de ese mercado y en consecuencia renovando la capacidad para capturar datos personales en gran escala. Simultáneamente, el gobierno chino hizo saber que podía impedir las exportaciones de “tierras raras” a EUA, poniendo en riesgo una vez más el desarrollo de la más alta tecnología en atención a que CHINA es el mayor productor mundial y abastecedor principal de EUA de materias primas indispensables para la producción de dispositivos e insumos estratégicos en el rubro de las TIC.

Aquí corresponde abrir un paréntesis y preguntarse por qué pueden replicarse con relativa facilidad los sistemas operativos para productos digitales y, en líneas generales, por qué los estatutos de propiedad intelectual están siendo sobrepasados hasta el punto de haberse desatado un frenético y descontrolado proceso de sustituciones tecnológicas y cuyos efectos adversos alcanzan a las actividades productivas con tecnologías que van siendo desplazadas en esa misma vorágine.

El ejemplo de los “códigos abiertos” en el caso de los sistemas operativos para dispositivos electrónicos, indica que la pérdida del tradicional halo de protección proporcionado por los registros de propiedad intelectual equivale a un precio a pagar para que a través de los procesos creativos e innovadores las ETN puedan perseverar en la conquista y manipulación de los mercados. Esto se explica por la muy acelerada depreciación de las innovaciones, que sólo puede contrarrestarse a través del vértigo cognoscitivo impreso a las actividades de investigación (desde la investigación básica y hasta la investigación industrial). A este ritmo febril se realimentan datos y relaciones

DOI: https://doi.org/10.24215/24689912e019

lógicas encadenadas (algoritmos), que van componiendo sistemas caracterizados como de "inteligencia artificial".

Dentro del panorama indicado, han de comprenderse las políticas empecinadas de los Estados nacionales para poner coto, ya no a las tradicionales estrategias empresariales montadas sobre la propiedad intelectual sino a sus antípodas, esto es, para enfrentar de algún modo a las estrategias empresariales que apuntan al acaparamiento y depredación de los mercados. La experiencia en el caso HUAWEI parece demostrar dos cosas. Ante todo, que por la vía de las restricciones comerciales adoptadas de manera unilateral por los Estados nacionales, difícilmente puedan encauzarse semejantes porfías. Luego, que urge algún tipo de intervención intergubernamental frente al "derrame" de conocimientos que en sí mismo constituye un potencial capital reproductivo difícilmente mensurable y que, además de perforar la intimidad de las personas, puede tener directa incidencia política y militar.

En la búsqueda de acuerdos intergubernamentales para las TIC, no se puede pasar por alto que en materia de protección de los datos personales está en vigencia un mecanismo extraordinariamente versátil y en el que confluyen Estados nacionales y las ETN. Es el *"PrivacyShield"*, un conjunto de reglas ("principios") para los datos personales transmitidos desde el territorio de la UNIÓN EUROPEA (UE) al territorio de EUA. Paralelamente, las condiciones políticas, económicas y sociales, presionan dentro de la propia UE a fin de relajar el nivel de protección y atender con mayor cuidado el papel de las ETN. En tal sentido, a la hora de aplicar las rigurosas disposiciones vigentes para la protección de los datos personales, la jurisprudencia comunitaria toma nota sobre las eventuales retaliaciones que podrían limitar el acceso a la información de sus residentes; los requerimientos del proselitismo político partidario en esta era cibernética; y la necesidad de apoyar a las fuerzas de seguridad en su lucha contra el delito.

En el caso de los países latinoamericanos, resalta la necesidad de compatibilizar el objetivo de captar y promover las TIC en el frente interno minimizando sus efectos sociales adversos, con el objetivo externo, esto es, de valerse de las TIC para mejorar los términos de la inserción internacional de sus economías. ¿Cómo hacerlo? Las legislaciones nacionales relativas a protección de datos, incluyendo los datos personales, parecen insuficientes en la medida que se trata de una materia inserta en las relaciones económicas internacionales. De modo que, más allá de las

DOI: https://doi.org/10.24215/24689912e019

disposiciones legales que han ido adoptando los distintos países latinoamericanos unilateralmente y tomando como un modelo de orientación a las disposiciones de la UE, se insinúa una vía que corre paralelamente a ella: la de los tratados de libre comercio de última generación (TLC) con países extra-regionales. Sin embargo, y después de revisar las tan escuetas como difusas cláusulas contenidas en los TLC de países latinoamericanos con la UE y con CHINA, cabe preguntarse si no llegó la hora de diseñar un sistema jurídico más adecuado para encauzar los flujos de informaciones y datos que conectan a los países de la región entre sí y con el resto del mundo.

Por lo demás, debería tenerse presente que la conectividad global sólo podría perseverar como un recurso estratégico para el desarrollo de la humanidad, si contara con un marco multilateral que, con motivo del tendido de redes y flujos de informaciones y datos, armonizara regulatoriamente los progresos de la ciencia y la tecnología con las demandas por una mayor equidad y mejor calidad de vida por encima de las fronteras nacionales.

BIBLIOGRAFÍA

Estévez, J. (03 de diciembre 2018). Convergencia de las TIC, mejora regulatoria y crecimiento. *Portafolio.* Recuperado de https://www.portafolio.co/opinion/juan-benavides-estevez/convergencia-de-las-tic-mejora-regulatoria-y-crecimiento-524033

Bergel, S. (2014). Investigación científica y patentes: análisis ético-jurídico de sus relaciones. *Revista Bioética*, 22(3), 419. http://dx.doi.org/10.1590/1983-80422014223023.

Bojalil, P., Egan, M. & Vela-Treviño, C. (2019). Despuntan las reformas en materia de protección de datos en América Latina (BID). Recuperado del sitio de Internet de Banco Interamericano de Desarrollo: https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/

Comisión Económica para América Latina (CEPAL). (2010). *Las TIC para el crecimiento y la igualdad: renovando las estrategias de la sociedad de la información* (LC/G.2464). Santiago, Chile: Naciones Unidas. Recuperado de https://www.cepal.org/es/publicaciones/2971-tic-crecimiento-la-igualdad-renovando-estrategias-la-sociedad-la-informacion

Jordan, V., Galperin, H. & Peres, W. (2013). (Coords.). *Banda ancha en América Latina: más allá de la conectividad* (LC/L.3588). Santiago, Chile: Naciones Unidas

Recuperado de: https://www.cepal.org/es/publicaciones/2971-tic-crecimiento-la-igualdad-renovando-estrategias-la-sociedad-la-informacion

da Motta Veiga, P. (16 de mayo de 2011). Os subsidios chineses absolvidos. *Diario O Estado de S. Paulo.* Recuperado de https://acervo.estadao.com.br/pagina/#!/20110516-42944-nac-1-pri-a1-not

Diario Oficial de la Unión Europea (2016). *Reglamento (UE) 2016/679*. Recuperado de: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Executive Order On Securing the Information and Communications Technology and Services Supply Chain. Precidencia de los Estados Unidos de América. 15 de mayo 2019. Recuperada de: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

Fitzsimons, A. (2016) ¿Qué es el "fetichismo de la mercancía"?. Un análisis textual de la Seccion cuarta del capítulo primero de El Capital de Marx. *Revista de Economía Crítica*, (21), 43-58. Recuperado de https://cicpint.org/es/fitzsimons-a-2016b-que-es-el-fetichismo-de-la-mercancia-un-analisis-textual-de-la-seccion-cuarta-del-capitulo-primero-de-el-capital-de-marx-revista-de-economia-critica/

Guidotti Simon, O. (7 de diciembre de 2018) ¿Cuál es finalmente el tratamiento que la nueva Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales (LOPD) da a nuestros datos y las opiniones que dejamos en las redes sociales y cómo nos va a afectar en el futuro? *Legaltoday*. Recuperado de http://www.legaltoday.com/practica-juridica/publico/proteccion_de_datos/cual-es-finalmente-el-tratamiento-que-la-nueva-ley-organica-de-proteccion-de-datos-personales-y-garantia-de-derechos-digitales-lopd-da-a-nuestros-datos-y-las-opiniones-que-dejamos-en-las-redes-sociales-y-como-nos-va-a-afectar-en-el-futuro

Halperin, M. (2016). Consecuencias del despoblamiento rural y la desorganización social en América Latina. En N. Mellado. (Ed.), Latinoamérica: inserción global e integración regional (pp. 35-72) Córdoba, Argentina: Lerner. Recuperado de http://hdl.handle.net/10915/59807

Halperin, M. (2017). Las empresas transnacionales en el escenario latinoamericano del capitalismo tardío. *Aportes para la Integración Latinoamericana*, (36), 001. https://doi.org/10.24215/24689912e001

Huawei Tecnologies USA, INC. & Huawei Tecnologies CO., LTA., vs UNITED STATS OF AMERICA. Case 4:19-cv-00159-ALM. 28 mayo 2019 Recuperado de: https://cdn.vox-cdn.com/uploads/chorus_asset/file/16305867/huawei_motion.pdf

Internacional Centre for Trade and Sustainable Development. (4 February 2016). EU, US Clinch Political Deal in "Safe Harbour" Talks, International Centre for Trade and Sustainable Development. *Bridges Weekly*, *20*(4). Recuperado de https://www.ictsd.org/bridges-news/bridges/issue-archive/eu-us-clinch-political-deal-in-safe-harbour-talks

Ley 115-232 John S. McCain National Defense Authorization Act for Fiscal Year 2019. Congreso de los Estados Unidos. Washington: Estados Unidos. 13 agosto 2018 Recuperado de: https://www.congress.gov/bill/115th-congress/house-bill/5515/text

Metz, C. (30 de noviembre de 2017). Computadoras inspiradas en el diseño del cerebro humano. *Diario La Nación*. 28-29. Recuperado de http://edicionimpresa.lanacion.com.ar/la-nacion/20171130

Nonaka, I. & Takeuchi, H. (1999). Capitulo 3: Teoría de la creación del conocimiento organizacional. En *La organización creadora de conocimiento* (pp. 61-103). DF, México: Oxford University Press.

Organización Mundial de Comercio (1994). Acuerdo General Sobre Aranceles Aduaneros y Comercio. Ginebra: Suiza. Recuperado de: https://www.wto.org/spanish/docs_s/legal_s/gatt47_01_s.htm

Organización Mundial de Comercio (OMC) (2001) *Declaración relativa al acuerdo sobre los ADPIC y la Salud Pública*. Recuperado de: https://www.wto.org/spanish/thewto_s/minist_s/min01_s/mindecl_trips_s.htm

Organización Mundial de Comercio (2001). *Adhesión de la República Popular de China*. (WT/L/432). Recuperado de: https://www.wto.org/spanish/thewto_s/acc_s/completeacc_s.htm#chn

Organización Mundial de Comercio (OMC) (2003) *Aplicación del párrafo 6 de la declaración de Doha relativa al acuerdo sobre los ADPIC y la salud pública*. Recuperado de: https://www.wto.org/spanish/tratop_s/trips_s/implem_para6_s.htm

Organización Mundial de Comercio (2014a). *Informe del Órgano de Apelaciones* (WT/DS437/AB/R). Recuperado de: https://www.wto.org/spanish/tratop_s/dispu_s/cases_s/ds437_s.htm

Organización Mundial de Comercio (2014). *Informe del Grupo Especial* (WT/DS431/ABR; WT/DS432/AB/R; yWT/DS433/AB/R.). Recuperado de: https://www.wto.org/spanish/tratop_s/dispu_s/cases_s/ds431_s.htm

Organización Mundial de Comercio (2014). *Informe del Órgano de Apelaciones* (WT/DS431/ABR; WT/DS432/AB/R; yWT/DS433/AB/R.). Recuperado de: https://www.wto.org/spanish/tratop_s/dispu_s/cases_s/ds431_s.htm

Ortega, A. (30 de septiembre de 2018). Colonialismo digital. *Diario El País*. Recuperado de https://elpais.com/elpais/2018/09/28/opinion/1538132878_521032.html

Polanyi, M. & Sen, A. (2009). The Tacit Dimension. Chicago, USA: The University Chicago Press Books.

Unión Europea (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Sistema de Información de Comercio Exterior (OEA-SICE). (2009). *Tratado de libre comercio Perú-China*. Recuperado de: http://www.sice.oas.org/TPD/PER_CHN/Texts_28042009_s/Index_s.asp

Sistema de Información de Comercio Exterior (OEA-SICE) (2012). *Acuerdo de Asociación Centroamérica-Unión Europea.* Recuperado de: http://www.sice.oas.org/Trade/CACM_EU/Text_Sept14/Index_s.asp

Sistema de Información de Comercio Exterior (OEA-SICE). (2017). Protocolo de Modificación del Tratado de Libre Comercio y del Acuerdo Complementario sobre Comercio de Servicios entre el Gobierno de la República de Chile y el Gobierno de la República Popular China. Recuperado de: http://www.sice.oas.org/Trade/CHL_CHN/CHL_CHN_s/Modernized_2019/CHL_CHN_Amending_Protocol_s.pdf

Tribunal de Justicia de la Unión Europea (Gran Sala) (02 de octubre 2018). *Sentencia ECLI:EU:C:2018:788.* Recuperado de: http://curia.europa.eu/juris/liste.jsf?language=es&td=ALL&num=C-207/16

Tavares de Araujo Jr, J. (Noviembre 2016). Progresso Técnico e Política Industrial: O caso dos paineis de LCD (Breves CINDES 96). Recuperado del sitio de Internet de Centro de Estudos de Integração e Desemvolvimento: http://www.cindesbrasil.org/site/index.php?option=com_jdownloads&Itemid=14&view=viewcategory&catid=4

Zamudio Salinas, M. (Julio-Diciembre 2012). El marco normativo latinoamericano y la ley de protección de datos personales del Perú. *Revista Internacional de Protección de Datos Personales*, (1), 1-21. Recuperado de https://habeasdatacolombia.uniandes.edu.co/?page_id=718

DOI: https://doi.org/10.24215/24689912e019

HALPERIN MARCELO: Abogado, Universidad Nacional de Buenos Aires. Egresado de la Escuela de Sociología. Doctor en Derecho y Ciencias Sociales por la Universidad Nacional de Córdoba, Argentina. Consultor de organismos internacionales de integración y cooperación económica. Investigador y docente del Instituto de Integración Latinoamericana de la Universidad Nacional de La Plata.

Fecha de recepción: 31-05-2019 Fecha de aceptación: 17-06-2019