INFORME *OBSERVATORIO*

INSTITUTO DE INTEGRACIÓN LATINOAMERICANA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

UNIVERSIDAD NACIONAL DE LA PLATA

IIL–FCJS–UNLP

CALLE 10 Nº 1074 – (1900) LA PLATA – REPÚBLICA ARGENTINA

TEL/FAX: 54–0221–421–3202

E–MAIL integra.unlp@gmail.com

www.iil.jursoc.edu.ar

LAS DISPUTAS QUE INVOLUCRAN A LOS ESTADOS NACIONALES Y LAS CORPORACIONES TRANSNACIONALES EN EL SECTOR DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC). IMPACTO SOBRE AMÉRICA LATINA

Marcelo Halperin
Instituto de Integración Latinoamericana de la Universidad Nacional de La Plata

1. Introducción

Es notorio el proceso de aceleración de las fracturas geoeconómicas y geopolíticas que están jaqueando la tan mentada "globalización" de la que hicieron alarde los gobiernos, foros académicos y voceros de corporaciones transnacionales desde fines del siglo pasado y durante las primeras dos décadas del siglo actual[1].

Conviene repasar las manifestaciones contextuales más recientes. Ante un vertiginoso desmadre o desbocamiento de las condiciones de producción y sus efectos sociales adversos, los Estados nacionales ya no pueden controlar dentro de sus propios territorios el desplazamiento hacia la pobreza y la marginalidad de poblaciones cada vez más numerosas, sino a un costo fiscal que tiende a crecer de manera exponencial. Y tampoco pueden contener los aludes migratorios desde países periféricos.

Estos desplazamientos o segregaciones en los sistemas de estratificación social, al interior de las fronteras y a través de ellas, siguen la secuencia del ritmo impuesto por las innovaciones tecnológicas, es decir, los procesos de acumulación y reproducción del capital bajo la matriz productiva impuesta por las corporaciones transnacionales en el sector de la informática y las comunicaciones (TIC).

Como es sabido, la sustitución febril de tecnologías se realimenta por un sucedáneo de la plusvalía que genera ingresos siderales: los datos no remunerados que aportan consumidores y usuarios de contenidos digitales y cuya utilidad va en aumento a medida que son procesados con mayor velocidad y sofisticación, para luego

[1] Las manifestaciones políticas más descarnadas de este proceso de fragmentación han sido vertidas recientemente por la Secretaria de Comercio del Gobierno de Estados Unidos de América. En el curso de 2023, la funcionaria Katherine Tai se expidió reiteradamente al respecto. Una de sus primeras intervenciones fue la que tuvo lugar en el *National Press Club* el 15 de junio y difundida por la Oficina Ejecutiva del Presidente el mismo día: "*Ambassador Katherine Tai´s Remarks at the National Press Club on Supply Chain Resilience*".Véase la nota del autor comentando dicha disertación en: "La nueva política comercial norteamericana", publicada por el sitio web www.tradenews.com.ar el 9 de julio de 2023.

monetizarse y ser reutilizados a fin de condicionar las subsiguientes demandas de los mismos consumidores y usuarios[2].

En este marco el desafío político es doble: por un lado, sostener el ritmo de expansión al que deben seguir contribuyendo los consumidores y usuarios aunque se vayan empobreciendo, lo que demanda mayores recursos del erario público; y, por otro lado, desplegar políticas internacionales predatorias y acaparadoras de mercados ("guerra comercial") para mitigar así el daño producido por la competencia desplegada en el curso de pugnas frenéticas que tienen como finalidad última el sostenimiento de la dinámica de acumulación y reproducción del capital.

Ante todo, cabe advertir que las mencionadas confrontaciones y, en particular, la "guerra comercial" entre los Estados Unidos de América (EUA) y la República Popular China (RPC) tienden, ya no a la destrucción de mercados, sino a su acaparamiento. Así, EUA y RPC pelean por el predominio en los mismos mercados mundiales. Luego, los principales recursos e instrumentos en disputa son los asociados a las TIC debido a que dichas tecnologías condicionan directa e indirectamente los procesos de innovación productiva.

Esta carrera desaforada por la apropiación de mercados no se limita al sector de las TIC. Pero las batallas tienden a concentrarse sobre áreas que directa o indirectamente dependen del desempeño de las corporaciones transnacionales en el sector.

Ello se debe por un lado a la incidencia de sus prestaciones en el comercio y las inversiones internacionales, atravesando las más diversas cadenas de suministro y de valor; y, por otro lado, a la extraordinaria concentración y el frenético ritmo de reproducción del capital reflejado por las oleadas de sustituciones tecnológicas promovidas a partir de sus propias innovaciones.

Es un escenario en el que se destacan las regulaciones adoptadas tanto por EUA, la RPC y la UNIÓN EUROPEA (UE) con el objeto de acotar las actividades de corporaciones transnacionales en el sector de las TIC, aduciendo especialmente motivos de seguridad y para contrarrestar prácticas tanto de evasión y elusión tributaria como de abuso de posiciones dominantes con respecto a las reglas de competencia y al avance sobre los derechos individuales de los usuarios.

[2] Numerosos trabajos abordan las implicaciones históricas de estas prácticas de explotación. Al respecto son ilustrativas las asociaciones de ideas propuestas por Yanis Varoufakis en "Tecnofeudalismo. El sigiloso sucesor del capitalismo", Deusto 2024.

Ahora bien, con respecto a las políticas de los países centrales para controlar y luego poder succionar la cuantiosa rentabilidad de las corporaciones, el análisis debería considerar no sólo las regulaciones sino los procedimientos administrativos y jurisdiccionales a través de los cuales EUA, la RPC y la UE procuran controlar su desempeño.

Esta simultaneidad de perspectivas –la normativa y la casuística- se justifica porque, debido al ritmo de las innovaciones tecnológicas, las normativas más recientes (por ejemplo, acerca de la inteligencia artificial) no sustituyen necesariamente a las precedentes –elaboradas con vistas a tecnologías digitales ya consolidadas- y teniendo presente que los valores o bienes jurídicos a proteger (seguridad o concepto extensivo de la defensa nacional; reglas de competencia y lealtad comercial; responsabilidad fiscal; confidencialidad) son esencialmente los mismos valores que las sucesivas tandas de regulaciones declaran proteger. De ahí que aquí se proponga el estudio de estas cuestiones desde ambas vertientes, esto es, desde las esferas normativas, por un lado; y por otro lado desde las instancias de confrontación o controversia entre los Estados nacionales y las corporaciones transnacionales del sector.

2. Valores o bienes jurídicos protegidos

Aquí emerge una característica de las fracturas geoeconómicas y geopolíticas en curso: el papel central que pasa a ocupar el valor o bien jurídico de la “seguridad”, esto es, la extraordinaria importancia de los recursos para neutralizar amenazas en la lucha por la preservación y acaparamiento de mercados. En tal sentido, la “seguridad” es un valor a considerar no sólo a propósito de las regulaciones directamente referidas a la “defensa” militar. En la medida que los Estados aducen prácticas anticompetitivas y deslealtades comerciales en la operatoria de las TIC, también están sirviendo a los objetivos de “seguridad” porque en un mundo fragmentado la depredación y el acaparamiento de mercados se pueden leer como agresiones a la integridad política o menoscabo de la gobernabilidad[3].

[3] La muy lábil frontera entre la vulneración de secretos comerciales y secretos militares se pone de manifiesto repetidamente. Por ejemplo, el 9 de marzo de 2024 fue noticia de portada la información difundida por la agencia AFP: “Un ingeniero de software chino fue detenido este miércoles por robar tecnología de inteligencia artificial de GOOGLE mientras trabajaba en secreto para dos empresas de China, informó el fiscal general de EUA…” El acusado “se enfrenta a cuatro cargos por robo de secretos comerciales (…)”.

La extraordinaria magnitud que caracteriza a la concentración de capital y control sobre múltiples actividades económicas y comerciales utilizando las redes virtuales mereció una referencia del Fiscal General Adjunto del Departamento de Justicia de EUA cuando el 21 de marzo de 2024 anunció que su gobierno demandaba a APPLE por prácticas monopólicas. Al referirse al universo digital en general, el funcionario habló sobre un enfrentamiento "a los monopolios más grandes y más duros de la historia"[4]. En tal sentido, si bien se suelen difundir datos que cuantifican estas operaciones, quizás todavía no ha sido registrada la verdadera dimensión del problema en los mercados globales.

A su turno, las corporaciones suelen encubrir prácticas anticompetitivas y desleales invocando la protección a la privacidad de los usuarios. Es el caso aducido precisamente por APPLE para su *walled garden*" (o "jardín amurallado") que a través de una combinación de *hardware* y *software* obstaculizaría, al operar sus dispositivos como el iPhone, las filtraciones de información personal que en cambio facilitarían los programas de software de su rival ANDROID (GOOGLE). La réplica de las autoridades, al esgrimir la legislación antimonopólica, es que tratan de justificar así los elevados márgenes de ganancias debidos a la elevación desmesurada del precio de los dispositivos mientras esa misma corporación mantiene acuerdos con otras empresas (como sería la misma GOOGLE), recreando por distintas vías el mismo riesgo de filtraciones no consentidas de datos personales[5].

Y aun tratando de proteger el derecho a la confidencialidad está presente la inquietud por la propia seguridad del Estado cuyos residentes pueden padecer la manipulación informática de sus datos personales. Esta fue la preocupación del gobierno de EUA cuando anunció, el 28 de febrero de 2024, la emisión de una Orden Ejecutiva del Presidente para instruir a distintas reparticiones estatales a fin de introducir regulaciones destinadas a proteger datos personales sensitivos frente a intromisiones eventuales de otros Estados elípticamente calificados como "*countries of concern*". En tal sentido, el documento oficial que anticipó, desde la oficina del Presidente, dicha

[4] Citado en la nota de Michael Liedtke, Lindsay Whitehurst, Mike Balsamo y Frank Bajak: "El Departamento de Justicia demanda a APPLE, alegando que monopolizó ilegalmente al mercado de teléfonos inteligentes", para la agencia AP del 21 de marzo de 2023.
[5] Véase la nota precedente de Michael Liedtke, Lindsay Whitehurst, Mike Balsamo y Frank Bajak: ""El Departamento de Justicia demanda a APPLE, alegando que monopolizó ilegalmente al mercado de teléfonos inteligentes".

Orden Ejecutiva[6], advirtió que el acceso a estos datos personales sensitivos puede estar facilitado por la mediación de empresas:

> "Companies are collecting more of Americans' data than ever before, and it is often legally sold and resold through data brokers. Commercial data brokers and other companies can sell this data to countries of concern, or entities controlled by those countries, and it can land in the hands of foreign intelligence services, militaries, or companies controlled by foreign governments".

Finalmente, para la fijación de responsabilidades fiscales a corporaciones transnacionales que procuran evadirlas buscando el amparo de la "nube", se suma otra vez una cuestión de seguridad nacional atendiendo a la necesidad de los Estados para captar recursos destinados a neutralizar o al menos reducir la segregación o marginación social en un mundo donde prevalece aquel poderoso sucedáneo de la plusvalía en cabeza de las corporaciones transnacionales en el sector de las TIC.

La responsabilidad fiscal cuando se opera en la "nube" es de difícil detección[7]. Por lo demás, una fuente alternativa de recaudación tributaria, en especial para la UE, consiste en la imposición de multas cuantiosas a las corporaciones infractoras. Al establecer y aplicar dichas sanciones, no sólo se considera en cada caso la magnitud del perjuicio ocasionado por la infracción, sino también la envergadura económica de la corporación. Esta dualidad de fundamentos ha sido puesta de manifiesto en repetidas oportunidades y en alguna medida responde a un criterio que permite sortear la dificultad para detectar los hechos imponibles. En tal sentido, un ejemplo, entre muchos otros, puede ser extraído de la exposición de M. Vestager, vicepresidenta ejecutiva de la Comisión Europea que supervisa la política de competencia, cuando al informar sobre una multa impuesta a APPLE por abuso de su posición dominante a

[6] *FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data",* Februrary 28, 2024.
[7] De ahí las expectativas puestas en el proyecto de la OCDE y el G20 "*Base erosion and profit shifting*" (BEPS) que desde 2015 diseña procedimientos para facilitar la recaudación tributaria sobre las actividades de corporaciones que al operar con activos intangibles como son los servicios digitales y aplicarlos mediante transacciones transfronterizas, se encuentran en condiciones de eludir sus obligaciones tributarias mediante distintas maniobras de ocultamiento y re-localización contable. Véase el trabajo de Noemí B. Mellado: "Tecnologías digitales e interrogantes en materia tributaria" publicado por la Revista Aportes para la Integración Latinoamericana, Año XXIX número 48, junio 2023.

través de la AppStore, dijo que la cantidad de la multa "*refleja tanto el poder financiero de APPLE como el daño que su conducta infligió a millones de usuarios europeos*"[8].

En consecuencia, a la hora de apreciar tanto las regulaciones como los pronunciamientos administrativos y jurisdiccionales habrá que considerar la superposición de los distintos valores o bienes jurídicos afectados.

La profusión de regulaciones y procedimientos administrativos y jurisdiccionales emprendidos por los Estados de países desarrollados frente a las corporaciones transnacionales que operan las TIC contrasta con la pasividad de muchos Estados periféricos. Precisamente las sociedades de países catalogados como "en desarrollo" están sujetas a los estímulos compulsivos de la economía digital tanto como las sociedades de los países centrales. Pero en líneas generales su vulnerabilidad es mayor, debido a las condiciones de vida que prevalecen en ellas y la consiguiente proclividad para captar contenidos virtuales bajo la forma de ofertas o promesas engañosas. De ahí que resulte indispensable apreciar las políticas regulatorias y los procedimientos que están llevando a cabo EUA, la RPC y la UE para esbozar posibles líneas de acción de los Estados de países en desarrollo para que se compatibilicen y complementen con ellas.

3. Las TIC como herramienta de dominación: competencia, poder y seducción masiva[9]

Acerca de los criterios y las reglas para regular la competencia comercial, el advenimiento de las TIC marcó un quiebre conceptual, si bien estuvo anticipado por el papel reconocido a los proveedores de telecomunicaciones básicas desde los últimos años del siglo XX. Tanto las disposiciones nacionales como los acuerdos intergubernamentales (y en especial los tratados de libre comercio de última generación en sus capítulos relativos a las telecomunicaciones), ya habían dado por

[8] Nota de Tripp Mickle y Adam Satariano: "La UE multa a APPLE por usar la AppStore para obstaculizar a la competencia", en The New York Times, 4 de marzo de 2024. Se trata de un criterio ya establecido por las regulaciones de la UE. Por ejemplo, el Reglamento de Inteligencia Artificial establecido por Resolución legislativa del Parlamento Europeo del 13 de marzo de 2024 (catalogado P9_TA (2024) O 138) al fijar las sanciones a empresas (capitulo XII) aplica porcentuales sobre el volumen de negocios "mundial total", cuando fueran superiores a los montos predeterminados por las respectivas disposiciones. En los considerandos del Reglamento, el numeral 168 enumera los criterios a tener en cuenta por los Estados miembros para imponer la cuantía de las sanciones y, entre ellos, destaca la naturaleza, gravedad y duración de la infracción y sus consecuencias y, concordantemente, "el tamaño del proveedor".

[9] Este apartado reproduce y sintetiza lo expuesto por el autor en: "La ciudadanía digital en el cielo latinoamericano", publicado en Informe Integrar, Instituto de Integración Latinoamericana de la Universidad Nacional de La Plata número 124, octubre 2020.

sentada la necesidad de hacer una importante salvedad sobre los preceptos sobre la defensa comercial frente a los proveedores de telecomunicaciones "básicas". Hubo que reconocerles posiciones dominantes[10] pero a cambio de exigirles un trato no discriminatorio y de facilitación para las actividades desplegadas por otros proveedores, incluyendo a empresas oferentes de "contenidos" o "de valor añadido".[11] Pero en un corto período estos últimos oferentes han ido acaparando la cadena en sus distintos eslabones, apropiándose de márgenes crecientes de participación en los negocios relativos a infraestructura, redes y aún el diseño y producción de dispositivos. Así, por ejemplo, en 2019 algunas de las más destacadas corporaciones (BIG-TECH) como Microsoft, Google, Facebook y Amazon habían pasado a controlar bajo distintas figuras jurídicas una parte sustancial de la infraestructura submarina de fibra óptica, en tanto Alphabet (Google) y Microsoft venían invirtiendo en la rama de los equipos de

[10] En los TLC celebrados por países latinoamericanos entre sí y con terceros países, son muy frecuentemente incorporadas dentro del capítulo sobre servicios públicos de telecomunicaciones, distintas obligaciones específicamente destinadas a proveedores "monopólicos", "dominantes" o "importantes". Debe tenerse en cuenta que aquí "dominante" o "importante" suelen utilizarse como adjetivos equivalentes. Se reconoce dicha sinonimia y se califica como: "*proveedor dominante o importante* (…) (al que) *tiene la capacidad de afectar de manera importante las condiciones de participación, desde el punto de vista de los precios y del suministro en el mercado relevante de redes o servicios públicos de telecomunicaciones, como resultado de: (a) el control de los elementos esenciales, o (b) el uso de su posición en el mercado"*. En este marco, las medidas que se reservan las Partes en el marco de los TLC a fin de contrarrestar las prácticas abusivas son usualmente denominadas "salvaguardias competitivas".
Entre los TLC con las características indicadas pueden mencionarse, entre otros: CENTROAMÉRICA-PANAMÁ (artículo 13); CENTROAMÉRICA-UE (artículos 185 y 188); CENTROAMÉRICA-CHILE (artículos 13.02 y 13.07); CENTROAMÉRICA-MÉXICO (artículos 13.1 y 13.5); COLOMBIA-MÉXICO (artículo 11.07); COLOMBIA-EUA (artículo 14.4); CHILE-EUA (artículo 13.4); CHILE-COREA DEL SUR (artículo 12.6); CHILE-MÉXICO (artículos 12.01 y 12.06); CHILE-AUSTRALIA (capítulo 11 sección C); MÉXICO-PANAMÁ (artículos 12.1 y 12.5); MÉXICO-URUGUAY (artículo 11.06); PANAMÁ-EUA (artículos 13.4 y 13.17); PERÚ-EUA (artículos 14.4 y 14.17); PERÚ-JAPÓN (artículos 117 y 120); PERÚ-CANADÁ (artículos 1003 y 1014). En el Acuerdo ARGENTINA-CHILE, los términos de la definición son similares a los anteriores con una sutil diferencia: la capacidad de afectar las condiciones de participación en un mercado dado de telecomunicaciones aquí se asigna ya no al control de "*instalaciones esenciales*" sino de "*facilidades* esenciales" (artículo 10.1). De tal modo, queda establecida la posibilidad de reconocerle carácter dominante a una empresa proveedora de servicios de telecomunicaciones aunque no tenga estrictamente un control de las instalaciones siempre que pueda disponer de ellas.

[11] Las negociaciones multilaterales sobre telecomunicaciones básicas condujeron a la suscripción del Cuarto Protocolo anexo al Acuerdo General sobre el Comercio de Servicios que entró en vigencia en 1998 incorporando listas de concesiones otorgadas por todos los países industrializados y más de cuarenta países en desarrollo. En muchos casos, la imprecisión conceptual sobre el alcance del trato nacional se acrecentó por las ulteriores transformaciones tecnológicas aplicadas al sector, hasta devenir anacrónicas dichas concesiones y justificar la proliferación de compromisos bilaterales y plurilaterales dentro de los capítulos sobre telecomunicaciones incorporados en los tratados de libre comercio de última generación. Véase: "Negociaciones sobre telecomunicaciones básicas posteriores a la Ronda Uruguay" en http://wto.org

telecomunicaciones[12]. La integración pasó a ser también horizontal dentro de las TIC[13]. Y empezó a sobrepasar el horizonte inicial de las TIC, a partir de las ventajas competitivas obtenidas por la captura de datos estratégicos sobre productos y servicios que son objeto de transacciones a través de las plataformas[14]. Por lo demás, al estar dirigidas al público en general y ya mimetizadas con las telecomunicaciones básicas, estas empresas han inducido a los gobiernos a equipararlas, total o parcialmente, con las empresas de telecomunicaciones prestatarias de "servicio público".

El desempeño de posiciones dominantes en los mercados tiene un componente adicional para el sector de las TIC, en especial si se pone de relieve el desempeño de las BIG-TECH. Se trata de su capacidad para el condicionamiento del poder político. En efecto, desde el punto de vista de los Estados nacionales, los conflictos con las BIG-TECH no se reducen a los temas más conocidos y que de todos modos están lejos de haber sido resueltos: la elusión tributaria, la vulneración de derechos de propiedad intelectual y la manipulación de datos personales**.** Regular y controlar a empresas proveedoras de servicios de telecomunicaciones básicas es una cosa. Regular y controlar a empresas que han acaparado el mercado mundial de los contenidos es otra. Para difundir sus mensajes y así propagar la narrativa que sostiene su autoridad, los gobiernos deben recurrir a los mismos sistemas de comunicación que hipotéticamente son objeto de su regulación y control, aunque al intentarlo quedan entrampados y expuestos por la horizontalidad de los formatos interactivos.

Finalmente, la superación de las barreras convencionales de la competencia comercial y el condicionamiento al poder político se asientan sobre una capacidad de seducción sin precedentes. Debido al desarrollo tecnológico aplicado a la manipulación de los dispositivos, el aprendizaje requerido a los usuarios resulta cada vez más sencillo. Una vez adquiridos los rudimentos, tal como sucede con el manejo de otros dispositivos en la vida cotidiana, el saber se incorpora y en este sentido hasta puede ser asimilado a las reacciones inconscientes o primarias envueltas en la noción de "saber" utilizada

[12] Información recolectada por el documento de UNCTAD: "Informe sobre la economía digital 2019. Creación y captura de valor: repercusión para los países en desarrollo", página XV.
[13] Véase un inventario de diversificaciones productivas de las BIG-TECH en Josué G. Veiga: "Laboratorio de Estudios sobre Empresas Transnacionales. BIGTECH el gran ganador de la pandemia" en www.clacso.org, junio 2020.
[14] Es uno de los principales argumentos invocados por el informe de un Comité de la Cámara de Representantes de EUA publicado el 6 de octubre de 2020 para catalogar a las cuatro BIG-TECH descritas en conjunto por la sigla GAFA (Google, Apple, Facebook y Amazon) como monopólicas y abusadoras de su posición dominante.

por Lacan para distinguirla del "conocimiento" racional o consciente[15]. Así, cabría especular acerca de la poderosa incidencia de las comunicaciones electrónicas sobre el inconsciente a través de una encarnadura del "Otro" en los dispositivos por los cuales uno puede leerse o escucharse, pues: *"…es la imagen del Otro la que define el interior, el sentimiento del interior, el sentimiento de la intimidad. No hay forma de situar este adentro más que por el dominio que el sujeto experimenta a partir de la imagen del Otro*"[16].

Por lo demás, las comunicaciones electrónicas forman parte del habla y en tal sentido J. Lacan marcó "*la escisión que se produce entre el sujeto como pregunta, el sujeto supuesto no saber y el Otro que habla y es el sujeto supuesto saber*"[17]. Al respecto, la agencia de noticias AP recogió una expresión atribuida a Patrick Wardle, experto en seguridad informática y ex investigador de la Agencia de Seguridad Nacional de EUA: "*I always think of phones as like our digital soul*" ("siempre pienso en los teléfonos como nuestra alma digital"). Como es sabido, estos procesos mentales son sistemáticamente inducidos desde las BIG-TECH para modelar y luego captar el consumo masivo, en tanto se libran en otros planos furiosas batalla en aras del control de redes de la más alta velocidad posible con objetivos políticos y militares[18].

4. Regulaciones de EUA, la RPC y la UE destinadas a controlar los mercados digitales

4.1. Antecedentes cercanos: la influencia del régimen sobre protección de los datos personales en la UE

En su momento mereció particular atención la iniciativa de la UE que se canalizó a través del Reglamento General sobre la Protección de Datos (RGPD) o *"General Data Protection Regulation" (GDPR)* vigente desde mayo de 2016[19]. Entre otras previsiones prohibió la transferencia de datos personales fuera de la UE, a menos que el país

[15] Véase: Jacques Lacan: "El Seminario de Jacques Lacan Libro 17 El Reverso del Psicoanálisis", texto establecido por Jacques-Alain Miller, ediciones Paidós, Buenos Aires-Barcelona-México 1992, página 41 y ss.
[16] Jacques-Alain Miller: "Extimidad", Paidós, Buenos Aires 2010 página 31.
[17] Jacques-Alain Miller: "Extimidad" citado, página 443.
[18] Véase, del autor: "Datos personales: seguridad nacional y concertación internacional. La disyuntiva latinoamericana", revista Aportes para la Integración Latinoamericana año XXV número 40, junio 2019.
[19] Es el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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. Debe distinguirse del Reglamento UE 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.

importador brindara una protección adecuada de la privacidad o bien se cumplieran determinadas condiciones para recabar el consentimiento de los usuarios. E influyó en la legislación de la RPC, una de cuyas principales fuentes normativas sobre protección de datos es la Ley de Protección de Información Personal vigente desde noviembre de 2021. Esta última, que presenta semejanzas con la GDPR de la UE, se complementa con la Ley de Seguridad de Datos vigente desde el 1 de septiembre de 2021 y una precedente Ley de ciber-seguridad que rige desde el 7 de noviembre de 2016[20].

Conviene no perder de vista que, bajo las actuales circunstancias, en RPC la protección de los datos personales está enlazada fuertemente con la seguridad nacional y, en especial, con el régimen legal sobre secretos de Estado. En tal sentido, el 27 de febrero de 2024 fue aprobada una enmienda a la ley de secretos de Estado incluyendo previsiones sobre secretos laborales o adquiridos en el trabajo. Estos "secretos", si bien inicialmente no constituyen secretos de Estado, podrán ser considerados potencialmente lesivos para la seguridad nacional en caso de producirse determinadas filtraciones de información[21].

El GDPR también inspiró la legislación brasileña, pues la Ley General de Protección de Datos de Brasil, de julio de 2018, refleja muchas de sus disposiciones[22].

4.2. Disciplinas recientes de la UE dirigidas al sector digital

Rigen desde 2022: el "Reglamento del Parlamento y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales)[23] individualizado en inglés como "DMA"; y el "Reglamento 2022/2065 del Parlamento Europeo y del Consejo del 19 de octubre de 2022 relativo a un mercado único de

[20] Puede accederse a versiones no oficiales de las referidas disposiciones del gobierno de la RPC en los siguientes sitios: https://www.chinalawtranslate.com/en/Personal-Information-Protection-Law/; https://www.chinalawtranslate.com/en/datasecuritylaw/; y https://www.chinalawtranslate.com/en/2016-cybersecurity-law/

[21] Véase la nota de Daisuke Wakabayashi, Keith Bradsher y Claire Fu titulada "China amplía el alcance de la ley de secretos de Estado" en The New York Times del 28 de febrero de 2024. Las autoras recuerdan que la ley de referencia ya se había modificado en 2010 cuando la RPC impuso requisitos estrictos para las empresas de telecomunicaciones e Internet a fin de facilitar su cooperación con las autoridades en caso de detectarse filtraciones de secretos de Estado.

[22] Paulina Bojalil, Michael Egan y Carlos Vela-Treviño: "Despuntan las reformas en materia de protección de datos en América Latina", publicado en el sitio web del Banco Interamericano de Desarrollo https://blogs.iadb.org el 12 de febrero de 2019. Véase también: Christian Perrone and Sabrina Strassburger: "Privacy and Data Protection. From Europe to Brazil", Panor.Braz.law, Year 6 Numbers 9 and 10, 2018.

[23] En inglés: "*Regulation 2022/1925 of the European Parliament and of the Council of 14 september 2022 on contestable and fair markets in the digital sector*". Rige desde el 1 de noviembre de 2022 y devino aplicable el 2 de mayo de 2023.

servicios digitales y por el que se modifica la Directiva 2000/31/CE ("Reglamento de Servicios Digitales") individualizado en inglés como "DSA" o "SMA"[24].

El Reglamento en materia de Mercados Digitales (DMA) procura contrarrestar prácticas monopólicas identificando a los "guardianes" ("*gatekeepers*") de acceso, es decir, a las grandes plataformas digitales que ofrecen los servicios de plataforma central (motores de búsqueda en línea; tiendas de aplicaciones; servicios de mensajería). En tal sentido el 6 de septiembre de 2023 la Comisión Europea individualizó a seis "guardianes" como responsables para el cumplimiento de sus disciplinas: ALPHABET, AMAZON, APPLE, Byte Dance, META y MICROSOFT. Asimismo individualizó a veintidós "*core platform services*" provistos por dichos guardianes.

La entrada en vigencia del DMA en marzo de 2024 marca el fin de una etapa y el comienzo de otra, quizás tan o más problemática que la anterior. Por ejemplo, se impone la obligación de "abrir" el iPhone de APPLE a tiendas de aplicaciones competidoras, en lugar de requerir el uso de sus propias aplicaciones para las ventas de servicios ofrecidos por empresas competidoras y percibir comisiones por esta intermediación. Pero APPLE se anticipó a la reforma ofreciendo alternativas basadas en una interpretación extensiva de la norma que otras empresas –como SPOTIFY- ya rechazaron por abusiva[25].

Con respecto al Reglamento sobre Servicios Digitales (DSA), si se pudieran resumir sus objetivos habría que hacer referencia a las normas sobre los servicios de intermediación en línea y que están destinadas a neutralizar los contenidos ilegales, la desinformación y la publicidad engañosa.

Sobre la base de las previsiones del DSA, en diciembre de 2023 la Comisión Europea inició un primer procedimiento informal, en este caso para investigar los sistemas y políticas de la plataforma en línea "X" a fin de determinar si se presentaban

[24] La "Digital Service Act" rige desde el 16 de noviembre de 2022. Las normas del Reglamento se aplican a todo tipo de plataformas a partir del 17 de febrero de 2024.
[25] Días antes de la puesta en vigor del DMA, APPLE fue multada con mil ochocientos millones de euros por la entidad reguladora de la competencia de la UE, por obstaculizar la competencia entre empresas rivales de *streaming*, culminando una investigación de cinco años puesta en marcha por SPOTIFY. Ésta y otras disputas anteriores fueron motivadas por la exigencia de APPLE para utilizar su servicio de pago dentro de la propia aplicación para las compras a terceras empresas (en el caso, servicio de música en emisión continua) y así percibir comisiones excesivas. Véase la nota de Tripp Mickle y Adam Satariano: "La UE multa a APPLE por usar la AppStore para obstaculizar la competencia" en The New York Times del 4 de marzo de 2024.

infracciones al Reglamento. Entre otras cuestiones, habían aflorado preocupaciones por difusión de informaciones aparentemente falsas, presuntas desinformaciones y contenido terrorista (discurso del odio) en relación a la guerra entre el Estado de Israel y la agrupación Hamas. Bajo la mira de la Comisión se incluyó el análisis de los servicios de suscripción, la transparencia y una eventual manipulación informativa[26].

Una segunda intervención de la Comisión Europea pero ahora como primera apertura formal de investigaciones, quedó establecida el 19 de febrero de 2024 cuando se realizó la apertura del procedimiento contra la plataforma TIK TOK. Se fijaron los siguientes objetivos: (i) focalizar el análisis sobre los posibles efectos negativos del diseño del sistema informático en la medida que pudieran estimular comportamientos adictivos y crear el hábito llamado "de la madriguera del conejo" ("*rabbit hole effects*") que consiste en repetir búsquedas afines a las precedentes para conformar un perfil de usuario susceptible de manipulación; (ii) sobre la base del análisis indicado, advertir si se afectan derechos de la minoridad al facilitarse el acceso a contenidos inapropiados; (iii) luego, apreciar el posible impacto sobre la realimentación de procesos de radicalización ideológica; y (iv) comprobar si se cumplen los recaudos para la transparencia de los mensajes publicitarios[27].

4.3. Iniciativa reciente de EUA dirigida al sector digital

En EUA la normativa por el momento parece orientada por la casuística y de manera errática si se compara con la UE. Por ejemplo, a fines de abril de 2024 el Senado en acuerdo con la Cámara de Representantes modificó el proyecto de ésta última y sancionó una ley que extendió a nueve meses (originalmente era de seis meses) con un plazo de gracia de tres meses más, el plazo impuesto a la firma propietaria de Tik-Tok, cuya matriz se encuentra en RPC (*ByteDance*) para la venta de sus activos (des-invertir) a una entidad que satisfaga al gobierno de EUA. En caso de no efectuarse dicha transferencia, pasarían a la ilegalidad la distribución y actualización de esa aplicación en EUA por parte de las tiendas de aplicaciones y las empresas de almacenamiento en la web. Según uno de los principales argumentos esgrimidos por los especialistas norteamericanos Tik-Tok estaría captando datos personales de

[26] Kelvin Chan/AP: "EUROPEAN UNION investigating Musk´s X over possible breaches of social media law", The Washington Post, December 18, 2023.
[27] "Commission Opens Formal Proceedings Against TikTok under the Digital Services Act", Press Release, 19 February 2024. Véase la nota de Liz Alderman: "La UE investigará a TikTok por su diseño adictivo", en The New York Times, 20 de febrero de 2024.

quienes ingresan al sitio, que no serían necesarios para su operatoria. De ahí la sospecha sobre su potencial utilización por los servicios de inteligencia de RPC.

Sin embargo, el temor de una eventual captura de dichos datos por los servicios de inteligencia de RPC no había sido todavía respaldado por sospechas verosímiles, dando lugar a quejas como las del mismo Canciller de la RPC. En tales circunstancias, el candidato opositor a la presidencia, D. Trump, se expidió prontamente sobre la cuestión, indicando que el vetaría la norma, si llegara a convertirse en Ley, por dos motivos: porque podría tener un efecto negativo sobre los jóvenes norteamericanos adictos a ese sitio web; y porque las sanciones favorecerían indirectamente a su competidora FACEBOOK propiciando la consolidación de la posición dominante de esta última[28].

4.4. Regulaciones de EUA y la UE destinadas específicamente al área de la inteligencia artificial

En el caso de EUA, el Presidente dictó una Orden Ejecutiva en octubre de 2023 entre cuyos objetivos figura una imposición para compartir con autoridades gubernamentales, bajo las previsiones de la Ley de Producción de Defensa, las pruebas de seguridad de nuevos modelos de inteligencia artificial que supongan riesgos para la seguridad nacional.

Mucho más ambiciosa está resultando la acción de la UE, en cuyo ámbito se debatió extensa y pormenorizadamente una normativa que aborda por primera vez de manera sistemática los riesgos que conlleva la IA. El resultado es la introducción de un orden disciplinario novedoso aunque de difícil instrumentación teniendo en cuenta el carácter vertiginoso de las transformaciones tecnológicas. De ahí las alertas pero también el enfoque prudente de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se “establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión”. El Reglamento, cuya Propuesta inicial se publicara el 21 de abril de 2021, fue formalizado por el Parlamento el 14 de junio de 2023 abriéndose la instancia de negociación con los Estados Miembros. El 8 de diciembre de 2023 se dio un paso adelante al celebrarse un “acuerdo político” a la espera de la ratificación por el

[28] Curiosamente, ByteDance dejó trascender por distintos medios que el sesenta por ciento de su patrimonio sería propiedad de los fondos de inversión Susquehanna International Group y BlackRock, lo que impediría que el gobierno de RPC pudiera ejercer presión sobre ella para la captación de su acervo informativo. Véase la nota de Tom Gerken y Tom Singleton: “Tik Tok vows to fight unconstitutional US ban” publicada por la BBC el 26 de abril de 2024.

Parlamento y el Consejo de la UE. Finalmente, el Reglamento de Inteligencia Artificial fue sancionado como Resolución legislativa del Parlamento Europeo el 13 de marzo de 2024[29].

Para llegar a la firma de dicho acuerdo, se zanjaron algunas discrepancias sensibles, para llegar a convenir:

(i) la prohibición de cámaras de reconocimiento facial en espacios públicos[30], salvo casos excepcionales para los cuales se requerirá autorización judicial; y

(ii) la regulación de los modelos fundacionales de inteligencia artificial, sistemas en los que se basan programas como ChatGPT de la empresa OpenAI y Bard de GOOGLE[31]. Los problemas de seguridad en los modelos surgen especialmente con motivo de los llamados "modelos de IA de uso general con riesgo sistémico"[32].

Una vez convalidado por el Consejo, el Reglamento regiría desde 2026. Más precisamente: luego de ser publicado en el Diario Oficial, entrará en aplicación veinticuatro meses después. De todos modos, las distintas disposiciones tienen prevista su vigencia con posterioridad a dicha fecha[33].

Para empezar:

> "*Resulta necesario definir con claridad el concepto de sistema de IA en el presente Reglamento y armonizarlo estrechamente con los trabajos de las*

[29] Este es el texto pertinente a efectos del EEE. Fue catalogado: P9_TA (2024) O 138.
[30] Entre los sistemas de IA expresamente prohibidos se incluyen aquellos dirigidos a la identificación biométrica remota en tiempo real (véase al respecto el considerando 32); en tanto los sistemas de identificación biométrica remota deben clasificarse, en general, como de alto riesgo (conforme argumentos del considerando 54).
[31] "Aunque los modelos de IA son componentes esenciales de los sistemas de IA, no constituyen por sí mismos sistemas de IA. Los modelos de IA requieren que se les añadan otros componentes, como por ejemplo una interfaz de usuario, para convertirse en sistemas de IA (…) Debe entenderse que las obligaciones de los proveedores de modelos de IA de uso general deben aplicare una vez que los modelos de IA de uso general se introduzcan en el mercado…" (Reglamento de IA citado, considerando 97).
[32] La significación del "riesgo sistémico" puede inferirse por los ejemplos mencionados en el considerando 110 del Reglamento de IA citado, tal como el del "riesgo de que un acontecimiento concreto de lugar a una reacción en cadena con efectos negativos considerables que podrían afectar incluso a una ciudad entera, un ámbito de actividad entero o una comunidad entera".
[33] En tal sentido: la prohibición de determinadas prácticas luego de seis meses; los códigos de buenas prácticas luego de nueve meses; las normas sobre IA de uso general luego de doce meses; y las obligaciones para los sistemas de alto riesgo luego de treinta y seis meses (véanse las Disposiciones finales en el Reglamento citado, capítulo XIII y el considerando 179)

> *organizaciones internacionales que se ocupan de la IA, a fin de garantizar la seguridad jurídica y facilitar la convergencia a escala internacional y a una amplia aceptación, al mismo tiempo que se prevé la flexibilidad necesaria para dar cabida a los rápidos avances tecnológicos en este ámbito (…) Una característica principal de los sistemas de IA es su capacidad de inferencia. Esta capacidad de inferencia se refiere al proceso de obtención de información de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos y virtuales, y a la capacidad de los sistemas de IA para deducir modelos o algoritmos a partir de la información de entrada a datos (…) La capacidad de inferencia de un sistema de IA trasciende el tratamiento básico de datos y permite el aprendizaje, el razonamiento o la modelización. El término "basado en una máquina" se refiere al hecho de que los sistemas de IA se ejecutan en máquinas (…)*"[34].

La caracterización mencionada deriva en una ímproba tarea de caracterización de riesgos. Al calificar a los sistemas de IA atendiendo a niveles de riesgo y contemplando variadas hipótesis de excepción y de transitoriedad, este Reglamento se presenta como ensayo germinal de una futura normativa multilateral o plurilateral en la materia. El valor del modelo normativo radica entonces en su metodología, pues introduce categorías aptas para encasillar –y des-encasillar- distintos tipos de contenidos según la envergadura de los daños que pudieran ocasionar.

Para describir la metodología puede resultar útil recurrir a la Exposición de Motivos difundida en Bruselas el 21 de abril de 2021 acompañando el texto original de la referida Propuesta de Reglamento. El objetivo final allí está resumido como la búsqueda de "*un marco jurídico destinado a lograr que la IA sea fiable*". Siguiendo esta guía inicialmente se afirma el criterio de la "proporcionalidad":

"*La propuesta se fundamenta en los marcos jurídicos existentes y es proporcionada y necesaria para alcanzar sus objetivos, ya que sigue un enfoque basado en los riesgos y únicamente impone cargas normativas cuando es probable que un sistema de IA entrañe altos riesgos para los derechos fundamentales y la seguridad. A los demás sistemas de IA que no son de alto riesgo tan solo se les imponen obligaciones muy limitadas en materia de transparencia; por ejemplo, en lo que se refiere a la*

[34] Reglamento citado, considerando 12.

presentación de información para comunicar el uso de un sistema de IA cuando éste interactúe con humanos…"[35].

Ahora bien, la sola enunciación de semejante criterio interpretativo ya plantea dudas con respecto a su preservación en el tiempo, debido a la creciente facilidad con la que un sistema de IA de bajo riesgo puede tornarse una amenaza e inducir su re-calificación. El legislador no ignoró esta fuente de incertidumbre, pues:

"*La lista de sistemas de IA de alto riesgo que figura en el anexo III contiene un número limitado de sistemas de IA cuyos riesgos ya se han materializado o es probable que lo hagan próximamente. La Comisión podría ampliar la lista de sistemas de IA de alto riesgo utilizados en determinados ámbitos predefinidos mediante la aplicación de un conjunto de criterios y una metodología de evaluación del riesgo, a fin de garantizar que el Reglamento pueda adaptarse a los nuevos usos y aplicaciones de la IA*"[36].

Habida cuenta de la referida ductilidad o flexibilidad normativa, imprescindible cuando se trata de una materia caracterizada por un ritmo de frenéticas innovaciones, se destacan en la tipología normativa europea para los sistemas de IA las dos categorías de máxima restricción: (i) las prácticas de inteligencia artificial prohibidas; y (II) los sistemas de alto riesgo, los cuales con anterioridad a su introducción en el mercado o puesta en servicio, deben someterse a una evaluación de la conformidad que garantice que son altamente fiables[37].

(i) Con respecto a la lista de prácticas de inteligencia artificial prohibidas, están establecidas en el texto del capítulo II del Reglamento. Ellas abarcan todos los sistemas de IA cuyo uso se considera inaceptable por ser contrario a los valores de la UE, comenzando por la violación de los derechos fundamentales. Las prohibiciones incluyen aquellas prácticas con gran potencial para manipular a las personas mediante técnicas subliminales que trasciendan su conciencia o que aprovechen las vulnerabilidades de grupos concretos, en ambos casos con el fin de alterar de manera sustancial su comportamiento introduciendo la probabilidad de provocar perjuicios físicos o psicológicos. Se prohíbe igualmente que las

[35] Exposición de Motivos de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial y se modifican determinados actos legislativos de la Unión", Bruselas 21 de abril de 2021 (catalogado COM (2021) 206 final), numeral 2.3.
[36] Exposición de Motivos de la Propuesta de Reglamento citada, numeral 5.2.3.
[37] Reglamento citado, considerandos 123 y 125.

autoridades públicas realicen calificaciones sociales basadas en IA cuando dichas calificaciones provoquen un trato perjudicial o desfavorable a determinadas personas o colectivos de manera injustificada o desproporcionada. Aquí cabe destacar la prohibición de "*sistemas de IA que permiten a agentes públicos o privados llevar a cabo una puntuación ciudadana de las personas físicas*",[38] sin perjuicio de tolerar, aunque considerándolos como de alto riesgo, tal como se indica más abajo, a los sistemas que categorizan o evalúan a las personas en ámbitos educativos, laborales y a propósito de los servicios y prestaciones esenciales. Por último se prohíbe, salvo excepciones reguladas, el uso de sistemas de identificación biométrica remota en tiempo real en espacios de acceso público aunque se pretenda su aplicación aduciendo fines de aplicación de la ley[39].

(ii) Con respecto a los sistemas de IA de alto riesgo, están regulados por el capítulo III y catalogados inicialmente por el anexo III del Reglamento. La evaluación de la conformidad, si bien en principio recae sobre los proveedores, se extiende durante todo el período de aplicación de cada sistema, involucrando a los responsables de su "despliegue".[40] Acerca de las figuras contempladas para caracterizar a dichos sistemas, cabe resaltar la importancia de las previsiones ya indicadas sobre los sistemas utilizados en la educación o formación profesional; en el empleo; y para la evaluación de la calificación crediticia o solvencia de personas físicas con motivo del otorgamiento de prestaciones esenciales. La magnitud del daño potencial que puede producir su aplicación surge de los *Considerandos* del Reglamento. Por ejemplo, aquellos sistemas que determinan el acceso o distribuyen a las personas entre distintas instituciones educativas y de formación profesional o que evalúan a las personas a partir de pruebas realizadas en el marco de su educación o como condición necesaria para

[38] Reglamento citado, considerandos 31 y 44.
[39] Exposición de Motivos en la Propuesta de Reglamento citada, numeral 5.2.2. Uno de los debates más acalorados y que dio lugar a modificaciones en la redacción final del Reglamento, fue precisamente la nómina de situaciones excepcionales para las cuales debe admitirse el uso de sistemas de identificación biométrica, en especial con motivo de la persecución de actividades delictivas.
[40] Por lo demás, el artículo 14 determina la obligatoriedad de una *"vigilancia humana", pues "los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas"*.

acceder a ella "*pueden decidir la trayectoria formativa y profesional de una persona y, en consecuencia, afectar a su capacidad para asegurar su subsistencia*".[41] Son también de alto riesgo los sistemas de IA que se utilizan en el empleo, la gestión de los trabajadores y el acceso al auto-empleo, sobre todo para la contratación y la selección de personal, para la toma de decisiones relativas a la promoción y la rescisión de contratos; y para la asignación de tareas y el seguimiento o la evaluación de personas en relaciones contractuales de índole laboral, dado que "*pueden afectar de un modo considerable a las futuras perspectivas laborales y los medios de subsistencia de dichas personas*".[42] Y acerca de los sistemas de IA que condicionan el acceso a determinados servicios y prestaciones esenciales, de carácter público y privado, necesarios para participar plenamente en la sociedad y mejorar el nivel de vida, su alto riesgo consiste en que a través de ellos pueden adoptarse decisiones sobre la legitimidad de ese acceso vulnerando derechos fundamentales[43].

Independientemente de las obligaciones impuestas para la convalidación de sistemas de IA de alto riesgo, rigen las obligaciones de transparencia para determinados sistemas de IA, en especial con relación a dos situaciones típicas: (i) cuando una persona interactúa con un sistema de IA y sus emociones o características son reconocidas por medios automatizados, es preciso informarla de tal circunstancia; y (ii) cuando un sistema de IA se utiliza para generar o manipular imágenes, audios o videos que a simple vista parezcan contenido auténtico, en cuyo caso debe ser obligatorio informar que dicho contenido se ha generado por medios automatizados, salvo excepciones que respondan a fines legítimos[44].

Tanto la tipología elaborada para regular los sistemas de IA como las previsiones de extra-territorialidad contempladas por el Reglamento, son de necesaria consideración para los países periféricos para que, mediante regulaciones semejantes, puedan resguardar a sus residentes de los riesgos mencionados. Con respecto a las cláusulas de extra-territorialidad, el Reglamento de la UE se aplica a los proveedores de sistemas de IA

[41] Reglamento, considerando 56.
[42] Reglamento, considerando 57.
[43] Reglamento, considerando 58.
[44] Reglamento capítulo IV: Obligaciones de transparencia de los proveedores y responsables del despliegue de determinados sistemas de IA.

establecidos en territorio de un tercer país[45] cuando la información de salida generada por dichos sistemas se utilice de algún modo en territorio de la UE[46].

Y sobre la base de los compromisos multilaterales, la UE también contempla la suscripción de acuerdos internacionales para el reconocimiento mutuo de los resultados de las evaluaciones de la conformidad a regulaciones semejantes a las establecidas en el Reglamento. En efecto:

"En consonancia con los compromisos contraídos por la Unión en virtud del Acuerdo sobre Obstáculos Técnicos al Comercio de la Organización Mundial del Comercio, es adecuado facilitar el reconocimiento mutuo de los resultados de las evaluaciones de la conformidad realizados por organismos de evaluación de la conformidad competentes, con independencia del territorio en el que estén establecidos, siempre que dichos organismos de evaluación de la conformidad establecidos con arreglo al Derecho de un tercer país cumplan los requisitos aplicables del presente Reglamento y la Unión haya celebrado un acuerdo en ese sentido. En este contexto, la Comisión debe estudiar activamente posibles instrumentos internacionales a tal efecto y, en particular, procurar celebrar acuerdos de reconocimiento mutuo con terceros países"[47].

5. <u>Medidas restrictivas justificadas por imperativos de seguridad nacional y dirigidas contra corporaciones en el sector de las TIC asociadas o relacionadas con otros Estados (en el marco de la "guerra comercial" entre EUA y RPC) y que dieron lugar a la imposición de restricciones</u>

El caso paradigmático fue abierto por la Orden Ejecutiva del Presidente de EUA dictada el 16 de mayo de 2019 por la cual se prohibió a las empresas estadounidenses utilizar dispositivos elaborados por compañías cuyas actividades hicieran suponer un

[45] En términos del considerando 21 del Reglamento: "Con el objetivo de garantizar la igualdad de condiciones y la protección efectiva de los derechos y libertades de las personas en toda la Unión, las normas establecidas en el presente Reglamento deben aplicarse a los proveedores de sistemas de IA sin discriminación, con independencia de si están establecidos en la Unión o en un tercer país (…)".
[46] La posibilidad de elusión intenta ser neutralizada mediante la aplicación del Reglamento a los proveedores y responsables del despliegue de sistemas de IA establecidos en un tercer país, en la medida que se pretenda que la información de salida generada por dichos sistemas de utilice en la Unión y aunque el sistema en cuestión no sea introducido en el mercado. Véase al respecto la descripción del Reglamento en su considerando 22.
[47] Reglamento, considerando 127.

riesgo para la seguridad nacional[48]. Esta Orden Ejecutiva estuvo anticipada e inspirada por la Ley de Defensa Nacional (*National Defense Authorization Act for 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 de *"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"*. Esta descripción procuró abarcar a los equipos de telecomunicaciones o servicios producidos o provistos por entidades que la Secretaría de Defensa, en consulta con otras autoridades, estimara razonablemente como pertenecientes, controladas o conectadas con un gobierno extranjero al que, por lo demás, se lo identificaba expresamente como RPC (Sección 898 (f) Definiciones, 3 D). La misma Ley mencionó a determinadas empresas, como HUAWEI TECHNOLOGIES COMPANY y ZTE CORPORATION, con respecto a las cuales ni siquiera se requirió el cumplimento de las presunciones indicadas más arriba para llevar a cabo las restricciones contra ellas.

Esta discrecionalidad gubernamental estuvo fundada en la imputación de una capacidad actual o potencial de las empresas afectadas para la apropiación y manipulación de datos mediante el control de redes informáticas de alta velocidad.

El referido trato discriminatorio mereció prontos cuestionamientos por la RPC, que era –y sigue siendo- uno de los mayores productores y abastecedores mundiales de las materias primas indispensables para la producción de dispositivos e insumos en numerosos rubros de las TIC. Son las denominadas "tierras raras" respecto de las cuales ya con anterioridad RPC venía aplicando restricciones a sus exportaciones argumentando la protección de recursos naturales no renovables (GATT artículo XX g) y la reducción de la contaminación ambiental. Como es sabido, ello dio lugar a litigios sustanciados en el SSD ante presentaciones de EUA, UE y Japón que en las dos instancias rechazaron los citados argumentos de RPC[49].

Por su parte, la RPC ha venido replicando a las restricciones discriminatorias de EUA mediante disposiciones también restrictivas y bajo el mismo paraguas de la seguridad

[48] Las referencias reproducen citas del autor en el documento "Datos personales: seguridad nacional y concertación internacional. La disyuntiva latinoamericana", en Revista Aportes para la Integración Latinoamericana número 40, año XXV junio 2019.
[49] WT/DS431 a requerimiento de EUA; WT/DS432 a requerimiento de UE; y WT/DS433 a requerimiento de Japón.

nacional. Inicialmente sancionó una Lista de Entidades No Confiables (UEL) y un Catálogo de Tecnologías Prohibidas y Restringidas de Exportación 2020 en sintonía con modificaciones a la Ley de Control de Exportaciones (FTL). El referido Catálogo fue acompañado por un mecanismo de aprobación previa para la exportación de bienes y servicios susceptibles de doble uso (comercial y militar) o relacionados con el mantenimiento de la seguridad y los intereses nacionales[50].

6. Procedimientos administrativos y judiciales contra corporaciones transnacionales del sector de las TIC dentro de la misma zona de influencia geopolítica del Estado u Estados actuantes.

Desde esta perspectiva habría que contabilizar durante los últimos tiempos el desarrollo de instancias controversiales como las siguientes:

(i) Demanda del gobierno federal y diecisiete gobiernos estaduales de EUA a AMAZON por prácticas anticompetitivas, en setiembre de 2023;

(ii) Demanda del gobierno federal de EUA a GOOGLE por abuso de posición dominante, también en septiembre de 2023 con respecto a la tienda de aplicaciones ("*play store*") de dispositivos ANDROID[51]. En diciembre del mismo año se difundió la noticia de un acuerdo, en el marco del citado litigio, por el cual GOOGLE quedaba comprometido al pago de setecientos millones de dólares[52] aceptando además métodos de facturación alternativos para su "*play store*". Habían sido controvertidos los contratos de GOOGLE con fabricantes de teléfonos inteligentes, operadores de redes y desarrolladores de juegos que debido a las tarifas excesivas afectaban la competencia[53].

(iii) Apertura en junio de 2023 de un procedimiento administrativo por la Comisión Europea contra GOOGLE por abuso de posición dominante

[50] Véase al respecto el artículo de Zhou, W., Jiang, H. y Chen, Z.: "*Trade vs. Security: recent developments of global trade rules and China´s policy and regulatory responses from defensive to proactive"*, World Trade Review, vol.22 number 2, may 2023, p.193-211.
[51] Véase la nota de Paul Wiseman y Michael Liedtke *"US claims GOOGLE pays more than ten billion a year to mantain its search dominance"* publicada por la agencia AP el 12 de septiembre de 2023.
[52] Seiscientos treinta millones de dólares a un fondo e conciliación para los consumidores y setenta millones de dólares a un fondo para los Estados.
[53] Michael Acton: "GOOGLE pagará setecientos millones de dólares en un acuerdo antimonopolio por la tienda de aplicaciones de Android", Financial Times, December19, 2023.

en sus anuncios en línea que según se presumía venía ocurriendo desde 2014 y que podía justificar la aplicación de multas siderales.

(iv) Requerimiento de APPLE solicitando que para habilitar el acceso a los datos de notificaciones "*push*" (alertas automáticas dirigidas a los usuarios sobre noticias, mensajes entrantes, boletines meteorológicos y otros contenidos), las autoridades del gobierno de EUA contaran con órdenes judiciales. Esta petición surgió como medida defensiva de la corporación con motivo de las revelaciones de un senador del Estado de Oregon, quien había advertido que agencias gubernamentales de otros países estaban exigiendo datos de notificaciones "*push*" de teléfonos inteligentes tanto de GOOGLE como de APPLE. Este senador interpretó, en su comunicación al Fiscal General, el 6 de diciembre de 2023, que "*APPLE y GOOGLE están en una posición única para facilitar la vigilancia gubernamental de cómo los usuarios usan aplicaciones particulares*"[54].

(v) Multa fijada por la UE contra la empresa APPLE por obstaculizar la competencia en marzo de 2024. Se trató de la culminación de un procedimiento de investigación que llevó alrededor de cinco años, impulsado por SPOTIFY, empresa que se consideró afectada por las comisiones requeridas por APPLE con motivo del ofrecimiento de servicios de emisión de música continuada mediante la *AppStore*. Si bien al entrar en vigor el Reglamento europeo sobre Mercados Digitales APPLE quedaría obligada a la apertura de su iPhone a tiendas de aplicaciones competidoras, la empresa ya había iniciado maniobras evasivas, con antelación a esta puesta en vigencia[55].

(vi) Demanda del gobierno federal de EUA contra APPLE el 21 de marzo de 2024 por monopolizar el mercado de teléfonos inteligentes. La acusación aludió a distintas estrategias de acaparamiento como las destinadas a disminuir la funcionalidad de relojes inteligentes que no son de APPLE, limitar el acceso al pago sin contacto para billeteras

[54] "APPLE ahora requiere órdenes judiciales en EEUU para acceder a los datos de las notificaciones push", noticia publicada por la agencia AP el 20 de diciembre de 2023.
[55] Véase la nota de Tripp Mickle y Adam Satariano "La UE multa a APPLE por usar la AppStore para obstaculizar la competencia" en The New York Times del 4 de marzo de 2024.

digitales de terceros y negarse a permitir que la aplicación *iMessage* intercambiara mensajes cifrados con plataformas de la competencia[56].

La mera enumeración de casos indica que por un lado EUA y la UE y, por otro lado las BIG-TECH, están transitando una etapa de confrontación caracterizada por la incertidumbre que provocan las prácticas de abuso de posiciones dominantes cuando en este mercado las reglas de transparencia todavía no han logrado consolidarse. Siendo aún borrosos los límites entre lo permitido y lo prohibido, las corporaciones afinan sus estrategias para seguir incrementando las fuentes de ingresos.

7. Efecto *boomerang*: límites que la economía global impone a las restricciones comerciales aplicadas en el sector de las TIC

Con respecto a los obstáculos del gobierno de EUA a la penetración de empresas de la RPC en el área de las TIC, tal como se resume más arriba, cabe recordar que algunos países asociados a EUA y las corporaciones asentadas en ellos, como es el caso de la República de Corea, dependen de la importación de variados suministros tecnológicos, empezando por los mismos semiconductores[57].

Y también asoman dificultades operativas del lado de RPC, pues sus obstáculos para el uso en las agencias estatales de dispositivos de marcas extranjeras como APPLE no parecen haber considerado que millones de trabajadores en ese país trabajan directa o indirectamente para su propia fabricación y que, por otro lado, APPLE es uno de los mayores compradores de chips en el mundo[58]. En el mismo sentido, a principios de 2024 se informó que durante el año anterior APPLE había encabezado el mercado chino de *smartphones*[59].

[56] Esta demanda fue comentada por la nota ya citada de Michael Liedtke, Lindsay Whitehurst, Mike Balsamo y Frank Bajak: "El Departamento de Justicia demanda a APPLE, alegando que monopolizó ilegalmente el mercado de teléfonos inteligentes".
[57] Véase la nota en The New York Times del 27 de septiembre de 2023: *"What the U.S.-China chip war means for a criticial american ally*".
[58] Véase la nota de Dan Gallagher en The Wall Street Journal del 8 de septiembre de 2023: "APPLE queda en el centro de la guerra económica entre EUA y China".
[59] "APPLE se hizo con el primer puesto en envíos de teléfonos inteligentes en el mercado chino por primera vez el año pasado, según datos publicados el viernes, a pesar de la creciente competencia de fabricantes nacionales (…) La cuota de mercado (de APPLE) en RPC se situó en el 19% indicó el proveedor de datos del sector CANALYS (…) Tres fabricantes nacionales, VIVO, OPPO y HONOR se situaron el año pasado por detrás de APPLE con cuotas de mercado en RPC del 16% cada uno (…) HUAWEI en el cuarto trimestre regresó al top 5 del mercado de *smartphones* de RPC después de diez trimestres (…)" (FRANCE 24, 26 de enero de 2024¸ citando como fuente a AFP).

Por lo demás, debe tomarse en consideración la dificultad para llevar a la práctica distintas restricciones comerciales, cuando las corporaciones se valen de programas de software ajenos de acceso irrestricto aunque no susceptibles de reformulación (*open source software*) para potenciar sus propias innovaciones.

Entre los ejemplos recientes que ponen en evidencia las dificultades generadas por esta interdependencia de recursos, pueden mencionarse:

a) El caso de los semi-conductores aplicados a super-computadoras que utilizan instrucciones destinadas a implementar arquitecturas catalogadas como "*Risc*" y que están siendo desarrolladas por RPC. La única opción parecería consistir, para el gobierno de EUA, en impedir, mediante distintas estrategias, que corporaciones asentadas en su territorio pudieran contribuir de algún modo a ese desarrollo tecnológico llevado a cabo por corporaciones de RPC[60].
b) El modelo de IA de la empresa china 01.AI, basado en LLaMA (de la empresa META). Según el creador de dicha herramienta en 01.AI, esta utilización de LLaMA no sería excepcional, sino que reflejaría una conducta semejante a "la mayoría de las otras empresas de IA", agregando que el uso de tecnologías de código abierto consistiría en una práctica habitual[61].

Al recrudecer las preocupaciones del gobierno de EUA por la protección de los datos personales de sus residentes, inevitablemente aparecen también signos de inquietud al advertirse que las medidas restrictivas pueden tener efecto contraproducente para la fluidez de la conectividad global. En tal sentido, al anunciar la emisión de una Orden Ejecutiva del Presidente Biden el 28 de febrero de 2024 "*to Protect Americans' Sensitive Personal Data*" frente a eventuales intromisiones de países elípticamente catalogados como "*countries of concern*", la oficina gubernamental distribuyó un papel en el que, luego de enumerar las instrucciones dadas a distintas reparticiones públicas, advierte:

> *"(…) That these activities do not stop the flow of information necessary for financial services activities or impose measures aimed at a broader decoupling*

[60] Véase, por ejemplo, la nota publicada por The New York Times el 10 de enero de 2024 titulada "*The Next Front in the U.S. China Battle Over Chips*".
[61] Nota de Paul Mozur, John Liu y Cade Metz: "China quiere liderar en IA pero hay un detalle: depende de tecnología de EEUU", en The New York Times del 3 de marzo de 2024.

of the substantial consumer, economic, scientific, and trade relationships that the Unites States has with other countries".

En suma, la dificultad para avanzar en la aplicación de restricciones y retaliaciones recíprocas entre EUA y RPC, habida cuenta de la interdependencia económica y comercial preexistente, puede ser ilustrada por el título de una nota de Peter Goodman publicada el 15 de noviembre de 2023 en el New York Times: "*The rise and fall of the world's most successful joint venture. China and the US both gained from their economic integration. As they pull apart, each is finding it will be hard to fully replace the other*".

8. Los nuevos términos de la dependencia tecnológica con motivo de las regulaciones en el sector de las TIC. Perspectiva latinoamericana

La profusión de regulaciones y procedimientos administrativos y jurisdiccionales emprendidos por los Estados de países desarrollados frente a las corporaciones transnacionales que operan las TIC contrasta con la pasividad de muchos Estados periféricos[62].

Las sociedades del mundo elípticamente catalogadas como "en desarrollo" están sujetas a los estímulos compulsivos de la economía digital tanto como las sociedades de los países centrales. Pero en líneas generales, su vulnerabilidad es mayor debido a las condiciones de vida que prevalecen en ellas y la consiguiente proclividad de amplios segmentos de su población para asimilar contenidos virtuales bajo la forma de ofertas o promesas engañosas. De ahí que resulte indispensable apreciar las políticas regulatorias que están llevando a cabo EUA, la RPC y la UE para esbozar posibles

[62] Sin embargo, el caso del Brasil puede representar un ejemplo aleccionador. Con motivo de una investigación sobre noticias falsas difamatorias y amenazantes contra jueces de la Corte Suprema, en abril de 2024 seguía su curso un procedimiento de investigación sobre la plataforma "X". En tales circunstancias y a título personal, el aparente propietario o accionista mayoritario, E. Musk, utilizó la misma plataforma para conjeturar acerca de un eventual incumplimiento por la corporación de las órdenes judiciales que habían sido ya dictadas para bloquear determinadas cuentas. Ello dio lugar a que uno de los jueces de la Corte incluyera al mismo Musk en la investigación, aduciendo que "*la conducta flagrante de obstrucción de la justicia brasileña, la incitación al crimen, la amenaza pública de desobediencia a órdenes judiciales y la futura falta de cooperación de la plataforma son hechos que irrespetan la soberanía de Brasil*". Y el fiscal general del Brasil escribió en la misma red: "*No podemos vivir en una sociedad en la que multimillonarios domiciliados en el extranjero tengan el control de las redes sociales y se pongan en condiciones de violar el Estado de derecho, incumpliendo órdenes judiciales y amenazando a nuestras autoridades. La paz social es innegociable*" (nota publicada por la agencia AP el 8 de abril de 2024: "Elon Musk será investigado por *fake news* y obstrucción en Brasil tras orden del Tribunal Supremo").

líneas de acción de los Estados de países en desarrollo que se compatibilicen y complementen con ellas.

Por el momento está expedita una vía de negociación institucionalizada entre algunos Estados latinoamericanos y otros Estados de mayor desarrollo relativo que podría encauzar nuevas regulaciones y acuerdos. Por ejemplo, el Tratado Integral y Progresista de Asociación Transpacífico (CPTPP)[63] incluye, con motivo del comercio electrónico, previsiones sobre protección al consumidor en línea, protección de la información personal y transferencia transfronteriza de información por medios electrónicos. Si bien esencialmente se trata de cláusulas permisivas, que apenas consagran un reconocimiento recíproco de las regulaciones nacionales en la materia, podrían ser objeto de futuras acciones de complementación y cooperación[64].

Más específicamente, el Acuerdo de Asociación de Economía Digital (DEPA)[65] reproduce disposiciones similares al CPTPP y es otra vía de interacción que originariamente propulsaron los gobiernos de Chile, Nueva Zelanda y Singapur pero que tiende a expandirse[66].

Entretanto, en el campo de la IA y, en particular de la IA generativa, se potencian los riesgos para poblaciones que, como las asentadas en los países latinoamericanos, padecen condiciones de vida que llevan a sobrevalorar las promesas y ofertas digitales. Por ejemplo, los tres tipos de aplicaciones posibles de la IA para la educación, el trabajo y el acceso a prestaciones esenciales, incluyendo el crédito, contempladas por el Reglamento de la UE y mencionadas más arriba para ilustrar los sistemas de IA de alto riesgo, pueden dar lugar a daños masivos en las sociedades latinoamericanas si no son objeto de cuidadosa regulación y control.

Como se apuntó, tanto la tipología elaborada para regular los sistemas de IA como las previsiones de extra-territorialidad contempladas por el Reglamento de la UE son de

[63] En inglés: *Comprehensive and Progressive Agreement for Transpacific Partnership*. En este acuerdo participan Chile, México y Perú junto a Brunei, Malasia, Singapur, Vietnam, Japón, Australia, Nueva Zelanda, Canadá y el Reino Unido.
[64] Las disposiciones mencionadas figuran en el capítulo 14 "Comercio electrónico". Son los artículos 14.7, 14.8 y 14.11.
[65] En inglés *"Digital Economy Partnership Agreement"*.
[66] En junio de 2023 los miembros del DEPA se reunieron con una delegación de la República de Corea en el marco de una sesión ministerial de la OCDE y anunciaron el cierre sustantivo de negociaciones para el ingreso de dicho país al acuerdo. Por otro lado avanzan grupos de trabajo con vistas a la adhesión de RPC, Canadá y conversaciones avanzadas con Costa Rica y Perú.

necesaria consideración en los países periféricos para que, mediante regulaciones semejantes, puedan resguardar a sus residentes de los riesgos mencionados.

A propósito de las cláusulas de extra-territorialidad, el Reglamento de la UE se aplica a los proveedores de sistemas de IA establecidos en territorio de un tercer país en la medida que la información de salida generada por dichos sistemas se utilice en territorio de la UE. De modo que una normativa semejante podría proteger a los usuarios residentes en países periféricos ante operatorias similares a las prohibidas o restringidas por la UE y por otros Estados que adopten disposiciones afines.

Complementariamente, los países en desarrollo deberían proteger a los usuarios localizados en sus territorios frente a operatorias que hubieran sido prohibidas o restringidas a los proveedores de dichas ofertas tecnológicas en los países industrializados. Ahora bien, ¿cómo hacerlo? En una publicación reciente[67] el autor propuso seguir la previsión del Reglamento de la UE, acordando el reconocimiento mutuo sobre procedimientos de evaluación de conformidad a los reglamentos establecidos para operatorias de IA consideradas como de alto riesgo, según las respectivas legislaciones de los países signatarios. De tal modo podrán inhibirse las operaciones transfronterizas que pretendan introducir en los mercados latinoamericanos proveedores de software de IA cuando por el nivel de riesgo rijan restricciones en las contra-Partes, cualquiera fuese la radicación territorial o contable de dichos proveedores o emisores.

Por último, debería plantearse un problema más intrincado pero de necesaria consideración: el referido a la carga de datos en los sistemas de IA de alto riesgo, tales como los destinados a la tipificación y evaluación de personas en ámbitos educativos, laborales y de prestaciones esenciales. ¿Habrá que admitir a libro cerrado una supuesta homogeneidad universal de los datos con los que se alimentan los sistemas de IA de alto riesgo? ¿O bien las particulares condiciones de vida en sociedades periféricas tendrían que ser tenidas en cuenta no sólo a la hora de operar dichos sistemas sino mucho antes, esto es, a partir de las instancias de su programación?

9. Conclusiones

[67] "Inteligencia artificial: ¿deberíamos arriesgarnos a perder el control de nuestra civilización?" publicado por Latinoamérica21 el 22 de junio de 2023.

A. Las sociedades periféricas y, en particular, las de los países latinoamericanos, están padeciendo una desarticulación cuyos motivos no han sido suficientemente visibilizados. Numerosos datos corroboran masivos desplazamientos o segregaciones en los sistemas de estratificación social, al interior de las fronteras y a través de ellas. Pero no suele advertirse cuál es la relación entre estas calamidades y el ritmo impuesto por las innovaciones tecnológicas, es decir, los procesos de acumulación y reproducción del capital bajo la matriz productiva impuesta por las corporaciones transnacionales en el sector de la informática y las comunicaciones (TIC). La frenética sustitución de tecnologías compromete la subsistencia de agregados sociales cada vez más extensos en la medida que van eclosionando condiciones de producción preestablecidas. Y en las periferias este impacto se suma al generado por las fracturas geo-económicas y geo-políticas que al calor de la "guerra comercial" hacen que los circuitos económicos y comerciales se vayan concentrando dentro de territorios dotados de mayores garantías de confiabilidad. En este marco el desafío político tanto para los gobiernos de países centrales como para los periféricos consiste en sostener el ritmo de expansión al que deben seguir contribuyendo los consumidores y también usuarios de los sistemas digitales aunque se vayan empobreciendo, lo que demanda mayores recursos del erario público. Entretanto EUA y la RPC despliegan políticas internacionales predatorias y acaparadoras de mercados ("guerra comercial") para mitigar así el daño producido por la competencia en el curso de estas pugnas que tienen como finalidad última el sostenimiento de la dinámica de acumulación y reproducción del capital. Si bien la carrera desaforada por la apropiación de mercados no se limita al sector de las TIC, las batallas tienden a concentrarse sobre áreas que directa o indirectamente dependen del desempeño de las corporaciones transnacionales en el sector. Ello se debe por un lado a la incidencia de sus prestaciones en el comercio y las inversiones internacionales, atravesando las más diversas cadenas de suministro y de valor; y, por otro lado, a la extraordinaria concentración y el ritmo de reproducción del capital que, animado por un potente sucedáneo de la plusvalía, se refleja en las incesantes oleadas de sustituciones tecnológicas promovidas dentro del propio sector de las TIC y hacia todo el espectro de la actividad económica. Así, las corporaciones de mayor envergadura caracterizadas inicialmente por la emisión y procesamiento de contenidos

digitales (BIG-TECH) están exhibiendo una explosiva diversificación productiva y de negocios.

B. Frente a tamaña expansión, son cada vez más abundantes y detalladas las reglamentaciones y también los procedimientos jurisdiccionales y administrativos en los países centrales para regular al sector de las TIC. Aquí conviene atender a la superposición de valores o bienes jurídicos protegidos. En primer lugar se destaca el papel de la "seguridad", esto es, la extraordinaria importancia que asignan los gobiernos a la necesidad de neutralizar amenazas en la lucha por la preservación y acaparamiento de mercados. En tal sentido, la "seguridad" es un valor a considerar no sólo a propósito de las regulaciones directamente referidas a la "defensa" militar. En la medida que los Estados aducen prácticas anticompetitivas, deslealtades comerciales y vulneración de la privacidad en la operatoria de las TIC, también están sirviendo a los objetivos de "seguridad" porque en un mundo fragmentado tanto la depredación y el acaparamiento de mercados como la vulneración de la confidencialidad se pueden leer como agresiones a la integridad política o menoscabo de la gobernabilidad. En este último aspecto puede resultar ilustrativa la conceptualización empleada por una Orden Ejecutiva del Presidente de EUA en febrero de 2024, al disponer medidas para proteger la confidencialidad de datos personales de residentes en su país contra la intromisión de operaciones alentadas desde otros Estados calificados como inquietantes ("*countries of concern*"). Por su lado las corporaciones suelen encubrir prácticas anticompetitivas y desleales invocando la protección a la privacidad de los usuarios. Tal es el caso de APPLE cuando enarbola la hipotética garantía de confidencialidad que ofrece a sus usuarios: el jardín amurallado ("*walled garden*"). Finalmente, para la fijación de responsabilidades fiscales a corporaciones transnacionales que procuran evadirlas buscando el amparo de la "nube", se suma otra vez una cuestión de seguridad nacional atendiendo a la necesidad de los Estados para captar recursos destinados a neutralizar o al menos reducir la segregación o marginación social atribuida a los abruptos saltos de innovación tecnológica. Pero la responsabilidad fiscal cuando se opera en la "nube" es de difícil detección. De ahí que una fuente alternativa de recaudación tributaria, en especial para la UE, consiste en la imposición de multas cuantiosas a las corporaciones infractoras. Al establecer y aplicar dichas sanciones, no sólo se considera en cada caso la magnitud del

perjuicio ocasionado por la infracción, sino también la envergadura económica de la corporación.

C. Durante los últimos años e invocando a los bienes jurídicos mencionados, se han ido superponiendo regulaciones a través de las cuales EUA, la RPC y la UE intentan controlar la compleja operatoria de las corporaciones involucradas en las TIC. Un avance significativo lo produjo la UE al dictar el Reglamento General sobre la Protección de Datos (2016), adoptado como modelo en RPC y Brasil para el diseño de sus propias disciplinas. La segunda generación de disposiciones de la UE sobre la materia se materializó con el diseño y reciente puesta en vigor de dos Reglamentos paralelos, uno de ellos acerca de los mercados digitales (individualizado como DMA) y otro enfocado sobre los servicios digitales (individualizado como DSA). El DMA procura contrarrestar de manera sistemática prácticas monopólicas mediante la identificación y encuadramiento de las consideradas grandes plataformas digitales ("*gatekeepers*"). Y el DSA tiene por objeto proteger a los usuarios frente a contenidos ilegales, desinformaciones y publicidad engañosa. Dicho Reglamento proveyó las referencias normativas utilizadas por la Comisión Europea a fines de 2023 para investigar a la plataforma en línea "X" y más tarde a TIK-TOK. En este caso las autoridades habilitaron investigaciones acerca de la inducción de comportamientos adictivos, maniobra que en la jerga es calificada por sus efectos: la madriguera del conejo ("*rabbit hole effects*"). Esta última plataforma fue poco tiempo después señalada por la Cámara de Representantes de EUA, pero por otro motivo: un proyecto de ley la catalogó como amenaza potencial para la seguridad del Estado.

D. Con respecto a los sistemas de IA la UE lleva la delantera en los ímprobos esfuerzos por encauzar la operatoria comercial que deriva de procesos de conocimiento que están en plena y acelerada evolución. De ahí el extenso y pormenorizado debate sobre los lineamientos más adecuados para una normativa que pudiera cubrir por primera vez y de manera sistemática los riesgos que conlleva la IA. El resultado parece auspicioso, si bien cualquier ordenamiento disciplinario es en esta instancia de difícil instrumentación habida cuenta del carácter vertiginoso de las transformaciones tecnológicas en curso. De ahí las alertas pero también el enfoque prudente que caracteriza al Reglamento del Parlamento Europeo y del Consejo por el que se "establecen

normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial)" finalmente sancionado como Resolución legislativa del Parlamento Europeo el 13 de marzo de 2024. El Reglamento de la UE califica y pondera los sistemas de IA atendiendo a niveles de riesgo, contemplando variadas hipótesis de prohibición, control, excepción y transitoriedad. Merece ser considerado como ensayo germinal de una futura normativa multilateral o plurilateral sobre la materia. Su principal valor radica entonces en la metodología, pues introduce categorías aptas para encasillar –y des-encasillar- distintos tipos de contenidos según la envergadura de los daños que pudieran ocasionar a las personas físicas individualmente y a diversos agrupamientos y colectivos humanos.

E. Al efectuar un relevamiento de los procedimientos jurisdiccionales y administrativos que EUA, la UE y la RPC llevan a cabo para acotar los márgenes de acción de las corporaciones transnacionales en el sector de las TIC, ha de advertirse su relación con las ostensibles fracturas geoeconómicas y geopolíticas usualmente sintetizadas bajo la expresión "guerra comercial". De ahí que en este documento se consideren, por separado: (i) las medidas adoptadas por el gobierno de EUA contra corporaciones de la RPC y las posteriores acciones del gobierno de la RPC asimilables a retaliaciones; (ii) los procedimientos llevados a cabo por el gobierno de EUA y por la UE contra corporaciones transnacionales dentro de su propia zona de influencia geopolítica; y (iii) el carácter contraproducente de algunas de estas acciones (efecto *boomerang*), habida cuenta de la interdependencia económica y comercial que a escala global sigue condicionando al sector de las TIC, ya sea por la necesidad de contar con el suministro de materias primas e insumos cuya oferta está circunscripta a determinados orígenes o bien por la imposibilidad de impedir el uso de programas de software de acceso irrestricto (*open source*).

F. Entretanto en América Latina todavía no se han aplicado políticas consistentes para contrarrestar tanto los perjuicios actuales como los riesgos potenciales de la sociedad digital. En general, vastas poblaciones de los países en desarrollo, dadas las consecuencias del empobrecimiento y la marginalidad, están sujetas a los estímulos compulsivos de los contenidos virtuales en condiciones de mayor vulnerabilidad que las de los usuarios radicados en países centrales. De ahí la proclividad para incurrir en conexiones adictivas y padecer

desinformaciones y engaños. Por ello no debería demorarse la apreciación por los gobiernos latinoamericanos de las políticas regulatorias que están llevando a cabo EUA, la RPC y la UE para esbozar posibles líneas de acción que se compatibilicen y complementen con ellas. En este sentido resalta que el Reglamento de la UE prevea su aplicación a los proveedores de sistemas de IA establecidos en territorio de un tercer país en la medida que la información de salida generada por dichos sistemas se utilice en territorio de la UE. La adopción de una normativa semejante por gobiernos de países latinoamericanos podría proteger a sus residentes, en calidad de usuarios, ante operatorias similares a las prohibidas y a las restringidas por su alto riesgo en la UE. Adicionalmente debería protegerse a los usuarios locales frente a operatorias que hubieran sido prohibidas o restringidas a los proveedores en países industrializados, recurriendo a convenios de reconocimiento mutuo sobre procedimientos de evaluación de conformidad a los reglamentos establecidos para operatorias de IA de alto riesgo, tal como lo contempla el mismo Reglamento de la UE. De este modo podrán inhibirse las operaciones transfronterizas que pretendan introducir en los mercados latinoamericanos proveedores de software de IA cuando por el nivel de riesgo rijan prohibiciones o restricciones en las contra-Partes, cualquiera fuese la radicación territorial o contable de dichos proveedores o emisores. Quedaría pendiente una cuestión más compleja: la pertinencia de los datos con los cuales se alimentan los sistemas de IA de alto riesgo. Las particulares condiciones de vida bajo las cuales se desenvuelven las sociedades periféricas como son las latinoamericanas, justifican que al menos se ponga en duda la conveniencia de aplicar, en ámbitos tan sensibles como el educativo, el ocupacional y el de las prestaciones asistenciales, los mismos tipos de datos utilizados para su procesamiento por los sistemas de IA operados en países centrales.

Referencias bibliográficas

Acton, M. (2023, 19 de diciembre.).GOOGLE top pay 700 mn. in antitrust settlement over Android app store. *Financial Times*. https://www.ft.com/content/e7f7c7d6-79b4-4de4-aa4b-f656546a91ca

Alderman, L. (2024, 20 de Febrero). La UE investigará a TikTok por su diseño adictivo. *The New York Times*. https://www.nytimes.com/es/2024/02/20/espanol/tiktok-comision-europea.html

Bojalil, P., Egan, M., y Vela-Treviño, C. (2019, 12 de Febrero). *Despuntan las reformas en materia de protección de datos en América Latina*. Banco Interamericano de

Desarrollo. https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/

Chan, K. (2023, 18 de dicembre). European Union investigating Musk´s X over possible breaches of social media law. *The Denver Post*. https://www.denverpost.com/2023/12/18/european-union-investigating-musks-x-over-possible-breaches-of-social-media-law/

China Law Translate. (2016, 7 de noviembre). *2016 Cibersecurity Law*. https://www.chinalawtranslate.com/en/2016-cybersecurity-law/

China Law Translate. (2021, 10 de junio). *Data Security Law of the PRC*. https://www.chinalawtranslate.com/en/datasecuritylaw/

China Law Translate. (2021, 20 de agosto). *Personal Information Protection Law*. https://www.chinalawtranslate.com/en/Personal-Information-Protection-Law/

Clark, D. y Swanson, A. (2024, 10 enero). The Next Front in the U.S. China Battle Over Chips. *The New York Times*. https://www.nytimes.com/2024/01/10/technology/risc-v-china-united-states-chips-security.html

France24. (2024, 26 de enero). *Apple encabeza por primera vez el mercado chino de smartphones.* AFP. https://www.france24.com/es/minuto-a-minuto/20240126-apple-encabeza-por-primera-vez-el-mercado-chino-de-smartphones

Gallagher, D. (2023, 8 de Septiembre). Apple queda en el centro de la guerra económica entre EUA y China. *La Nación*. https://www.lanacion.com.ar/el-mundo/apple-queda-en-el-centro-de-la-guerra-economica-entre-eeuu-y-china-nid08092023/

Garcia Veiga, J. (2020, Junio). *Laboratorio de Estudios sobre Empresas Transnacionales. BIGTECH el gran ganador de la pandemia*. CLACSO. https://www.clacso.org/corporaciones-transnacionales-frente-al-covid-19-i/

Halperin, M. (2019). Datos personales: seguridad nacional y concertación internacional. La disyuntiva latinoamericana. *Revista Aportes para la Integración Latinoamericana*, (40). https://doi.org/10.24215/24689912e019

Halperin, M. (2020). La ciudadanía digital en el cielo latinoamericano. *Informe Integrar*, (124). https://www.iil.jursoc.unlp.edu.ar/sitio/index.php/site-administrator/boletin

Halperín, M. (2023, 22 de junio). Inteligencia artificial: ¿deberíamos arriesgarnos a perder el control de nuestra civilización? *Latinoamérica21*. https://latinoamerica21.com/es/inteligencia-artificial-deberiamos-arriesgarnos-a-perder-el-control-de-nuestra-civilizacion/

Halperin, M. (2023, 9 de Julio). La nueva política comercial norteamericana. *TradeNews*. https://tradenews.com.ar/la-nueva-politica-comercial-norteamericana/

House of representatives of USA. (2020, 6 de octubre). *Investigation of Competition in Digital Markets Majority Staff Report and Recommendations*.

https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/html/CPRT-117HPRT47832.htm

Lacan, J. (1992). *El seminario de Jacques Lacan. Libro 17. El Reverso del Psicoanálisis 1969-1970. Texto establecido por Jacques-Alain Miller* (pp.41 y ss.). Paidós.

Liedtke, M., Whitehurst, L., y Balsamo, M. (2024, 21 de marzo). *EEUU demanda a APPLE, acusándola monopolio en mercado de smartphones*. AP. https://apnews.com/us-news/general-news-354d206cc56e1c881b7173b81ba615ce

Liu, J., y Yu, Y. J. (2023, 1 de octubre). What the U.S.-China chip war means for a criticial americanally. *The New York Times*. https://www.nytimes.com/2023/09/27/business/samsung-hynix-south-korea.html

Mellado, Noemí B. (2023). Tecnologías digitales e interrogantes en materia tributaria. *Revista Aportes para la Integración Latinoamericana*, (48). https://doi.org/10.24215/24689912e049

Mickle, T., y Satariano, A. (2024, 4 de marzo). La UE multa a APPLE por usar la App Store para obstaculizar a la competencia. *The New York Times*. https://www.nytimes.com/es/2024/03/04/espanol/apple-multa-europa.html

Miller, J. A. (2010). *Extimidad*. Paidós.

Mozur, P., Liu, J., y Metz, C. (2024, 3 de marzo). China quiere liderar en IA, pero hay un detalle: depende de tecnología de EEUU. *The New York Times*. https://www.nytimes.com/es/2024/03/03/espanol/china-inteligencia-artificial.html

OMC. (1988). *Acuerdo General sobre el Comercio de Servicios. Cuarto Protocolo. Anexo relativo a las negociaciones sobre telecomunicaciones básicas*. https://www.wto.org/spanish/docs_s/legal_s/26-gats_02_s.htm#annbas

OAS. (1994, 13 de junio). *TLC Colombia-México. Artículo 11.07*. http://www.sice.oas.org/ctyindex/COL/COLagreements_e.asp

OAS. (1998, 17 de abril).*TLC Chile-México.ACE41.Artículos 12.01 y 12.06*. http://www.sice.oas.org/Trade/chmefta/indice.asp

OAS. (1999). *TLC Centroamérica-Chile*. *Artículos 13.02 y 13.07*. http://www.sice.oas.org/TPD/CACM_CHL/CACM_CHL_e.ASP

OAS. (2002, 6 de marzo). *TLC Centroamérica-Panamá*. Artículo 13. http://www.sice.oas.org/Trade/Capan/indice.asp

OAS. (2003, 15 de febrero). *TLC Chile-Corea del Sur. Artículo 12.6*. http://www.sice.oas.org/Trade/Chi-SKorea_e/ChiKoreaind_e.asp

OAS. (2003, 6 de junio). *TLC Chile-EUA. Artículo 13.4*. http://www.sice.oas.org/Trade/chiusa_e/chiusaind_e.asp

OAS. (2003, 15 de noviembre). *TLC México-Uruguay*. *ACE60*. *Artículo 11.06*. http://www.sice.oas.org/Trade/mexurufta_s/mexuruind_s.asp

OAS. (2006, 12 de abril). *Acuerdo de Promoción Comercial Perú-EUA*. *Artículos 14.4 y 14.17*. http://www.sice.oas.org/Trade/PER_USA/PER_USA_s/Index_s.asp

OAS. (2006, 22 de noviembre). *TLC Colombia-EUA*. *Artículo 14.4*. http://www.sice.oas.org/Trade/COL_USA_TPA_e/Index_e.asp

OAS. (2007, 28 de junio). *Acuerdo de Promoción Comercial Panamá-EUA*. *Artículos 13.4 y 13.17*. http://www.sice.oas.org/Trade/PAN_USA_TPA_Text0607_e/Index_e.asp

OAS. (2008, 29 de mayo). *TLC Canadá-Perú. Artículos 1003 y 1014*. http://www.sice.oas.org/Trade/CAN_PER/CAN_PER_s/CAN_PER_index_s.asp

OAS. (2008, 30 de julio). *TLC Chile-Australia*. *Capítulo 11. Sección C*. http://www.sice.oas.org/Trade/CHL_AUS_Final_e/CHL_AUSind_e.asp

OAS. (2011, 31 de mayo). *Acuerdo de Asociación Económica Japón-Perú. Artículos 117 y 120*. http://www.sice.oas.org/Trade/PER_JPN/EPA_Texts/ESP/Index_PER_JPN_s.asp

OAS. (2011, 20 de noviembre). *TLC Centroamérica-México. Artículos 13.1 y 13.5*. http://www.sice.oas.org/Trade/CACM_MEX_FTA/Index_s.asp

OAS. (2012, 29 de junio). *TLC Centroamérica-UE*. *Artículos 185 y 188*. http://www.sice.oas.org/Trade/CACM_EU/Text_Sept14/Index_e.asp

OAS. (2014, 3 de abril). *TLC México-Panamá*. *Artículos 12.1 y 12.5*. http://www.sice.oas.org/TPD/MEX_PAN/Draft_MEX_PAN_FTA_s/Index_PDF_09.05.2014_s.asp

OMC. (2014a, 7 de agosto). *WT/DS431/AB/R. China- Medidas relacionadas con la exportación de tierras raras, volframio, (tungsteno) y molibdeno*. https://www.wto.org/spanish/tratop_s/dispu_s/cases_s/ds431_s.htm

OMC. (2014b, 7 de agosto). *WT/DS432/AB/R. China- Medidas relacionadas con la exportación de tierras raras, volframio, (tungsteno) y molibdeno.* https://www.wto.org/spanish/tratop_s/dispu_s/cases_s/ds432_s.htm

OMC. (2014c, 7 de agosto). *WT/DS433/AB/R. China- Medidas relacionadas con la exportación de tierras raras, volframio, (tungsteno) y molibdeno.* https://www.wto.org/spanish/tratop_s/dispu_s/cases_s/ds433_s.htm

OAS. (2017, 2 de noviembre). *TLC Argentina-Chile*. *Artículo 10.1*. http://www.sice.oas.org/Trade/ARG_CHL/ARG_CHL_Index_s.asp

OAS. (2018a, 8 de marzo). *The Comprehensive and Progressive Trans-Pacific Partnership (CPTPP). Chapter 14. Electronic Commerce*. *Artícles 14.7, 14.8 and 14.11*. http://www.sice.oas.org/Trade/TPP/Final_Texts/English/TPP_Index_e.asp

OAS. (2018b, 8 de marzo). *The Comprehensive and Progressive Trans-Pacific Partnership (CPTPP). Digital Economy Partnership Agreement (DEPA).* http://www.sice.oas.org/trade/DEPA/DEPA_index_e.asp

Perrone, C., y Strassburger, S. (2018). Privacy and Data Protection. From Europe to Brazil. *Panorama of Brazilian Law*, *6*(9-10), 82-100. https://www.e-publicacoes.uerj.br/pbl/article/view/38253

Satter, R. (2023, 13 de diciembre). *Apple now requires a judge's consent to hand over push notification data*. Reuters. https://www.reuters.com/technology/apple-now-requires-judges-consent-hand-over-push-notification-data-2023-12-12/

UE. (2016, 27 de abril). *Reglamento UE 2016/679 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*. https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html

UE. (2021, 21 de abril). *COM/2021/206 final. Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial y se modifican determinados actos legislativos de la Unión. Exposición de Motivos*. *Numerales 2.3., 5.2.2. y 5.2.3.* https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52021PC0206

UE. (2022, 1 de noviembre). *PE/17/2022/REV/1. Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance)*. http://data.europa.eu/eli/reg/2022/1925/oj

UE. (2022, 16 de noviembre). *Reglamento de servicios digitales*. https://eur-lex.europa.eu/ES/legal-content/summary/digital-services-act.html

UE. (2024, 19 febrero). *Press Release. Commission opens formal proceedings against Tik Tok under the Digital Services Act*. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926

UE. (2024, 13 de narzo). *COM/2021/0206 – C9-0146/2021 – 2021/0106(COD). P9_TA (2024)O138*. *Reglamento de Inteligencia Artificial. Considerandos 12,21,22,31,32,44,54,56,57,58,97,110,123,125,127,168 y 179. Artículos 14 y 50*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=EP%3AP9_TA%282024%290138

UNCTAD. (2019). *Informe sobre la economía digital 2019. Creación y captura de valor: repercusiones para los países en desarrollo* (pp. XV). https://comunidades.cepal.org/elac/es/grupos/discusion/informe-sobre-la-economia-digital-2019-creacion-y-captura-de-valor-repercusiones-6

Varoufakis, Y. (2024). *Tecnofeudalismo. El sigiloso sucesor del capitalismo*. Deusto.

Wakabayashi, D., Bradsher, K., y Fu, C. (2024, 28 de febrero). China amplía la aplicación de la ley de secretos de Estado. *The New York Times*. https://www.nytimes.com/es/2024/02/28/espanol/china-ley-secretos-estado.html

White House of USA. (2024, 28 de febrero). *Fact Sheet: President Biden Issues Executive Order to Protect Americans' sensitive personal data*. https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/

Wiseman, P., y Liedtke, M. (2023, 12 de septiembre). US claims GOOGLE pays more than $10 billion a year to maintain its search dominance. *Portland Press Herald*. https://www.pressherald.com/2023/09/12/its-google-versus-the-u-s-in-the-biggest-antitrust-trial-in-decades/

Zhou, W., Jiang, H. y Chen, Z. (2023). Trade vs. Security: recent developments of global trade rules and China´s policy and regulatory responses from defensive to proactive. *World Trade Review*, *22*(2), 193-211. https://www.cambridge.org/core/journals/world-trade-review/all-issues