¿SOBERANÍA DIGITAL O COLONIALISMO DIGITAL?

Renata Ávila Pinto

• *Nuevas tensiones alrededor de la privacidad, la seguridad y las políticas nacionales* •

RESUMEN

Renata Ávila, guatemalteca, es abogada internacional y defensora de los derechos digitales. Especializada en propiedad intelectual y tecnología, su trabajo se centra en la crucial intersección entre derechos humanos, comercio digital, información, cambio tecnológico y las disparidades de poder entre el Sur y el Norte globales. Como abogada en Guatemala, Ávila representó a indígenas víctimas de genocidio y otros abusos a los derechos humanos, incluida la destacada líder indígena y premio Nobel de la Paz Rigoberta Menchu Tum. Como parte de su larga trayectoria de trabajo de advocacy en el campo de derechos e internet, lidera con el inventor de la World Wide Web, Sir Tim Berners-Lee, una campaña global para mantener los derechos humanos en la era digital en más de setenta y cinco países. Ávila tiene asiento en el consejo de directores de Creative Commons, es consejera de la Courage Foundation –una organización que defiende a testigos en peligro – y es miembro de la junta consultiva de Diem25, que explora el potencial de las tecnologías descentralizadas en Europa. Actualmente vive parte del tiempo en Belgrado y parte en Guatemala, y está escribiendo un libro sobre colonialismo digital, además de asesorar a la Fundación Web en sus nuevas estrategias de Equidad Digital. Ella representa asimismo a la sociedad civil en el Comité de Políticas de Economía Digital de la OCDE.

PALABRAS CLAVE

Vigilancia | Soberanía tecnológica | Colonialismo digital | Software libre | Privacidad | Control de datos | Espionaje económico | Pueblos indígenas

Toda aplicación que pueda ser usada para vigilancia
y control será usada para vigilancia y control
Profesora Shoshana Zuboff[1]

1 • Definiendo el problema: colonialismo digital y pugnas tecnológicas

Un análisis simplista de la situación actual de las tensiones entre privacidad y seguridad (la narrativa que prevalece en los medios) probablemente dirá lo siguiente: los Estados están espiando a los ciudadanos nacionales y extranjeros y la tendencia solo aumentará a medida que adquieran tecnologías más baratas, proporcionales a su poderío militar y tecnológico. El sector privado también lo hace, pero no con intenciones inherentemente malas o propósitos políticos. Lo que busca el sector privado es la "experiencia" del usuario y la máxima captura de sus datos para poder ofrecerle mejores productos y servicios. Los daños colaterales, como el abuso de datos de Facebook por compañías como *Cambridge Analytica*, son la excepción a la regla.[2] En cuanto a las personas, no les preocupa que su gobierno las espíe. Están de alguna manera preocupadas por la vigilancia del sector privado, pero desean autorizarla, especialmente si eso les permite disfrutar de servicios "gratuitos" o mejorar su experiencia en general. Esto se da a pesar de que la consciencia sobre la privacidad está gradualmente aumentando y las reglas se están mejorando levemente en algunas regiones, sobre todo en Europa, por ejemplo después de la entrada en vigor del Reglamento General de Protección de Datos (RGPD), que viene a emparchar una situación sistémica de erosión de la privacidad y extracción abusiva de datos.

Más allá de ese análisis simplista, empero, la situación es más compleja e implica un elemento adicional que es a menudo pasado por alto. El poder de vigilancia y de concentración de los datos reunidos tanto por mecanismos públicos como privados está en manos de un pequeño número de actores, públicos y privados, principalmente bajo una jurisdicción, y llevando una la rápida erosión de la soberanía del Estado y de la democracia.

Nunca antes un pequeño sector había tenido tanto poder sobre el mundo entero, de monitorear los comportamientos presentes y predecir los futuros, no solo de los individuos, sino de poblaciones enteras. El problema es más alarmante si consideramos cómo los sectores público y privado se están uniendo en operaciones conjuntas en un afán de dominación global, de penetrar cada gobierno, cada movimiento ciudadano, mediando cada acción en cada vida de persona conectada a través de dispositivos digitales y recolección de datos.

Las tecnologías de la información y la comunicación (TIC), la innovación en inteligencia artificial y la capacidad de desplegar sistemas e infraestructura rápidamente en mercados emergentes, están concentradas en algunos pocos países, que ahora han entrado en una carrera por ser el número uno.

Dichos países y empresas cuentan con tres elementos que a la mayoría de las naciones en vías de desarrollo e incluso a los países de medianos ingresos les falta. El primero de ellos es el de los recursos, tanto recursos de capital (propiedad y control de cables y servidores, además de datos) como recursos intelectuales (los más avanzados técnicos e instituciones de investigación). El segundo elemento es la actual arquitectura legal doméstica e internacional, que impide a los países pequeños adoptar políticas que favorezcan la producción y la compra de bienes y servicios producidos domésticamente, con la amenaza de procesos legales en cortes internacionales por adoptar medidas anticompetitivas. Eso limita la capacidad de los países en desarrollos y de ingresos medios de investigar e innovar; el actual sistema de patentes y propiedad intelectual restringe artificialmente el intercambio de conocimiento y la capacidad de innovar a pasos avanzados. Tales restricciones solo se incrementarán, con poca posibilidad de reversión del proceso, debido al nuevo grupo de Tratados de Libre Comercio: el Acuerdo Transpacífico de Cooperación Económica (TPP, por sus siglas en inglés), la Asociación Transatlántica para el Comercio y la Inversión (TTIP, por sus siglas en inglés) y el Acuerdo en Comercio de Servicios (TISA, por sus siglas en inglés). Algunas de las disposiciones de la nueva generación de acuerdos llegan a considerar que legislaciones y políticas de privacidad más estrictas en un país constituyen una barrera para el comercio, despreciando la superioridad de los derechos humanos sobre cualquier otra ley.[3]

El tercer elemento, prontamente accesible a solo un grupo de países, es la disponibilidad del capital financiero para experimentar y diseñar nuevos modelos, ya sea mediante fondos públicos, capital de riesgo o alianzas público-privadas. Esos países están invirtiendo pesadamente en investigación y desarrollo, no solo para mantener su posición dominante en la industria y expandirla agresivamente hacia tantos mercados como sea posible, sino también para explorar formas innovadoras de integrar tecnología de la información a todos los aspectos de la administración pública, del sector privado, su defensa y seguridad y la aplicación de los derechos de los ciudadanos.

El escenario es radicalmente diferente para los países en desarrollo, donde la austeridad es la norma, y donde la desigualdad digital pronto será un problema visible, incluyendo brechas de educación e investigación que llevarán a una absoluta dependencia tecnológica. Estos países representan un terreno relativamente fácil de dominar y hay una carrera para hacerlo a través de compañías de tecnología, particularmente entre los Estados Unidos de América (EE.UU) y China, mientras Europa va rezagada y sus compañías luchan para competir con sus contrapartes estadounidenses y asiáticas.

De esta manera, las poblaciones del mundo que todavía están desconectadas son el territorio en disputa de los imperios tecnológicos, porque quienes logren integrarlos a su feudalismo digital tendrán la llave para el futuro. Los gigantes tecnológicos están, sin lugar a dudas, influenciando fuertemente la manera en que las campañas, los gobiernos y las políticas operan.

También influencian a la política para establecer normas globales que sirvan a sus modelos de negocio,[4] cada vez más basados en la obtención y monitoreo de datos,

y en la identificación de patrones – inevitablemente minando la privacidad de muchas personas. Más allá de Bruselas[5] y Washington, los gigantes tecnológicos están actualmente dedicados a invertir agresivamente en áreas que tradicionalmente pertenecían al Estado o a otras agencias o proveedores especializados. Ahora dos compañías de tecnología de California (Facebook y Google), un gigante espacial de California (SpaceX) y una compañía de satélite de Nueva Jersey (OneWeb) están comprometidas en carreras aceleradas para conectar a los desconectados.[6] Estas empresas están ofreciendo infraestructura fundamental a los ciudadanos a cambio de sus datos personales y de que se conviertan en recibidores potenciales de publicidad. En la mayoría de los países, ni el gobierno ni los inversionistas privados pueden competir con la velocidad y recursos de estas grandes corporaciones para proveer conectividad en áreas sub-atendidas.

Estas empresas, una de las cuales usualmente representa la primera experiencia digital de los usuarios, a menudo combinan sus programas con la provisión de hardware, software y contenido limitado, no dejando a los ciudadanos o al Estado mucha opción. Nuevos usuarios normalmente se sujetan a acuerdos privados de largo plazo, que permiten a las entidades pleno acceso a cualquier dato de esos usuarios. Esto se ve agravado por el hecho de que estamos hablando en general de territorios con protección limitada o nula a los datos y a la privacidad. Los contratos también suelen contener severas cláusulas de penalidad en caso de incumplimiento. Esta situación permite nuevas y encubiertas formas de explotación y subordinación.

Los programas de digitalización rápida se apoyan fuertemente en las tecnologías móviles para conectar a nuevos usuarios en la crecientemente comercializada Web. Este abordaje difiere de los programas iniciales, como "Una laptop por niño", que defendían el desarrollo de capacidades creativas y alfabetización a los pobres para que fueran completamente capaces de desarrollar sus habilidades de codificar, crear hardware y hasta entender de robótica.[7] Esos primeros programas contrastan con los actuales, que solamente permiten a los usuarios acceder a un conjunto previamente instalado de sitios web, inhiben cualquier capacidad de creación – ya que solo es posible hacer lo que permite un teléfono móvil. Además, aumentan el riesgo de vigilancia y elaboración de perfiles de las poblaciones menos favorecidas, porque los teléfonos celulares en muchos países están ligados a una tarjeta SIM registrada.[8] El monitoreo y monetización de todas las actividades en línea de los usuarios es la principal motivación de los esfuerzos cuasi filantrópicos para conectar a los siguientes mil millones, y por ende obtener sus datos. Los datos de los usuarios son la materia prima básica para el aprendizaje automático y la inteligencia artificial, cuando se los combina con los sofisticados algoritmos y el poder computacional de los concentrados conglomerados tecnológicos.

En la mayoría de los casos, las actuales políticas de conectividad por parte de actores corporativos externos – así como algunas caridades internacionales asociadas o cercanas a las compañías de telecomunicaciones o de tecnología – desconsideran el poder creativo y la autonomía de las personas o de la comunidad local. Los dispositivos,

software y hardware son frecuentemente diseñados para el consumo personal, en lugar de la creación o usos colectivos. Todos los programas actúan con urgencia para conectar a tantas personas como sea posible, lo más rápido posible, desatendiendo a consideraciones como contenido, sostenibilidad de largo plazo o conocimiento básico sobre algunos puntos como privacidad y seguridad en línea. Cuando la infraestructura básica es provista por otro, es difícil implementar o hacer cumplir mejoras en términos de privacidad, dado que la infraestructura y el equipamiento son a menudo diseñados para servir a los propósitos de los países donde la vigilancia masiva es la norma.[9] En su artículo "Dark Google",[10] la profesora Shoshana Zuboff explica las razones por detrás de la prisa en conectar a los pobres globales de una forma particular. Ella también advierte sobre los peligros de las puertas giratorias entre las mayores compañías y sus gobiernos, que permiten usar la tecnología para obtener ventajas geopolíticas:

> *Google, Facebook y otros se volcaron a un modelo de publicidad que requería la captura encubierta de los datos de los usuarios como la moneda para la venta de publicidad. Los réditos prontamente se materializaron y motivaron una obtención de datos aún más despiadada y determinada. Explotó la nueva ciencia de la minería de datos, impulsada en parte por el éxito espectacular de Google.*[11]

Hay experimentos que ya se están realizando en esa dirección. Por ejemplo, durante el último gobierno de izquierda en Argentina, YCombinator,[12] un fondo de capital de riesgo, financió y fundó un nuevo partido político de oposición, una situación que en 2018 podría causar un escándalo sin precedentes, y hoy pone de manifiesto que la tecnología tiene el potencial de alterar la política. El experimento no fue exitoso – el partido en cuestión ya no sigue como partido político registrado – pero demuestra las posibilidades de la intervención del Valle del Silicio en la política extranjera. El caso Zunzuneo en Cuba mostró cómo los gobiernos dependen cada vez más de la industria de tecnología para presionar por una nueva forma de intervención.[13] Y luego el escándalo de *Cambridge Analytica*, sacudiendo a las democracias occidentales desde inicios de 2018, simplemente confirmó que ni el país más poderoso del mundo está inmune a tales intervenciones.[14]

De hecho, no es solo un problema de los países menos desarrollados y más desconectados. De forma creciente, los gobiernos de medianos ingresos se están comprometiendo activamente con las empresas para asistirlas en la supresión de ciertas formas de discurso que consideran una amenaza para la seguridad de sus países. El discurso legítimo viene siendo monitoreado y suprimido si la plataforma en la cual se publica el material coincide con el gobierno acerca de que tal contenido el perjudicial, incluso si el material fue producido fuera o iba dirigido a distintos públicos[15] (Como ejemplos, ver Proyecto Censura en Línea: https://onlinecensorship.org.). Asimismo, los gobiernos son cada vez más víctimas de ataques a sus sistemas, activos o individuos clave, como en el reciente ataque al software patentado en la red eléctrica en Ucrania[16] o el ataque calculado de las cuentas de funcionarios de alto rango de varios países de América Latina.[17]

Naciones enteras y sus industrias son completamente dependientes de infraestructura básica, software y hardware provistos por un puñado de empresas con sede en un pequeño grupo de países. Casi todas las actividades son mediadas por nuestra interacción con las tecnologías y servicios ofrecidos por un conglomerado cada vez más concentrado. Si se observa el caso del software y el hardware, es crecientemente alarmante, y es uno de los temas más urgentes de tratar al discutir la seguridad de nuestra infraestructura de información y comunicación.

Pese a las recientes revelaciones sobre las posibilidades y prácticas de las agencias de inteligencia, son pocos los líderes globales (cuya totalidad es consciente del problema) que están tomando algunas medidas reales de solución que apunten a hacer respetar los derechos humanos universales, que sean compatibles con un mundo global e interconectado, y además sean asequibles, confiables y se puedan aplicar en escala. Es más, cualquier intento en esa dirección es precipitadamente rotulado como fragmentación o balcanización del internet.

La mayor parte de los elementos que permiten a cualquier individuo, empresa o gobierno conectarse a internet están concentrados en la jurisdicción de California. Casi todas las compañías proveedoras son estadounidenses, con mayoría de capital estadounidense. En un ambiente geopolítico conturbado, esa concentración de las compañías de tecnología podría resultar en una legal pero ilegítima suspensión de productos y servicios a un gobierno extranjero o a industrias clave en otro país.[18]

Las organizaciones comerciales son susceptibles a la presión política – como lo ha probado el caso de *WikiLeaks* cuando Visa, MasterCard, American Express, Western Union y PayPal bloquearon los pagos a la organización.[19] Las defensas al consumidor son débiles y caras de aplicar y, hasta para los ciudadanos de la Unión Europea, a menudo no hay remedio en tales circunstancias, tal como fue el caso para *WikiLeaks*[20] y también durante la crisis en Cataluña en 2017.[21] Cuando se trata de gobiernos, las sanciones pueden interrumpir severamente las actividades del día a día. La dependencia de ciertas tecnologías para manejar la administración pública es generalizada, en la medida en que pocas compañías en el mundo, situadas en poquísimos países, cumplen con los requisitos para proveer a los gobiernos los software y hardware que necesitan para conducir los asuntos públicos a un precio asequible que quepa en las reglas de compras públicas, cada vez más uniformes, en general favorables a la opción de menor precio. El resultado es un escenario en el cual los gobiernos son fuertemente dependientes de un pequeño grupo de proveedores para su infraestructura clave – proveedores que son generalmente susceptibles a órdenes secretas, presión política y suspensión de servicios en función de sanciones. El tema es que, si intentan sustituir un proveedor a favor de un proveedor local que pueda ofrecer un precio más bajo, los gobiernos sufren severas penalidades.

A medida que la tecnología avanza en la penetración de las actividades principales de cada una de las áreas de los gobiernos, estos se vuelven más vulnerables que nunca, dependiendo de infraestructura clave que no controlan. Cualquier gobierno, local o nacional, es ciertamente menos libre cuando el mercado es "libre", aunque en realidad es dominado por

cuasi monopolios.[22] Cuando discutimos tecnologías digitales en escala masiva, encontramos un conjunto de compañías que se beneficiaron de subsidios y financiación pesada de un gobierno que dominaba y sigue dominando las reglas del comercio internacional.[23] Estas reglas erosionan severamente la libertad de las oficinas de compras públicas, impidiéndoles tanto elegir alternativas locales más caras como subsidiar sus propias industrias locales.

La dependencia de la tecnología extranjera solo aumenta cuando se trata de infraestructuras clave. El 14 de abril de 2008, Microsoft anunció[24] que ya no ofrecería actualizaciones de seguridad para su sistema operativo Windows XP. El anuncio dejó a miles de sistemas estatales completamente vulnerables, porque dependían de ello para operar infraestructura clave, tal como el sistema de ingreso en la frontera de un país latinoamericano. Mientras una situación similar en el ambiente físico – una frontera llena de agujeros o controles débiles – probablemente acarrearía la convocación de una investigación parlamentaria, el bajo nivel de conciencia sobre la importancia de las infraestructuras tecnológicas cruciales permitió que este tema se mantuviera sin solución durante meses.

Varios gobiernos dependen de infraestructuras de comunicaciones completamente situadas en la nube (en centros de datos que están en el extranjero bajo leyes extranjeras). Es más, son servicios provistos bajo términos de uso en constante cambio y suspensión de servicios arbitraria. El problema no es solo la dependencia de un proveedor extranjero o de leyes extranjeras para los datos digitales; el problema es también la ausencia de políticas públicas a cargo de la cuestión en todos los niveles. La situación de dominación digital, cercana al colonialismo, aún no se ha incluido entre las prioridades de la agenda política global. Casi 40 años después de la invención del internet, la capacidad de los políticos y líderes sociales de comprender las dimensiones del problema todavía queda corta.

2 • Explorando espacios de resistencia y de soberanía tecnológica

América Latina guió los primeros pasos hacia la soberanía digital a principios de los años 2000. Algunos países tomaron las medidas adecuadas que les permitirían estar listos para sustituir a los proveedores extranjeros con sus pares locales. Aunque en la India el uso de software de código abierto por parte del Estado es obligatorio desde 2005,[25] países latinoamericanos como Brasil[26] y Venezuela[27] (Decreto No. 3.390 2004) fueron aún más adelantados, aprobando leyes en 2004 que establecían la migración al software libre de los datos gubernamentales. Iniciativas similares se siguieron en Ecuador (Decreto No. 1014 2008),[28] Uruguay[29] (Ley No. 19.179 2013) y Bolivia[30] (Decreto Supremo No. 1793 2013). En todos estos países, el giro estuvo combinado con estrategias para aumentar el conocimiento de manejo de software libre entre niños/as de la escuela primaria, desarrollando proyectos como el Plan Ceibal en Uruguay y Canaima en Venezuela. Los países latinoamericanos tenían suficiente capacidad técnica para producir domésticamente al menos parte del software que necesitaban, incluso exportando alguna producción, mientras simultáneamente invertían en construir capacidades. Como forma de contornar

el embargo estadounidense, Cuba desarrolló su propio sistema operativo, Nova. Cuba lo hizo no solo a causa del embargo, sino también como una manera de controlar sus propios sistemas. Tal adopción era vital, visto que el país tiene restricciones de acceso a licencias de software y actualizaciones de seguridad ofrecidas por los mayores proveedores. La total migración al software libre ha sido anunciada por Rusia recientemente, como forma de anticiparse al impacto de las actuales y próximas sanciones.[31]

Pero solo adoptar el software libre no es suficiente para que un Estado logre construir una política que garantice la soberanía tecnológica sobre sus comunicaciones. Al intentar reemplazar al propietario o a las opciones dominantes, las iniciativas de gobiernos y comunidades están encontrando crecientes desafíos para cumplir con las expectativas de los usuarios, en términos tanto de velocidad como de calidad de la experiencia del usuario. La sostenibilidad también cuenta entre los desafíos, al igual que alcanzar la adopción masiva, salvo que se determine por ley y su implementación sea financiada como política pública, como en el Plan Ceibal, en el cual todo el sistema de educación migró al software (y hardware) de código abierto. En lo que concierne a hardware y equipamientos, un grupo de médicos está desarrollando impresoras 3D para proveer estetoscopios a los hospitales de Gaza afectados por los bloqueos israelíes.[32] Modelos similares a estos podrían ser explorados por otros países que permanecen dependientes de otros Estados para equipamientos cruciales. Desarrollar nuevos modelos que favorezcan la producción nacional resulta particularmente importante después de las numerosas revelaciones de implantes y agujeros de seguridad permitidos por proveedores extranjeros para posibilitar el espionaje extranjero, comprometiendo la seguridad de los usuarios.[33]

El académico indio Sunil Abraham también apunta en esa misma dirección, destacando la importancia de desarrollar tecnologías que lleven en cuenta los derechos humanos en su diseño e incluyan un código que no pueda ser restringido por leyes de propiedad intelectual o usado como herramienta de resistencia contra ciertas leyes, lo que llevaría a nuevas tensiones. Abraham describe cómo "el código podría ser usado para resistir a la regulación por la ley, convirtiendo así tanto el software como el hardware de los dispositivos y redes en un campo de batalla por soberanía entre el hacker de software libre y el Estado."[34]

A medida que las personas alrededor del globo ganan acceso a la tecnología personal más sofisticada que han conocido desde el televisor, una nueva generación de desarrolladores y creadores está emergiendo. La próxima generación de tecnologías, producida fuera de los gigantes de la tecnología, debe traer las soluciones que estamos buscando, dado que son diseñadas, desarrolladas y distribuidas teniendo en cuenta un conjunto diferente de valores, comportamientos y dinámicas sociales. Pero tal poder creativo puede ser bloqueado si no revertimos la actual dirección de la arquitectura tecnológica que restringe la creatividad más que posibilitarla y que alienta el consumo y centraliza el poder.

Una vez que la autonomía tecnológica es alcanzada, los individuos y comunidades pueden incorporar sus principios de la forma que elijan para comunicarse. Como declararon los

pueblos indígenas maoríes al considerar la necesidad urgente de la población indígena de desarrollar su propia política de TIC: "…el reemplazo deliberado de las tecnologías locales por tecnologías cargadas de valores eurocéntricos y conducidas por la ganancia ha formado parte de la agenda colonizadora durante muchos siglos".[35]

La innovación constante también juega un papel en la resistencia y protección contra la dominación tecnológica. Pensar más allá del mercado es algo que las naciones desarrolladas ya están haciendo. Como afirma Francesca Bria:

> *Formas alternativas de propiedad pública y común para las plataformas ayudará a crear una economía más democrática, que trascienda la lógica del mercado, de la búsqueda de ganancia, de los sistemas de red privatizados. Muy a menudo todo esto último lleva a decisiones basadas en el cortoplacismo, la extracción de valor y la apropiación de los recursos comunes para rédito privado. Se necesita un abordaje de mucho más largo plazo para la tecnología, la economía y la política cuando los recursos y activos públicos son poseídos, administrados y distribuidos para el bien colectivo. De esta tarea se trata construir la democracia del siglo XXI.*[36]

Para los países de bajos y medianos ingresos que todavía siguen luchando para captar el potencial de las nuevas tecnologías – y al mismo tiempo evitar las violaciones de los derechos de sus ciudadanos – hay una gama de opciones que deben empezar a ser desplegadas con urgencia. La mayoría de estas opciones existe en la forma de compromiso nacional y regional de mediano a largo plazo en múltiples niveles e implicando una colaboración fluida entre gobiernos, ciudadanos y compañías nacionales. En el nivel constitucional, los países deben asegurar que mantendrán la capacidad de legislar y regular las nuevas tecnologías y su impacto en los derechos fundamentales de sus ciudadanos. Las constituciones deben ser reformadas de modo tal que no permitan el involucramiento del ejecutivo en compromisos internacionales que quiten al gobierno su capacidad de hacer cumplir los derechos internamente. Las constituciones deben garantizar también que el Estado ejerza autonomía y control sobre las infraestructuras de tecnología cruciales[37] y sobre las posiciones clave[38] en importantes activos e industrias.

Paralelamente, también es necesario desarrollar una estrategia fundada en el Estado para la soberanía digital. Esta debe cubrir todos los aspectos, entre ellos la modificación de los planes de estudios a fin de desarrollar los recursos humanos necesarios para los próximos 50 años; la inversión pesada en fondos como CAPS y otras iniciativas de investigación y desarrollo para que experimentos locales sean llevados a cabo; tener en cuenta las necesidades específicas, capacidades y visión de cada país; inversión proactiva de recursos en aplicaciones sociales de la tecnología. Se podrían fomentar y financiar asimismo el intercambio de capacidades, información e investigación con el Sur global.

Mientras tanto, la simple regulación de normas abiertas, software libre, hardware abiertamente disponible y transparencia de algoritmos podría ser desarrollada, al menos para las prácticas y compras estatales. Bolivia lo hizo recientemente,[39] bajo el liderazgo de la vicepresidenta de origen indígena del Parlamento boliviano, Nelida Sifuentes, asesorada por Richard Stallman.[40] Derechos iguales para todos y soluciones efectivas contra la vigilancia de masas para los ciudadanos del Sur global solo serán alcanzados con cambios políticos y tecnológicos hacia la autonomía y la soberanía, que sean amplios, de largo plazo y con presupuesto adecuado. Eso dará paso, gradualmente, a una cultura de la dignidad digital con normas basadas en derechos humanos incorporadas a los protocolos a nivel regional e internacional.

3 • Conclusión

Es necesario, por lo tanto, que los líderes globales – especialmente aquellos que defienden la igualdad y la justicia social – tomen consciencia de los peligros representados por la rápida mercantilización digital para los pueblos vulnerables del mundo y sus impactos sobre la democracia y la dignidad.

Como advierte el investigador Dan Schiller:

> *Para la mayoría de los pueblos del mundo, si el crecimiento rentable para el capital debe ser renovado y por parte de quién es de lejos menos importante que las consecuencias de la mercantilización digital para el empleo, la explotación y la desigualdad; para el porvenir del autogobierno democrático, para el medio ambiente devastado; y para el carácter y la calidad de los servicios culturales necesarios para mantener vidas cargadas de sentido. Los choques de la mercantilización digital están escribiendo un nuevo capítulo en la larga historia de dislocaciones violentas del capitalismo. Esto hace que la discusión de estrategias para alternativas sociales sea esencial y, de hecho, urgente.*[41]

Para empezar a solucionar las desigualdades digitales globales y abrazar un futuro que tenga a la autonomía digital y la dignidad humana en el centro, la innovación social debe ser alentada e institucionalizada a nivel ciudadano y de la comunidad, para asegurar su permanencia y reproducción en escala. Comunidades lingüísticas y autónomas deben ser fomentadas a desarrollar su propia tecnología y contenido digital y a preservar y exportar sus culturas al ambiente digital. Deben establecerse políticas públicas que garanticen que la adopción de nuevas tecnologías en escala masiva no cree más desigualdad, exclusión o la imposición de prácticas y valores extranjeros a las comunidades receptoras. En lugar de eso, podría ser una oportunidad para rescatar y desarrollar más conocimiento local. Enraizadas en lo local, en la descentralización y en la lógica del patrimonio digital común: esas son las características de las políticas que van a derrotar al colonialismo digital.

NOTAS

1 • Shoshanna Zuboff, "Dark Google." Frankfurter Allgemeine Zeitung, 30 de abril de 2014, visitado el 18 de enero de 2016, http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshanna-zuboff-dark-google-12916679.html.

2 • Carole Cadwalladr y Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." The Guardian,17 de marzo de 2018, visitado el 20 de junio de 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

3 • Michael Geist, "How the TPP Puts Canadian Privacy at Risk." Michael Geist website, 14 de octubre de 2015, visitado el 18 de enero de 2016, http://www.michaelgeist.ca/2015/10/how-the-tpp-puts-canadian-privacy-at-risk/; see also Tyler Orton, "From IP to Privacy — Why TPP is 'Potentially Dangerous' for B.C. Tech Sector." Business Vancouver,17 de noviembre de 2015, visitado el 18 de enero de 2016, https://www.biv.com/article/2015/11/trade-deal-potentially-dangerous-bc-tech-sector.

4 • James Fontanella-Khan, "Brussels: Astroturfing Takes Root." Financial Times, 26 de junio de 2013, visitado el 20 de junio de 2018, https://www.ft.com/content/74271926-dd9f-11e2-a756-00144feab7de; Nancy Marshall-Genzer, "Why US Tech Lobbyists Have Descended on Brussels." Marketplace, 11 de agosto de 2014, visitado el 20 de junio de 2018, https://www.marketplace.org/2014/08/11/world/why-us-tech-lobbyists-have-descended-brussels.

5 • Tony Romm, "Tech Giants Get Deeper Into D.C. Influence Game." Politico, 1 de enero de 2015, visitado el 20 de junio de 2018, http://www.politico.com/story/2015/01/tech-lobby-apple-amazon-facebook-google-114468#ixzz3wV2vx4H0.

6 • Tim Cross, "Connecting the World: Four Firms Hope to Bring Internet Access to Everybody." The World in 2016, 6 de noviembre de 2015, visitado el 18 de enero de 2016, http://www.theworldin.com/article/10646; las empresas son Google, Facebook, SpaceX y OneWeb.

7 • Anna Heim, "Uruguay's One Laptop Per Child Program: Impact and Numbers." TNW News, 17 de abril de 2013, visitado el 18 de enero de 2016, http://thenextweb.com/la/2013/04/07/uruguays-one-laptop-per-child-program-impact-and-numbers.

8 • Mohammed Lubowa, "Invasion Of Privacy: The Legal Implications of Mandatory SIM Card Registration on Mobile Users in Uganda." Master Thesis, 2013, visitado el 20 de junio de 2018, https://www.duo.uio.no/handle/10852/38120.

9 • "The Problem with Cell Phones," Electronic Frontier Foundation, 15 de febrero de 2015, visitado el 18 de enero de 2016, https://ssd.eff.org/en/module/problem-mobile-phones.

10 • Zuboff, "Dark Google." 2014.

11 • *Ibid.*

12 • Max Chafkin, "Why YCombinator Funded a Radical Political Party in Argentina." Fast Company,12 de marzo de 2015, visitado el 18 de enero de 2015, http://www.fastcompany.com/3043388/the-y-combinator-chronicles/why-y-combinator-funded-a-radical-political-party-in-argentina.

13 • Associated Press, "US Secretly Created 'Cuban Twitter' to Stir Unrest and Undermine Government." The Guardian, 3 de abril de 2014, visitado el 20 de junio de 2018, http://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest.

14 • Cadwalladr and Graham-Harrison, "Revealed..." 2018.

15 • Para diferentes ejemplos vea: Online Censorship Project, Homepage, 2018, visitado el 20 de junio de 2018, https://onlinecensorship.org/.

16 • Nick Buckley and Hanna Kuchler, "Hackers Shut Down Power Grid in Ukraine." Financial Times, 5 de enero de 2016, visitado el 20 de junio de 2018,

http://www.ft.com/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html.

17 • Claudio Guarnieri, John Scott-Railton, Morgan Marquis-Boirey Marion Marschalek, "Packrat: Seven Years of a South American Threat Actor." Citizen Lab, 8 de diciembre de 2015, visitado el 20 de junio de 2018, https://citizenlab.org/2015/12/packrat-report/.

18 • See Yochai Benkler, "WikiLeaks and the PROTECT-IP Act: A New Public-Private Threat to the Internet Commons," *Dœdalus*140, no. 4 (2011): 154-64, visitado el 18 de enero de 2016, http://benkler.org/WikiLeaks_PROTECT-IP_Benkler.pdf.

19 • Parmy Olson, "Has Western Union Snubbed WikiLeaks?" Forbes, 10 de diciembre de 2010, visitado el 20 de junio de 2018, http://www.forbes.com/sites/parmyolson/2010/12/29/has-western-union-snubbed-wikileaks.

20 • Don Reisinger, "Credit Card Companies' WikiLeaks Block Just Fine, EU Says." CNET.com, 27 de noviembre de 2012, visitado el 18 de enero de 2016, http://www.cnet.com/uk/news/credit-card-companies-wikileaks-block-just-fine-eu-says.

21 • Sam Jones, "Catalan Leaders Compare Spain to North Korea After Referendum Sites Blocked". The Guardian, 27 de septiembre de 2017, visitado el 20 de junio de 2018, https://www.theguardian.com/world/2017/sep/27/catalans-compare-spain-to-north-korea-after-referendum-sites-blocked.

22 • Christopher Williams, "Google Charged with Monopoly Abuse." The Telegraph,15 de abril de 2015, visitado el 20 de junio de 2018, http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/11537546/Google-charged-with-monopoly-abuse.html.

23 • Bruce Upbin, "Debunking the Narrative of Silicon Valley's Innovation Might." Forbes, 13 de junio de 2013, visitado el 18 de enero de 2016, http://www.forbes.com/sites/bruceupbin/2013/06/13/debunking-the-narrative-of-silicon-valleys-innovation-might.

24 • "Your Windows XP Computer Isn't as Secure as it Used to Be," Microsoft, [n.d.], visitado el 18 de enero de 2016, http://www.microsoft.com/windows/en-us/xp/default.aspx.

25 • Eileen Yu, "Indian Government Mandates Use of Open Source Software." ZDNet, 31 de marzo de 2015, visitado el 18 de enero de 2016, http://www.zdnet.com/article/indian-government-mandates-use-of-open-source-software.

26 • Todd Benson, "Brazil: Free Software's Biggest and Best Friend." The New York Times,29 de marzo de 2005, visitado el 20 de junio de 2018, http://www.nytimes.com/2005/03/29/technology/brazil-free-softwares-biggest-and-best-friend.html.

27 • En Venezuela, se aprobó un decreto en 2004 que declara el software libre y los estándares abiertos como el valor predeterminado para la administración pública, "Decreto 3390," Software Libre, 2004, visitado el 20 de junio de 2018, http://www.softwarelibre.gob.ve/images/stories/leyes/decreto3390softwarelibre.pdf.

28 • "Decreto 1014," Esteban Mendieta, 2008, visitado el 20 de junio de 2018, http://www.estebanmendieta.com/blog/wp-content/uploads/Decreto_1014_software_libre_Ecuador.pdf

29 • "Ley 19179," Parlamento Del Uruguay, 2014, visitado el 20 de junio de 2018, www.parlamento.gub.uy/leyes/ley19179.htm.

30 • "Plan de Implementación de Software Libre y Estándares Abiertos 2015-2022," Comité Plurinacional de Tecnologías de la Información y Comunicación – COPLUTIC, Bolivia, agosto de 2015, visitado el 20 de junio de 2018, http://coplutic.gob.bo/IMG/pdf/propuesta_plan_de_implementacion_de_software_libre_y_estandares_abiertos.pdf.

31 • Adrian Offerman, "Russia to Replace Proprietary Software with Free Software." Joinup, 23 de junio de 2015, visitado el 20 de junio de 2018, https://joinup.ec.europa.eu/community/osor/news/russia-replace-proprietary-software-open-source.

32 • Kashmira Gander, "Gaza Doctor Tarek Loubani Creates 3D Printed Stethoscopes to Alleviate Medical Supply Shortages Caused by Blockade." The Independent, 10 de septiembre de 2015, visitado el

20 de junio de 2018, http://www.independent.co.uk/news/world/middle-east/gaza-doctor-tarek-loubani-creates-3d-printed-stethoscopes-to-alleviate-medical-supply-shortages-10495512.html.

33 • Glenn Greenwald, "How the NSA Tampers with US-made Internet Routers." The Guardian, 12 de mayo de 2014, visitado el 20 de junio de 2018, http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

34 • Sunil Abraham, "The Fight for Digital Sovereignty," *Economic & Political Weekly* XLVIII, no. 42 (October 19, 2013), visitado el 18 de enero de 2016, http://cis-india.org/a2k/blogs/epw-vol-xlviii-42-october-19-2013-sunil-abraham-the-fight-for-digital-sovereignty.

35 • Tania Wolfgramm, "Re-Claiming our Technological Sovereignty." Planet Maori, 2015, visitado el 20 de junio de 2018, http://planetmaori.com/Files/Content/2015/Re-Claiming_our_Technological_Sovereignty_-_Paper_-_Tania_Wolfgramm_2014.pdf.

36 • Francesca Bria, *Public Policies for Digital Sovereignty* (New York: OR Books, 2015).

37 • Jonathan Watts, "NSA Accused of Spying on Brazilian Oil Company Petrobras." The Guardian, 9 de septiembre de 2013, visitado el 18 de enero de 2016, http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

38 • AFP, "NSA Spied on French Economy Ministers, Top Companies: Reports." Yahoo! News, 30 de junio de 2015, visitado el 18 de enero de 2016, http://news.yahoo.com/nsa-spied-french-economy-ministers-top-companies-reports-061342870.html; ver tambiénSpiegel Staff, "Embassy Espionage: The NSA's Secret Spy Hub in Berlin." Spiegel Online, 27 de octubre de 2015, visitado el 18 de enero de 2016, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

39 • "Plan de Implementación de Software Libre y Estándares Abiertos," Comité Plurinacional de Tecnologías de la Información y Comunicación - COPLUTIC, Bolivia, julio de 2016, visitado el 20 de junio de 2018, http://coplutic.gob.bo/rubrique3.html.

40 • "Free Software Designer in Bolivia," Prensa Latina, 1º de abril de 2013, visitado el 18 de enero de 2016, http://www.ssig.gov.my/blog/2013/04/01/free-software-designer-in-bolivia.

41 • Dan Schiller, "Geopolitics and Economic Power in Today's Digital Capitalism." Presentation to the Hans Crescent Symposium, 13 de diciembre de 2015, visitado el 20 de junio de 2018, http://informationobservatory.info/2015/12/14/geopolitics-and-economic-power-in-todays-digital-capitalism.

RENATA ÁVILA PINTO – *Guatemala*

Renata Ávila, guatemalteca, es abogada internacional y defensora de los derechos digitales. Especializada en propiedad intelectual y tecnología, su trabajo se centra en la crucial intersección entre derechos humanos, comercio digital, información, cambio tecnológico y las disparidades de poder entre el Sur y el Norte globales. Como abogada en Guatemala, Ávila representó a indígenas víctimas de genocidio y otros abusos a los derechos humanos, incluida la destacada líder indígena y premio Nobel de la Paz Rigoberta Menchu Tum. Como parte de su larga trayectoria de trabajo de advocacy en el campo de derechos e internet, lidera con el inventor de la World Wide Web, Sir Tim Berners-Lee,una campaña global para mantener los derechos humanos en la era digital en más de 75 países. Ávila tiene asiento en el consejo de directores de Creative Commons, es consejera de la *Courage Foundation* – una organización que defiende a testigos en peligro – y es miembro de la junta consultiva de Diem25, que explora el potencial de las tecnologías descentralizadas en Europa. Actualmente vive parte del tiempo en Belgrado y parte en Guatemala, y está escribiendo un libro sobre colonialismo digital, además de asesorar a la Fundación Web en sus nuevas estrategias de Equidad Digital. Ella representa asimismo a la sociedad civil en el Comité de Políticas de Economía Digital de la OCDE.

contacto: *renata.avila@webfoundation.org*

Recibido en mayo de 2018.
Original en inglés. Traducido por Celina Lagrutta.