3

Vector de esperanza, fuente de miedo

POR ROBERTO BISSIO, SOCIAL WATCH

La Agenda 2030 refleja entusiasmo con el "gran potencial" de la tecnología de la información y las comunicaciones y de la interconexión global para acelerar el progreso humano. Sin embargo, la ONU reconoce ahora "el lado oscuro de la innovación" y las amenazas a la seguridad cibernética, los riesgos para el empleo y los peligros a la privacidad desencadenados por la inteligencia artificial y el uso militar de "cyber operaciones" y cyber-ataques.

Al igual que con el cambio climático, el aumento de las desigualdades o la concentración de poder, estos desafíos no pueden ser resueltos por ningún país por si solo y requieren urgentemente un multilateralismo fortalecido.

Al mismo tiempo, es necesario un cambio tecnológico importante para implementar la transición global -requerida por la Agenda 2030- hacia modelos de desarrollo económico y social menos intensivos en recursos y más resilientes. Tales tecnologías ya existen, pero se necesitan nuevas estrategias para generalizarlas a nivel global.

"La tecnología está transformando la forma en que vivimos y trabajamos -desde la bioingeniería hasta la biología sintética, la inteligencia artificial, el análisis de datos y muchos otros aspectos", reconoció el Secretario General de las Naciones Unidas António Guterres en un discurso reciente.[1] Sin embargo, Guterres explicó que "así como la tecnología es un vector de esperanza, también es una fuente de miedo".

Al reconocer esto, Guterres instó a los Estados miembros a "abordar el lado oscuro de la innovación". Esto es un cambio significativo, ya que hasta ahora las nuevas tecnologías solo aparecían en el discurso oficial sobre el desarrollo sostenible como encarnación del progreso y generadores de optimismo.

Guterres dejó claro que estos temas no están aislados, ya que "después de todo, mientras nos aferremos a un modelo económico y social que impulsa la exclusión y la destrucción ambiental, la gente muere, se pierden oportunidades, se siembran las semillas de la división y los conflictos futuros y la fuerza total del cambio climático se vuelve cada vez más amenazante".

Esos son conceptos profundos y notablemente francos que van más allá del entusiasmo habitual sobre la innovación. En 2015, la Agenda 2030 adoptada al más alto nivel por los Estados miembros de la ONU declaró que "la difusión de la tecnología de la información y las comunicaciones y la interconexión global tiene un gran potencial para acelerar el progreso humano, cerrar la brecha digital y desarrollar sociedades del conocimiento, como lo hace la innovación científica y tecnológica en áreas tan diversas como la medicina y

1 Naciones Unidas (2018).

la energía".[2] Simultáneamente, un informe conjunto del Earth Institute de la Universidad de Columbia y la empresa sueca de telecomunicaciones Ericsson concluyó que "en esencia, las TIC (tecnologías de in formación y comunicaciones) tecnologías transformadoras, que permiten a los países 'saltar como sapos' (leapfrog) para cerrar muchas brechas tecnológicas a una velocidad récord".[3] Ni una palabra sobre los peligros potenciales, mientras que ahora" las desventajas de la marcha inexorable de la tecnología se están volviendo claras" hasta el punto de que algunos analistas consideran que el "neoludismo" está emergiendo.[4]

La mitad de la humanidad NO está en línea

Recuadro 3.1

Si la difusión de las TIC solo trae cosas buenas, no hay necesidad de regular estas tecnologías y la única pregunta es cómo acelerar su expansión para que todos puedan beneficiarse. Así, en el ODS 9 sobre industrialización e innovación, la meta 9.c se propone "aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos desarrollados para 2020".

Esta formulación es un poco incómoda. Parece implicar que habrá una cobertura mundial completa para 2020, si hasta los países más pobres tienen acceso universal para entonces. Pero dado que la mayoría de las personas que viven en la pobreza son ciudadanos de países del G20, la previsión de Cisco es que para 2020 solo la mitad de la población mundial estará en línea (4,1 mil millones de usuarios de Internet, de una población total de 8 mil millones). Para esa fecha, la cantidad de dispositivos conectados habrá superado los 26 mil millones, gracias a la rápida expansión del "Internet de las cosas".[1]

1 Cisco (2017).

Manos libres...

Internet comenzó en la década de 1970 como un proyecto de investigación financiado principalmente por el Departamento de Defensa y la National Science Foundation, ambos de Estados Unidos. En 1995, el gobierno de los Estados Unidos anunció que estaba terminando sus subsidios para la operación de la red troncal de Internet y, al mismo tiempo, permitió el uso comercial de la red, previamente restringida a fines educativos y de investigación.

Se suponía que los gobiernos servirían mejor al interés público mundial manteniendo sus manos fuera del ciberespacio. La red se expandió a gran velocidad y muy pronto llegó a ser descrita como un "bien público global". [5] Sin embargo, manteniendo el espíritu de no intervención, la única decisión que los gobiernos tomaron colectivamente sobre el nuevo ámbito fue la declaración de 1998 de la Organización

2 Naciones Unidas (2015), párr. 1. 15.

3 Earth Institute/Ericsson (2015), pág. 2.

4 Bartlett (2018).

5 Kaul et al. (1999).

Mundial de Comercio (OMC) declarando que sus miembros "continuarán su práctica actual de no imponer derechos de aduana a las transmisiones electrónicas".[6] Por lo tanto, un disco que transporta videos, música o software puede estar sujeto a un arancel aduanero al cruzar fronteras, pero ese mismo contenido, transmitido por Netflix o iTunes a un consumidor que paga por él en otro país continúa sin ser gravado.

Las dificultades técnicas para controlar el flujo transfronterizo de datos (sin cerrar totalmente las comunicaciones) agregaron un elemento de necesidad a esa decisión, según el dictado de "si no puedes vencerlos, únete a ellos".

El valor de los flujos de datos transfronterizos era insignificante cuando se tomó la decisión de no gravarlos, pero está creciendo exponencialmente. En 2014, Estados Unidos exportó US $ 399,7 mil millones e importó US $ 240,8 mil millones en servicios entregados por transmisión digital. Ese excedente es aún mayor si agregamos la prestación digital de servicios a través de afiliados de empresas estadounidenses ubicadas en el exterior. En 2011, las filiales en Europa de empresas de Estados Unidos vendieron servicios digitales por valor de 312 mil millones de dólares.[7] La UNCTAD estimó que las compras transfronterizas de productos físicos vía Internet fueron por valor de 189 mil millones de dólares en 2015, apenas el 1,1 por ciento de las importaciones totales de mercancías.[8] Noventa y tres por ciento del comercio electrónico global sigue siendo doméstico.

Esa ventaja económica de Estados Unidos ayuda a explicar su apoyo a la idea del ciberespacio como un ámbito separado, donde ningún (otro) gobierno debería ejercer autoridad (o cobrar impuestos). Sin embargo, el 'ciberespacio' es solo una metáfora. Todos los dispositivos conectados están en alguna parte y toda la información se almacena en algún lugar, sin importar qué tan rápido pueda circular. Las dificultades (y a veces la imposibilidad) que enfrentan los titulares de obligaciones para cumplir sus responsabilidades ante los derechohabientes (comenzando por sus propios ciudadanos) no diluyen los derechos u obligaciones, solo enfatizan la necesidad de abordar multilateralmente las amenazas identificadas por el Secretario. General Guterres. Sin abordar esas amenazas, las TIC podrían convertirse en obstáculos para lograr la Agenda 2030 en lugar de contribuir a ella.

Amenazas a la ciberseguridad

En un blog publicado en marzo de 2018 por la Rand Corporation, un think-tank creado en 1948 por Douglas Aircraft Company para ofrecer investigación y análisis a las Fuerzas Armadas de los Estados Unidos, Isaac R. Porche sostiene que "los estados nación y sus mercenarios espían y atacan en el ciberespacio a través de las fronteras nacionales con regularidad".[9] La acusación formal a 13 ciudadanos rusos en Estados Unidos por intentar interferir en las elecciones de 2016 se ofrece como ejemplo, junto con la acusación a siete ciudadanos iraníes en 2012 por instalar código malicioso en una computadora que controla una presa en el estado de Nueva York y el robo a compañías estadounidenses en noviembre de 2017, del que se acusa a piratas informáticos chinos.

Steve Ranger, editor en jefe del sitio web especializado ZDNet, sin embargo, advierte que el país con "las capacidades más importantes de defensa y ataque cibernéticos" es Estados Unidos.[10] Durante la Cumbre de 2016 del G20 en Hangzhou, China, el presidente Barack Obama dijo: "Estamos entrando en una nueva era aquí, donde varios países tienen capacidades significativas. Y, francamente, tenemos más capacidad que nadie, tanto ofensiva como defensivamente".[11]

La distinción entre herramientas ofensivas y defensivas es, en este caso, retórica. En 2014, Dan Geer, un experto en seguridad del Instituto de Tecnología de Massachusetts y asesor de la CIA, publicó un ensayo

6 OMC (1998).
7 Nicholson (2016).
8 UNCTAD (2017).
9 Porche (2018).
10 Ranger (2017).
11 White House (2016).

sobre "Ciberseguridad como Realpolitik", básicamente demostrando que "toda la tecnología de seguridad cibernética es de doble uso".[12] Geer enfatizó que "tal vez el uso dual es una perogrullada que se aplica a todas y cada una de las herramientas, desde el bisturí hasta el martillo. Todas se pueden usar para bien o para mal, pero yo sé que el doble uso es inherente a las herramientas de ciberseguridad." El corolario de esa percepción es que "el uso ofensivo es donde están ocurriendo las innovaciones que solo los Estados pueden pagar". Huelga decir que muy pocos Estados pueden permitirse la enorme inversión en equipos e investigación necesarios para desarrollar estas capacidades.

El Departamento de Defensa de los Estados Unidos considera el ciberespacio como su quinto dominio de operaciones, después de la tierra, el mar, el aire y el espacio. Su actual Manual de la Ley de Guerra incluye un largo capítulo sobre operaciones cibernéticas, definidas como aquellas que "usan capacidades cibernéticas, como computadoras, herramientas de software o redes" y buscan "lograr objetivos o efectos en o a través del ciberespacio"[13] en general antecediendo o apoyando el asalto militar mayor. Cuidadosamente se excluyen de la definición, el uso de computadoras "para facilitar el comando y control" y "las operaciones para distribuir información". Esto significa que un intento de usar redes informáticas para influir en las elecciones (distribuyendo información o propaganda, de manera amplia o específica) no califica como guerra cibernética en el Manual del Departamento de Defensa de los Estados Unidos.

¿Por qué es importante la distinción? Porque, la Carta de las Naciones Unidas y el derecho internacional prohíben el uso de la fuerza a excepción de dos situaciones, legítima defensa y acciones explícitas acordadas por el Consejo de Seguridad. El Departamento de Defensa de los Estados Unidos establece claramente que "el término ‚ataque' a menudo se ha utilizado en un sentido coloquial al discutir operaciones cibernéticas para referirse a muchos tipos diferentes de actividades cibernéticas hostiles o maliciosas, como la desfiguración de sitios web, intrusiones de red, el robo de información privada, o la interrupción de la provisión de servicios de internet. Pero las operaciones descritas como "ataques cibernéticos" o "ataques de redes informáticas" no son necesariamente "ataques armados" a los efectos de desencadenar el derecho inmanente de legítima defensa de un Estado bajo *jus ad bellum*".[14]

Que el Departamento de Defensa de los Estados Unidos llegue a estos extremos para limitar el potencial escalamiento de hostilidades en el ciberespacio puede verse como un intento de utilizar la fuerza como último recurso, tal como exige la Carta de las Naciones Unidas, o también podría considerarse como una forma de prevenir que operaciones realizadas regularmente en el ciberespacio por la Agencia de Seguridad Nacional (NSA) del Departamento de Defensa no se definan como 'casus belli' que podrían legitimar la represalia de otras potencias.

La idea de promover la colaboración internacional en ciberseguridad o de regular (y finalmente prohibir) la ciber-guerra ha estado apareciendo en diferentes foros durante al menos una década. Las dificultades son enormes Los dos obstáculos que se plantean con mayor frecuencia son las complejidades relacionadas con la definición de un arma cibernética (en oposición al software para fines pacíficos, incluido el de defensa contra los ciberataques) y las dificultades de verificación.

Prácticamente en todos los casos citados como ciberataques que han llegado al conocimiento público, no solo es cuestionable la ubicación exacta del origen, sino también la atribución a un Estado o a un grupo independiente.

Las actividades no realizadas por Estados sino por individuos o grupos privados no pueden calificarse estrictamente como "guerra", pero dado que el origen de los ataques puede ser difícil de atribuir en el ciberespacio, el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI) parece inclinarse hacia

12 Geer (2014).

13 Departamento de Defensa de EE. UU. (2015), pág. 995.

14 Ibíd. (2015), pág. 996.

una definición de guerra cibernética que incluye 'cyber-hooliganism', 'cyber-vandalismo', y 'cyber-terrorismo'.[15]

Pero la analogía entre las armas de destrucción masiva (prohibidas por la ley internacional) y las armas cibernéticas puede ser engañosa. Ningún gobierno siquiera pensaría en utilizar bombas atómicas sobre sus propias poblaciones, pero las mismas agencias militares que preparan (y probablemente también realizan) ciber-ataques están utilizando sistemáticamente esas herramientas sobre sus propios ciudadanos. A medida que las fronteras nacionales se diluyen en el ciberespacio, las cuestiones de la paz y los derechos humanos básicos se fusionan. Y ambos son indispensables para alcanzar los ODS porque "no puede haber desarrollo sostenible sin paz ni paz sin desarrollo sostenible".[16]

Las revelaciones de Edward Snowden sobre la magnitud de la vigilancia masiva realizada por las agencias de inteligencia llevaron a la Asamblea General de las Naciones Unidas a adoptar una Resolución sobre el Derecho a la Privacidad en la Era Digital,[17] en la que expresó su profunda preocupación por el impacto negativo que la vigilancia e interceptación de las comunicaciones pueden tener sobre los derechos humanos. La Asamblea General afirma que los derechos que poseen las personas fuera de línea también deben ser protegidos en línea, y pide a todos los Estados respetar y proteger el derecho a la privacidad en las comunicaciones digitales. La Oficina del Alto Comisionado para los Derechos Humanos concluyó que "los mecanismos nacionales de supervisión, cuando existen, a menudo son ineficaces ya que no garantizan la transparencia, ni la rendición de cuentas por parte de la vigilancia estatal de las comunicaciones, su interceptación y la recopilación de datos personales".[18]

El Consejo de Derechos Humanos creó el mandato de un Relator Especial sobre el derecho a la privacidad y el Profesor Joseph Cannataci, de Malta, fue nombrado en julio de 2015. En su informe al Consejo de Derechos Humanos en marzo de 2018, Cannataci recomienda la creación de un instrumento internacional sobre la vigilancia gubernamental, con autoridad legal para equilibrar las necesidades de seguridad legítimas de los gobiernos con sus obligaciones de proteger los derechos humanos.[19]

Los datos son el nuevo petróleo

La vigilancia a que nos somete un Estado (que puede o no ser el propio) no es la única amenaza a la privacidad. A través de sus plataformas digitales, grandes multinacionales están obteniendo, procesando y re-vendiendo información acerca de las personas, excediendo las autorizaciones que los usuarios pueden haber dado y potencialmente violando sus derechos mientras se vuelven enormemente ricas y poderosas.

Por un lado, la naturaleza abierta de Internet (cualquiera puede acceder sin pedir autorización) y su neutralidad (todo el tráfico se trata con igualdad, un principio que ahora dejo de ser ley en los Estados Unidos) son factores democratizadores: cualquiera puede publicar, comprar o vender en igualdad de condiciones y millones de personas han encontrado en Internet un canal para hacerse oír o acceder a mercados que antes estaban fuera de su alcance.

Al mismo tiempo, un puñado de empresas(Google, Amazon, Facebook, Apple, conocidas colectivamente como GAFA, o ahora GAFA-A con la adición de Alibaba, de China) concentran un enorme poder. Google afirma saber que un usuario está enfermo antes de que éste llame al médico y Amazon se jacta de que nuestro próximo pedido está siendo embalado antes de que uno lo compre. Facebook ha experimentado con el control de los estados de ánimo de sus usuarios, manipulando la entrega de buenas o malas noticias.

15 Véase: http://www.unicri.it/special_topics/securing_cyberspace/cyber_threats/explanations/

16 Naciones Unidas (2015), Preámbulo.

17 Naciones Unidas (2013).

18 OACNUDH (2018), párr. 6.

19 Consejo de Derechos Humanos (2018).

El matemático británico y analista de mercado Clive Humby dijo en 2006 que "los datos son el nuevo petróleo".[20] El petróleo necesita ser procesado para convertirlo en combustible o en plástico. Y, al igual que con el petróleo, los datos benefician más a quienes los refinan y venden que a las comunidades de donde se lo extrae. La conciencia de esa situación está llevando a algunos grupos a proponer que los individuos o las comunidades deben ser compensados por el valor generado a partir de los datos que proporcionan,[21] mientras que muchos países están considerando maneras de ejercer su soberanía sobre los datos (véase el recuadro 3.2).

20 Palmer (2006).

21 Tarnoff (2018).

Recuadro 3.2

Soberanía sobre los datos

POR IT FOR CHANGE[1]

En una economía plataformizante, las plataformas de comercio electrónico deben entenderse no solo como mercados, sino también como ecosistemas digitales que proporcionan una nueva arquitectura para la economía. Las plataformas como Amazon organizan y controlan ecosistemas completos de mercado que comprenden proveedores, productores, transportadores y consumidores/usuarios.[2]

Las empresas de comercio electrónico generan valor a partir de los datos de su ecosistema, utilizándolos datos para crear la inteligencia digital inclusiva que transforme completamente el ADN del mercado y los eleve a una posición de dominio. Amazon puede haber comenzado como un vendedor de libros en línea, pero se ha convertido en una 'super-plataforma', un monopsonio (único comprador) que se extiende a través de su portal de comercio electrónico para ofrecer servicios en la nube, billetera digital y video a pedido.[3]

Los países en desarrollo deben saber que en la economía de la información, cualquier paso hacia la creación de un campo de juego equitativo para sus plataformas locales debe abordar prioritariamente la cuestión de los datos en los regímenes de comercio digital. El discurso de los flujos libres de datos se basa en que un régimen global de datos puede generar valor económico de los datos y posibilidades de innovación. Sin embargo, las naciones en desarrollo son apenas 'minas de datos', territorios de los que los datos se extraen y, en el mejor de los casos, talleres administrativos o granjas de servidores para el procesamiento de datos de baja calidad. Incluso países que se han distinguido como centros tecnológicos a menudo desarrollan productos y servicios de innovación pero pierden el control intelectual[4] y los dividendos económicos ante los gigantes tecnológicos del Norte global. El discurso de los flujos de datos libres ignora el terreno desigual[5] sobre el cual compiten las

1 Extracted from the Submission to UNCTAD's Intergovernmental Group of Experts on E-Commerce and the Digital Economy by members of the Research Network on Policy Frameworks for Digital Platforms - Moving from Openness to Inclusion, led by Anita Gurumurthy, Geneva, April 2018. The complete text is available at: http://unctad.org/meetings/en/Contribution/tdb_ede2018_c03_ITforChange_en.pdf

2 Véase: www.itforchange.net/sites/default/files/1516/Platform_Policies_Research_Framework2018.pdf

3 Véase: www.forbes.com/sites/gregpetro/2017/08/02/amazons-acquisition-of-whole-foods-is-about-two-things-data-and-product/#740451d7a808

4 Véase: www.forbes.com/sites/venkateshrao/2012/09/03/entrepreneurs-are-the-new-labor-part-i/#36a53d3f4eab

5 Véase: www.itforchange.net/index.php/grand-myth-of-cross-border-data-flows-trade-deals

naciones “ricas en inteligencia” y las “pobres en inteligencia”.

Fomentar plataformas locales no se logra con soluciones simplistas que provienen del pensamiento pre-digital. La soberanía sobre los datos y el control de los datos de los sectores críticos es vital para las empresas y los gobiernos en el Sur global para que puedan beneficiarse verdaderamente de las posibilidades del comercio electrónico. El apoyo público es necesario para catalizar y habilitar los ecosistemas del mercado local en los que los actores pequeños y marginales puedan competir. Esto implica no solo la creación de datos públicos y abiertos que estén disponibles para usos públicos y comerciales, sino también el apoyo en forma de infraestructura pública de inteligencia digital.

Además, un marco legal y político ágil para frenar los excesos de las plataformas es una necesidad imperiosa. El Sur global corre el riesgo de convertirse en un campo de innovación no regulado para que los gigantes tecnológicos experimenten, a menos que desarrolle medidas políticas adecuadas e integrales que puedan regir sus operaciones. Las fronteras políticas críticas como la mano de obra, la protección del consumidor, la privacidad, las inversiones extranjeras y otras áreas que impactan directamente en los ingresos y derechos de los ciudadanos y usuarios de la plataforma no pueden someterse a las ganancias inmediatas a corto plazo que las grandes plataformas prometen.

Los contratos dudosos, los términos de servicio y las políticas de privacidad que dictan las plataformas no deberían ser un lastre para los marcos de políticas desarrollados por el Estado. Obligar a las empresas de plataforma a compartir parte de la información que recopilan con agencias públicas en sectores clave es importante para frenar sus prácticas anti-competitivas y promover el espacio para pequeñas empresas e innovadores locales que utilicen estos datos para crear sus propios productos.

Empleos: amenazas y esperanzas

Desde la primera revolución industrial, las máquinas han destruido empleos y creado otros nuevos. El resultado neto ha sido un aumento de la productividad y la gran pregunta social y política desde entonces es cómo esas ganancias se distribuyen en la sociedad.

Pero la difusión de las TIC no solo sustituye por máquinas la mano de obra humana, sino que también facilita la división de trabajos complejos en múltiples tareas menores y su distribución en todo el mundo a través de plataformas laborales digitales en las que los clientes ofrecen trabajos y los trabajadores compiten por obtenerlos. El mercado para el trabajo digital fue de 4.800 millones de dólares en 2016, y está creciendo a una tasa del 25% anual.[22] Se estima que 112 millones de trabajadores están ofreciendo sus servicios en ese mercado, pero solo uno de cada diez completó al menos una tarea pagada en el año.

Millones de graduados desempleados esperan trascender algunas de las limitaciones de sus mercados laborales locales y competir globalmente por tareas tales como traducciones, transcripciones, generación de textos, mercadotecnia, entrada de datos y asistencia personal. Hasta ahora, la globalización ha ampliado el alcance global del capital a costa de la mano de obra local. El trabajo en línea promete que no solo el capital, sino también los trabajadores puedan competir en un mercado global. En la práctica, sin embargo, como la oferta de trabajo es diez veces

22 Graham et al. (2017).

mayor que la demanda real, los trabajadores digitales tienen poco poder de negociación. Los trabajadores son considerados 'contratistas independientes' y, en las transacciones transfronterizas, la confusión en cuanto a qué legislación laboral aplicar generalmente resulta en la ausencia total de protección social.

Estudios empíricos han demostrado que en lugar de una economía sin fricciones, entre empleadores en países de altos ingresos y trabajadores en países en desarrollo (principalmente India, Filipinas, Pakistán y Bangladesh) "surgen intermediarios que usan la ubicación geográfica, las redes y otras ventajas posicionales para mediar entre compradores y vendedores de trabajo, exacerbando así las desigualdades globales".[23]

Sin embargo, "gobiernos como los de Nigeria, Malasia y Filipinas, y grandes organizaciones como el Banco Mundial, ven cada vez más al trabajo digital como un mecanismo para ayudar a algunos de los más pobres del mundo a escapar de las oportunidades limitadas de crecimiento económico en sus contextos locales".[24] Los beneficios que algunos trabajadores realmente obtienen no deben oscurecer la desigualdad intrínseca en este mercado, enfatizada por el rol de las plataformas que intermedian. El trabajo digital es solo uno de los aspectos en los que las nuevas tecnologías están transformando el futuro del trabajo, pero es necesario concebir alternativas y estrategias para esta forma extrema de relaciones humanas transfronterizas, para crear un mundo de trabajo más justo en todas partes.

23 Ibíd., pág. 149.

24 Ibíd., págs. 158-159.

Recuadro 3.3

Las máquinas (algoritmos) ya están decidiendo nuestro futuro

POR PRABIR PURKAYASTHA[1]

Los algoritmos digitales están tomando decisiones que antes tomaban los gobiernos, las empresas e incluso nosotros mismos.

Hoy en día, hay algoritmos que deciden quién conseguirá un trabajo, qué parte de una ciudad necesita desarrollarse, quién debe ingresar en una universidad y, en el caso de un delito, cuál debería ser la sentencia. Lo que amenaza la vida tal como la conocemos, no es la súper-inteligencia de algunos robots sino la proliferación de máquinas que toman miles de decisiones críticas para las vidas de las personas y para definir qué sociedad tendremos.

Supongamos que Usted solicita un préstamo. La gran cantidad de datos financieros que Usted ha creado - transacciones con tarjetas de crédito, transacciones bancarias, retiros de cajeros automáticos - todos estos datos son accedidos y procesados por algoritmos en alguna computadora. Esta información está almacenada para siempre; es más barato almacenar todos los datos que decidir cuáles guardar y eliminar los otros. Todos estos datos son procesados por los algoritmos para determinar su solvencia y con base en el puntaje final, se toma la decisión de otorgar un préstamo.

Lo que decide si Usted obtiene un préstamo o no es, finalmente, un puntaje establecido por una máquina, no quién es Usted, qué ha logrado, qué tan importante es su trabajo para el país (o la sociedad). Para la máquina, usted es solo el resultado de todas sus transacciones pasadas, procesadas y reducidas a un número simple.

Estos algoritmos son propiedad intelectual y, por lo tanto, sus secretos están celosamente guardados. Lo peor es que algunos de los algoritmos ni siquiera los

1 A longer version was originally published on https://newsclick.in/.

entienden quienes los escribieron; ¡incluso los creadores de tales algoritmos no saben cómo obtuvo un algoritmo particular un puntaje específico!

La matemática y científica de datos Cathy O'Neil, en un libro reciente, "Weapons of Math Destruction" (armas de destrucción matemática) nos dice que la aparente objetividad de procesar gran cantidad de datos mediante algoritmos es falsa. Los algoritmos en sí mismos no son más que nuestros sesgos y subjetividades codificados: "Son solo opiniones traducidas al lenguaje matemático".

¿Qué sucede cuando transformamos los datos que creamos con nuestras huellas numéricas cotidianas en "opiniones" o "decisiones" de las máquinas? Google ofrece más anuncios de trabajos bien remunerados a varones que a mujeres; los afro-descendientes reciben condenas más largas ya que son señalados como de alto riesgo de reincidir en el delito por un algoritmo de evaluación de riesgos judiciales. El algoritmo no utilizaba explícitamente la raza del delincuente, pero calculaba el riesgo tomando en cuenta su lugar de residencia, los antecedentes de otros miembros de la familia, la educación y los ingresos, todo lo cual, en conjunto, es un indicador de la raza.

El problema es más profundo que los sesgos subjetivos de los programadores de algoritmos y radica en los llamados modelos predictivos que construimos utilizando estos datos. Tales datos y modelos simplemente reflejan la realidad objetiva del alto grado de desigualdad que existe dentro de la sociedad, y lo replica en el futuro a través de sus predicciones.

¿Qué son los modelos predictivos? En pocas palabras, usamos el pasado para predecir el futuro. Utilizamos la gran cantidad de datos disponibles para crear modelos que relacionen el resultado "deseado" con una serie de datos de entrada. El resultado podría ser un puntaje de crédito, la posibilidad de tener éxito en una universidad, un trabajo, etc. Los datos históricos de las personas que han tenido "éxito", algunas variables de resultados específicos, se seleccionan como indicadores de éxito y se correlacionan con diversos datos sociales y económicos del candidato. Esta correlación se usa para clasificar a cualquier nuevo candidato en términos de posibilidades de éxito en función de su perfil. Para usar una analogía, los modelos predictivos son como conducir automóviles mirando solo a través del espejo retrovisor.

Una puntuación para el éxito, ya sea un trabajo, la admisión a una universidad o una pena de prisión, refleja de alguna forma la desigualdad existente en la sociedad. No hay falta que un afroamericano en los Estados Unidos, o un dalit o un musulmán en la India, sea identificado por raza, casta o religión. Los datos de sus transacciones sociales ya son prejuiciosos y tendenciosos. Cualquier algoritmo de puntuación terminará con una predicción de éxito futuro en función de qué grupos tienen éxito hoy. El peligro de estos modelos es que la raza, la casta o el credo pueden no existir explícitamente como datos, pero existe una gran cantidad de otros datos que actúan como sustitutos de estas "variables".

Dichos modelos predictivos son una fuerza intrínsecamente conservadora que intenta replicar las desigualdades existentes de la sociedad.

La comunidad de Inteligencia Artificial está reconociendo los peligros de tales modelos, que pueden, incluso, violar garantías constitucionales contra la discriminación.

Ya se discute en Estados Unidos la creación de una Junta de Seguridad de Algoritmos, que los pueda volver transparentes y responsables. Deberíamos saber qué se está codificando y, si es necesario, averiguar por qué el algoritmo emitió una determinada decisión: los algoritmos deberían poder auditarse. Ya no es suficiente decir "la computadora lo hizo".

¿Y ahora qué?

Mientras la mitad de la humanidad se comunica, se informa y cada vez más trabaja y compra en línea, la promesa original de democratización de las TIC está siendo reemplazada por la preocupación sobre el enorme poder que estas tecnologías han concentrado en unos pocos gobiernos y un puñado de mega-corporaciones. El público está preocupado en todas partes y la pregunta ya no es si la regulación es necesaria sino cómo hacerlo.

Reconocer al conocimiento y a Internet como bienes públicos globales debería implicar un enfoque multilateral, que solo puede basarse en la primacía de los derechos humanos y el reconocimiento de la soberanía (después de todo, el "ciberespacio" o la "nube" son solo metáforas: todas las computadoras y las personas que las operan están en algún lugar).

Las computadoras, los algoritmos y las leyes que rigen nuestro uso de ambos, son todas creaciones humanas, resultado de una construcción cultural y de decisiones políticas. Y como tales, pueden ser cambiadas. No será una tarea fácil, pero lo que la experiencia ha demostrado hasta ahora es que Internet no es viable como propiedad de un solo país y que las empresas no se han auto-regulado.

El principal activo de los gigantes corporativos digitales no es el capital físico sino la propiedad intelectual sobre sus algoritmos y los datos (proporcionados por los usuarios) sobre los que operan. En lugar de facilitar el intercambio, como su nombre lo indica, una nueva generación de acuerdos de "libre comercio" refuerza y extiende monopolios artificiales sobre los datos y la tecnología, en la medida en que, como dice el economista premio Nobel Joseph Stiglitz, "en campos como la tecnología de la información, una epidemia de exceso de patentes han dificultado la innovación posterior y han erosionado algunos de los beneficios de la creación de conocimiento".[25]

La percepción de que se necesita un enfoque diferente de la innovación y la propiedad intelectual, sumado al temor de la apropiación injusta de datos generados localmente por empresas que ni siquiera tienen representación en sus países, llevó a muchos países en desarrollo a rechazar la idea de iniciar negociaciones de comercio electrónico en la OMC en 2017.[26]

'Más de lo mismo' ya no es aceptable. La Agenda 2030 propone un cambio de paradigma en el desarrollo que no es posible con las tecnologías que prevalecen hoy en día, la dependencia continua de los combustibles fósiles y el uso insostenible de los recursos.

Para abordar las necesidades tecnológicas de "una transición global hacia modelos de desarrollo económico y social más resilientes y menos intensivos en recursos", en 2017 la organización belga de investigación y tecnología VITO, junto con socios de África, India y Brasil, inició una serie de conferencias mundiales sobre ciencia, tecnología e innovación. Sus conclusiones iniciales son optimistas: "Muchas de las tecnologías necesarias para alcanzar los objetivos de desarrollo sostenible ya están disponibles".[27] La efectividad de estas soluciones alternativas se ha demostrado bajo condiciones de la vida real. Lo que se necesita, entonces, es "desarrollar estrategias para desplegarlas a gran escala, al nivel necesario para alcanzar los ODS".

En el caso de la energía y los alimentos, un requisito clave para lograr los ODS es priorizar las "soluciones tecnológicas originadas en las bases y ampliamente distribuidas, de manera que sean apropiadas para las necesidades y circunstancias de las comunidades" para lograr, en última instancia, una "economía circular". En este nuevo modelo, las TIC se reconocen como "una herramienta indispensable" mientras que la "recuperación de los recursos y el uso de los desechos" se convierten en "la nueva normalidad".

25 Stiglitz et al. (2017).

26 Véase: www.twn.my/title2/wto.info/2017/ti171232.htm

27 Véase: https://2018.gstic.org/insights/2017-key-findings

Bibliografía

Bartlett, Jamie (2018): Will 2018 be the year of the neo-luddite? En: The Guardian, 4 de marzo de 2018. www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite

Casa Blanca (2016): Rueda de prensa del Presidente Obama tras la Cumbre del G20, 5 de septiembre de 2016, J.W. Marriott Hotel Hangzhou, China. https://obamawhitehouse.archives.gov/the-press-office/2016/09/05/press-conference-president-obama-after-g20-summit

Cisco (2017): Cisco Visual Networking Index: Forecast and Methodology, 2016–2021. www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf

Consejo de Derechos Humanos (2018): Report of the Special Rapporteur on the right to privacy, Appendix 7: Draft Legal Instrument on Government Led Surveillance. Ginebra (A/HRC/37/62). www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf

Earth Institute/Ericsson (2015): ICT and SDGs: How Information and Communications Technology Can Achieve The Sustainable Development Goals. Nueva York. http://unsdsn.org/wp-content/uploads/2015/09/ICTSDG_InterimReport_Web.pdf

Geer, Dan (2014): Cybersecurity as Realpolitik. http://geer.tinho.net/geer.blackhat.6viii14.txt

Graham, Mark/Hjorth, Isis/Lehdonvirta, Vili (2017): Digital labour and development: impacts of global digital labour platforms and the gig economy on worker livelihoods. En: Transfer: European Review of Labour and Research 23:2. http://journals.sagepub.com/doi/10.1177/1024258916687250

Kaul, Inge/Grunberg, Isabelle/Stern, Marc A., ed. (1999): Global Public Goods. International Cooperation in the 21st Century. Nueva York: Oxford University Press. www.researchgate.net/profile/Eugenio_Bobenrieth/publication/46440722_The_Political_Economy_of_International_Environmental_Cooperation/links/55ddb07308ae79830bb531ed.pdf#page=488

Naciones Unidas (2013): El derecho a la privacidad en la era digital. Resolución aprobada por la Asamblea General el 18 de diciembre de 2013 [sobre la base del informe de la Tercera Comisión (A/68/456/Add.2)] Nueva York (UN Doc. A/RES/68/167). https://undocs.org/es/A/RES/68/167

Naciones Unidas (2013):Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible. Nueva York (UN Doc. A/RES/70/1). https://sustainabledevelopment.un.org/post2015/transformingourworld

Naciones Unidas (2018): Observaciones del Secretario General al Consejo Económico y Social, serie de sesiones sobre actividades operacionales para el desarrollo. Martes, 27 de febrero de 2018. Nueva York. www.un.org/sg/en/content/sg/speeches/2018-02-27/remarks-ecosoc-activities-development-segment

Nicholson, Jessica (2016): Measuring the Economic Value of Cross-Border Data Flows. Presentación en UNCTAD/WTO/UPU Measuring E-Commerce Day, 22 de abril de 2016. Washington, D.C.: USA Department of Commerce, Office of the Chief Economist. http://unctad.org/meetings/en/Presentation/dtl_eweek2016_JNicholson_en.pdf

OACNUDH (2018): Concept Note. Taller de expertos con el propósito de identificar y aclarar principios, normas y mejores prácticas en relación con la promoción y protección del derecho a la intimidad en la era digital, 19 y 20 de febrero de 2018, Ginebra. www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf

OMC (1998): Declaración sobre el comercio electrónico mundial. Conferencia ministerial. Segundo período de sesiones, 25 de mayo de 1998. Ginebra (Wt/MIN(98)/Dec/2). https://www.wto.org/spanish/tratop_s/ecom_s/mindec1_s.htm

Palmer, Michael (2006): Data is the New Oil. En: ANA Marketing Maestros, 3 de noviembre de 2006. http://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Porche, Isaac R. (2018): Getting Ready to Fight the Next (Cyber) War. En: The RAND Blog, 3 de marzo de 2018. www.rand.org/blog/2018/03/getting-ready-to-fight-the-next-cyber-war.html

Ranger, Steve (2017): Cyberwar: A guide to the frightening future of online conflict. En: ZDNet, 29 de agosto de 2017. https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-online-conflict/

Stiglitz, Joseph/Baker, Dean/Jayadev, Arjun (2017): Innovation, Intellectual Property, and Development: A better set of approaches for the 21st century. Azim Premji University, University of Cape Town, Fundação Osvaldo Cruz. http://cepr.net/images/stories/reports/baker-jayadev-stiglitz-innovation-ip-development-2017-07.pdf

Tarnoff, Ben (2018): Big data for the people: it's time to take it back from our tech overlords. En: The Guardian, 14 de marzo de 2018. www.theguardian.com/technology/2018/mar/14/tech-big-data-capitalism-give-wealth-back-to-people

UNCTAD (2017): Information Economy Report 2017: Digitalization, Trade and Development. Ginebra (UNCTAD/IER/2017/Corr.1). http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf

US Department of Defense (2015): Law of War Manual. Washington, D.C. www.defense.gov/Portals/1/Documents/law_war_manual15.pdf

Roberto Bissio es Director Ejecutivo del Instituto del Tercer Mundo y coordinador de la red Social Watch.