

Geopolítica de la soberanía de datos en la competencia hegemónica. China, América Latina y la Inteligencia Artificial.

Norberto Emmerich – Michael Chong Pineda

“El desarrollo de la inteligencia artificial no debe ser dominado por un solo país, sino que debe ser una sinfonía de cooperación global” (ZNews, 2026), dijo el presidente chino Xi Jinping el viernes 17 de julio de 2026. Hablando en la Conferencia Mundial de Inteligencia Artificial en Shanghái, Xi agregó que los países deben cooperar para construir “un sistema global de gobernanza de IA justo y equitativo” e instó a adoptar salvaguardas más sólidas para mantener la IA.

El sistema nacional chino de vigilancia masiva por cámaras de seguridad (CCTV) y reconocimiento facial se llama Skynet (Shen, 2019). Se escribe 天网 y su pronunciación en pinyin es Tiānwǎng. La traducción tiene una equivalencia exacta término a término con el inglés y el español: 天 (Tiān): Cielo (Sky) y 网 (Wǎng): Red (Net)

Estas declaraciones y términos forman parte de la retórica actual china en torno a la soberanía de datos y la gobernanza tecnológica e ilustran cómo se están posicionando las potencias frente al extractivismo de datos y el control de la infraestructura digital.

Estas posturas públicas son una pieza fundamental para comprender la dimensión de la competencia tecnológica mundial y seguir las huellas del dragón digital en su estrategia de expansión e influencia en las políticas de adopción de IA a nivel internacional. Esta nueva problemática se involucra a toda velocidad y fuerza en la geopolítica mundial, en la forma de una disputa por la soberanía de datos.

Mientras tanto América Latina se ve enfrentada a un proceso extractivista de datos y una presión por parte de las potencias extrarregionales para adaptarse al status de prevalencia tecnológica que ellas ofrecen.

Palabras clave: extractivismo de datos – soberanía digital – Kondratieff-Wallerstein – crimen organizado – margen sistémico.

Descripción del problema

La competencia mundial por la soberanía de datos en la IA representa un aspecto específico dentro de la lucha general por el liderazgo del orden mundial futuro. En este caso es la lucha por controlar la infraestructura, los modelos y la información que impulsan estas tecnologías. En el interés de preservar la soberanía digital los países de la periferia y la semiperiferia buscan evitar la dependencia de las potencias extraregionales protegiendo la información sensible, creando modelos de desarrollo autónomos y garantizando que las plataformas extraregionales respeten las normativas locales.

Esta carrera geopolítica está dominada por las superpotencias tecnológicas debido a su masiva capacidad de cómputo y extensos repositorios de datos. Mientras Estados Unidos y China lideran el desarrollo de los modelos de frontera, Europa intenta establecer estándares éticos y de gobernanza a través de normativas como la Ley de IA. Quien domine esta cadena de valor controlará el poder económico y la seguridad nacional. Al ser una lucha geopolítica, es lógico que el crimen organizado sea un instrumento al servicio de la seguridad nacional de las potencias.

En el contexto regional, América Latina enfrenta el reto de superar el extractivismo digital y la dependencia de las plataformas extranjeras. La creación de centros de datos locales y el impulso de iniciativas regionales son estrategias clave para retener el valor y adaptar la inteligencia artificial a las realidades socioculturales locales.



Figura 1. La región registra más de 75.170 millones de dólares anuales en datos brutos que salen gratis hacia el Norte. El flujo de información hacia el exterior aumenta a una tasa constante del 12,9% cada año. Solo 10 países del mundo controlan más de dos tercios de todos los flujos de información internacionales (Estados Unidos, China, Reino Unido, Alemania, Singapur, Irlanda, Corea del Sur, Francia, Países Bajos, Japón).

La ley CLOUD Act permite a Estados Unidos exigir datos a sus empresas sin importar dónde estén guardados, mientras China asegura la dependencia tecnológica a largo plazo mediante infraestructura 5G y sistemas de vigilancia avanzados. Fuente: elaboración propia.

Marco teórico

La disputa por la soberanía de datos en la IA se ubica en el sexto ciclo tecnológico y productivo mundial según las ondas hegemónicas de Kondratieff-Wallerstein (2005).

En este marco teórico, cada ciclo económico de largo plazo (50 a 60 años) es impulsado por una innovación tecnológica disruptiva que redefine las dinámicas de acumulación de capital y reconfigura el poder geopolítico global. Así como el carbón, el acero o la microelectrónica sostuvieron los ciclos anteriores, la infraestructura de inteligencia artificial y el control geopolítico de los datos constituyen las materias primas estratégicas y la base productiva que articulan la transición hacia una nueva onda de expansión económica mundial.

En la transición de una fase a otra se produce la disputa hegemónica y esta fase de transición entre dos ondas de Kondratieff suele coincidir con una crisis de

acumulación y una intensa fricción por la sucesión de la potencia hegemónica. Actualmente, el declive relativo de la hegemonía estadounidense da paso a un periodo de transición caótico (interregno hegemónico) donde China emerge como el principal competidor por el liderazgo del nuevo ciclo de IA.

En este contexto general la competencia por la soberanía de datos no sería simplemente un debate técnico o comercial, sino una carrera para asegurar el monopolio tecnológico que permitirá a una superpotencia dictar las reglas del intercambio económico global y subordinar a las demás naciones en una nueva división internacional del trabajo.

Esta disputa por la soberanía de datos reproduce y profundiza la estructura tripartita del sistema-mundo en centro, semiperiferia y periferia. Las economías centrales (Estados Unidos y China) actúan como los grandes centros de procesamiento y desarrollo de modelos de frontera de IA, concentrando el capital y la infraestructura avanzada. En el otro lado, las regiones periféricas y semiperiféricas, como América Latina, corren el riesgo de quedar atrapadas en un rol de meras proveedoras de datos primarios y consumidoras de tecnología importada. La lucha por la soberanía digital en estas regiones representa un intento crítico por romper este esquema de extractivismo digital y evitar una transferencia neta de valor hacia los centros hegemónicos durante todo el transcurso de la sexta onda.

La competencia mundial por la soberanía de datos en IA representa la consolidación de la sexta onda de Kondratieff, funcionando como el nuevo eje de acumulación económica y disputa geopolítica que, según la teoría de Wallerstein, definirá qué potencia ejercerá la hegemonía global en el sistema-mundo durante el próximo siglo, después de un probablemente largo período de transición.

La Ruta de la Seda digital - DSR

En uno de los polos de la contienda mundial China lanzó la DSR en el año 2015 buscando conectar Europa y África a través de una nueva súper autopista de la información. Busca posicionarse como la primera potencia industrial y tecnológica cumpliendo un rol central en la Cuarta Revolución Industrial, junto con la Nueva Ruta de la Seda, el Plan China 2025 y la Iniciativa del Delta del Yangtzé.

Algunas empresas privadas líderes en Asia como Huawei y ZTE e importantes actores estatales, como la Universidad de Beijing y el Ministerio de Industria y Tecnologías de Información forman parte de la DSR.

La Belt and Road Initiative (BRI) ha evolucionado más allá de los puertos, las carreteras y los ferrocarriles, pero la verdadera arteria por la que circula el poder es invisible: cables de fibra óptica, satélites, redes 5G y sistemas de IA. Beijing apuesta por liderar el futuro del ciberespacio, reforzando el control y la captura de datos. Por ello el programa de escaneo urbano se llama muy apropiadamente Skynet.

La DSR es “la expresión más sofisticada del poder blando chino”, una herramienta para moldear no solo las infraestructuras, sino también los flujos de datos, las normas digitales y, en última instancia, las narrativas que circulan por el mundo. La tecnología, en este contexto, no es neutral: cada cable submarino tendido, cada torre 5G erigida, representa una decisión geopolítica.

Hay ciertos peligros, porque la tecnología china implica un modelo de gobernanza digital que prioriza la eficiencia y el control estatal por sobre la apertura y la privacidad. La DSR exporta hardware, pero también una visión del mundo donde la soberanía digital es un sinónimo de vigilancia estatal y predominio de los mecanismos de disciplina y control.

Joseph Nye (2021) afirma con razón que “la competencia por el poder en el siglo XXI se jugará menos en los campos de batalla tradicionales y más en el terreno de la interconexión global”, un tablero donde China busca tomar la delantera.

La DSR se asocia con Asia, África y Europa del Este, aunque su influencia alcanza rincones menos evidentes, como Haití. En 2022, China propuso financiar proyectos de telecomunicaciones en la isla caribeña, ofreciendo infraestructuras clave en un país marcado por la inestabilidad. Es una jugada estratégica porque cada nuevo socio en la Ruta de la Seda refuerza la red diplomática china, especialmente en regiones donde compite con la influencia de Estados Unidos. Robert Kaplan entiende que “China no construye solo puertos y cables; construye lealtades” (Castellanos, 2023). Ya que Haití reconoce a Taiwán, China asienta una base digital allí. Además, el Windward Passage (Canal de los Vientos) es un observatorio

importante del tráfico comercial global. China también está presente en Bolivia, Ecuador, Argentina, Perú, México, Colombia, Venezuela y Brasil.

Si la geopolítica es el poder aplicado a un territorio, la ubicación de infraestructuras digitales en determinados territorios es indicadora de pretensiones geopolíticas.

El crecimiento de la economía digital

En 2017 la economía digital China alcanzó casi el 4% de su PIB mientras el valor económico para otras economías del Asia-Pacífico oscilaba entre el 1% y 3%. En 2025 la cifra fue del 14% y en 2030 se espera que alcance un 22% de su PIB.

Todos los grandes poderes están reforzando sus estrategias geopolíticas para controlar, proteger y mejorar el crecimiento digital. China, buscando liderar la transformación digital, ha planeado una infraestructura digital agresiva, centrada en su propio beneficio.

Busca, entre otros objetivos, exportar su exceso de capacidad industrial a través de lo digital, facilitando:

- 1) la expansión de las corporaciones tecnológicas chinas,
- 2) el acceso a los grandes conjuntos de datos y
- 3) la proyección de un gran poder hacia el exterior.

El objetivo principal de la Ruta de la Seda Digital es impulsar la conectividad a nivel regional y global, a través de cuatro pilares:

- La inversión china en infraestructura digital en el extranjero, incluidos cables submarinos de fibra óptica, centros de datos y redes móviles 5G.
- El desarrollo de tecnologías avanzadas, de uso interno, esenciales para la obtención de poder económico y militar, incluidos los sistemas de navegación por satélite, la inteligencia artificial y la computación cuántica.
- La promoción del comercio electrónico a través de zonas de libre comercio digital, lo que favorece estratégicamente su influencia a través de la interdependencia económica y la integración regional, reduciendo las barreras comerciales transfronterizas y estableciendo centros logísticos optimizados para uso a nivel regional.

- El reforzamiento de su perfil geopolítico, a través del desarrollo tecnológico, estableciendo su entorno digital internacional ideal a través de la diplomacia digital y la gobernanza multilateral. Esto incluye el uso de instituciones multilaterales para establecer estándares tecnológicos –relacionados con la infraestructura de telecomunicaciones– más beneficiosos para China, promoviendo el principio de la ciber-soberanía en los foros de la ONU.

La Ruta de la Seda Digital en la disputa entre China y Estados Unidos

Debido a la omnipresencia de la digitalización, a los beneficios derivados de ella y al impacto socioeconómico que ejerce en el mundo, la industria tecnológica ha pasado a estar en el centro de las tensiones comerciales y geopolíticas.

El desarrollo tecnológico es un factor determinante en la carrera por la supremacía global y China está utilizando la Ruta de la Seda Digital para mejorar la conectividad digital en su entorno más próximo y extender su influencia, impulsando su ascenso como superpotencia tecnológica.

- Estados Unidos lanzó ataques directos contra compañías concretas, como Huawei, acusada de espionaje a través del suministro de cables de fibra óptica y redes 5G, que será la tecnología habilitadora para una multiconexión global.
- La verdadera razón por la que la tecnología puntera de Huawei (las redes inalámbricas 5G) creó alarma dentro de la administración Trump, es que apunta a un peligroso desplazamiento geopolítico y geoeconómico mediante el cual China pretende fijar los estándares tecnológicos y económicos del siglo XXI.
- Lo que también acontece es una guerra mundial cibernética entre las potencias mundiales por apropiarse de nuestros datos latinoamericanos. “Si los datos son el nuevo petróleo, China es la nueva Arabia Saudita”.
- Durante la pandemia de Covid 19 la carrera por desarrollar una vacuna formó parte de un intento por mantener una posición superior en la geopolítica mundial, en un momento en el cual la desconexión entre las potencias era evidente.
- El conflicto por el 5G es uno de los factores que más contribuye al retroceso de la interdependencia económica que caracterizaba al mundo, en un proceso que ha sido conocido como “desglobalización” o “desacople” (Orbe León, 2021). La

escalada comercial y la presión estadounidense para que las empresas abandonen las cadenas de valor de China afectó los costos de componentes y productos ensamblados.

- Las diferencias técnicas en las cadenas globales de valor pueden llevar al escenario de un internet no interoperable, que funcione bajo distintos parámetros según las distintas esferas de influencia, dejando de ser global.

En el campo de la tecnología, las tensiones existentes entre Estados Unidos y China son parte de la competición por la hegemonía global.

La competencia geopolítica camino a la bifurcación

Estados Unidos manifestó la rivalidad por la supremacía tecnológica y China respondió enfocándose en Asia, Europa y África para implementar su DSR. Aunque se trata de un enfrentamiento comercial, la disputa de la geopolítica digital entre Estados Unidos y China está centrada en el futuro en la infraestructura de telecomunicaciones globales y las tecnologías digitales.

Y a medida que crece esta competencia, también crece la posibilidad de una bifurcación en los ecosistemas tecnológicos globales de la información y la seguridad dividida entre los países que dependen de las TIC's con sede en China y los aliados de Estados Unidos (García-Herrero, 2023). No habría un solo internet para todo el mundo sino un internet fragmentado o "Splinternet".

La literatura sobre Relaciones Internacionales siempre ha marcado la importancia de las políticas tecnológicas, no solo como políticas de desarrollo económico por sí mismas, sino como política exterior. La tecnología sería un elemento determinante a la hora de evaluar el poder y diferenciaría fuertemente entre Estados que la poseen y aquellos que no. Las TICs no escapan a esta idea.

Podemos inferir las siguientes conclusiones:

- China busca convertirse en el principal proveedor global de telecomunicaciones (infraestructura y hardware digital, 5G, fibra óptica, satélites de navegación, la nube, la informática, etc.). Por lo que, en el marco de esa visión, se embarcó desde 2015 en el proyecto de la DSR. Hoy en día dicha estrategia es más

geopolítica, con capacidad para estructurar su infraestructura digital a pesar de las reacciones estadounidenses.

- Actualmente compañías chinas (grandes, medianas y pequeñas) se expanden por el mundo creando una estructura compleja de geopolítica digital. En ese contexto, los medios de pago y el comercio online han adquirido una relevancia estratégica para poder cumplir con esos propósitos.
- Es factible estimar que, en un corto horizonte de tiempo, la DSR se convertirá en la principal prioridad en la política exterior china, para conseguir ventaja tecnológica sobre Estados Unidos, lo que le permitirá incrementar también su influencia política en el mundo.
- Con el proyecto chino se expande el grupo oligopólico de proveedores de productos y servicios digitales, centrándose en los participantes de la DSR y en las economías en desarrollo. Sin embargo, este alcance no se limita a ellos, ya que la iniciativa china llena los vacíos digitales, incluyendo a las grandes economías europeas como Alemania e Italia.
- La disputa de la geopolítica digital entre Estados Unidos y China está centrada en la infraestructura de telecomunicaciones globales y las tecnologías digitales. Sin embargo, a medida que crece esta competencia también se incrementa la posibilidad de una polarización en los ecosistemas tecnológicos globales de la información y la seguridad (dividida entre los países que dependen de las TIC's chinas y los aliados de Estados Unidos).

La guerra de los semiconductores

La guerra de semiconductores entre Estados Unidos y China no es un conflicto aislado, sino la manifestación de problemáticas profundas relacionadas con el dominio tecnológico y la competencia económica. Durante décadas, Estados Unidos mantuvo su posición como líder mundial en diseño e innovación de semiconductores, con empresas estadounidenses como Intel, Nvidia y Qualcomm liderando la industria.

Los semiconductores son la base de la economía digital moderna y el eje de los avances en meta-tecnologías críticas como la Inteligencia Artificial (IA), las redes

5G y los sistemas militares avanzados. Como resultado, el control sobre la producción y la innovación en semiconductores se ha vuelto central para el equilibrio de poder global, lo que la convierte en una de las industrias estratégicamente más importantes del mundo.

En la rivalidad entre Estados Unidos y China, los semiconductores han surgido como un campo de batalla crucial y ambos países reconocen que el dominio en este campo podría determinar el liderazgo global en innovación tecnológica y seguridad nacional.

Sin embargo, la capacidad de producción se ha desplazado hacia el este de Asia, a Taiwán y Corea del Sur. Taiwán Semiconductor Manufacturing Company (TSMC) se ha convertido en el mayor fabricante de chips por contrato del mundo.

Este cambio ha expuesto vulnerabilidades en la cadena de suministro global, en particular para Estados Unidos, que sigue dependiendo en gran medida de proveedores extranjeros para sus semiconductores más avanzados.

En el centro de este conflicto entre Estados Unidos y China se encuentra la ambición de China de lograr la autosuficiencia tecnológica. En el marco de la iniciativa “Hecho en China 2025”, China ha impulsado agresivamente el desarrollo de su industria nacional de semiconductores, invirtiendo miles de millones de dólares en investigación y desarrollo (I+D) y tratando de reducir su dependencia de chips fabricados en el extranjero (CSIS,2026).

Desde hace casi dos décadas, tanto Estados Unidos como China están tratando de asegurar su acceso a la producción de semiconductores de Taiwán, con Estados Unidos alentando a TSMC a expandir su capacidad de fabricación en Estados Unidos y China haciendo movimientos estratégicos para desarrollar sus propias capacidades de semiconductores.

La guerra de semiconductores entre Estados Unidos y China no solo tiene que ver con quién controla la producción de chips, sino también con quién liderará el panorama tecnológico mundial en el siglo XXI.

El problema para América Latina

Hay una nueva desigualdad global que, disfrazada con la inocencia del lobo en la manada, expone el riesgo inminente que sobreviene para América Latina en caso de quedar confinada a la oprobiosa servidumbre de exportar datos brutos gratuitos e importar inteligencia arancelada. Una repetición actualizada del intercambio desigual que dio origen a la teoría de la dependencia.

Pensando desde la periferia amerita trazar un diagnóstico y un pronóstico sobre el porvenir cognitivo de nuestra región en caso de persistir las impositivas y asimétricas reglas de juego actuales. Es preciso fijar un estándar analítico ante las oleadas extractivas que derivan de la fragmentación mundial, porque nuestra región está pasando de la exportación de materias primas a una exportación masiva de datos crudos (rostros, ubicaciones y datos biométricos) que son procesados por las potencias extranjeras.



Figura 2. Las instituciones latinoamericanas pagan anualmente 60.000 millones de dólares para usar servicios de nube externos. Brasil lidera el gasto regional con el 38% de este mercado, seguido de cerca por México. Fuente: elaboración propia.

1. Soberanía y poder en la era de la fragmentación

En la estructura actual del poder, el instrumento digital ya no es un simple instrumento técnico o logístico de intercomunicación y desplazamiento como había sucedido con la irrupción de las TICs a fines del siglo XX. Ahora se ha convertido

en un vehículo primario, excluyente y coercitivo de acceso discriminado a un mejor conocimiento y apropiación cognitiva de la realidad material.

Cualquier quiebre, alteración, subordinación o acceso no soberano a dicho conocimiento deriva en una desventaja estratégica inmediata y crecientemente irreversible dentro de la ecuación fundamental que compone la alta política contemporánea, donde soberanía y poder se co-construyen y retroalimentan.

Asistimos a una doble fragmentación del mapa mundial: por un lado, experimentamos una fractura geopolítica que balcaniza las capacidades de los Estados periféricos, característica propia de un mundo fragmentado. Por otro lado, se acrecienta una fragmentación social respecto al acceso a esos instrumentos digitales, segmentando a las poblaciones en base a su nivel y capacidad de inserción en los flujos globales de información.

Esta matriz asincrónica e híbrida determina que el acceso a los recursos estratégicos posea hoy un componente, entre otros varios, que es estrictamente digital. Cada recurso material, yacimiento mineral o reserva acuífera pueden ser nominalmente nacionales y estar protegidos por las leyes formales del Estado westfaliano, pero si el acceso digital a la información y el procesamiento de los datos territoriales son extranjeros, la soberanía real se diluye y queda en discusión. Esta forma fragmentada de acumulación, que intercambia asimétricamente recursos y conocimiento, supone y demanda una resignificación de la soberanía tradicional.

Esta dislocación entre la materia y el dato constituye el núcleo duro de la dependencia posmoderna. Los aparatos burocráticos del Estado continúan atrapados en lógicas arcaicas sobre el control territorial o la propiedad jurídica de dicho control, ignorando que mientras tanto y a toda velocidad las corporaciones transnacionales operan en una dimensión territorial diferente, vinculadas a territorialidades intangibles que operan sobre esos territorios tangibles.

El actor que controle el flujo informático detenta el control de la inteligibilidad del territorio en cuestión, vaciando de contenido la autoridad formal de nuestras naciones periféricas sobre un territorio determinado. Esta mencionada fragmentación social del acceso profundiza la asimetría, rompiendo el tejido social

comunitario e impidiendo la construcción de una respuesta unificada frente a este asedio tecno-político.

Analizar críticamente la soberanía digital exige una ruptura epistemológica que asuma la totalidad del fenómeno sin dejarse tentar por los atajos y las zonas de confort: la tecnología no es un factor neutral de desarrollo, sino un dispositivo de disciplinamiento y extracción de valor de última generación que rediseña las fronteras del subcontinente sin necesidad de movilizar a los ejércitos tradicionales.

2. El flujo de información y el mapa de las asimetrías

La información territorial es, por definición, la primera aproximación al control territorial fáctico. El despliegue de las plataformas digitales contemporáneas ha operado una exaptación de los saberes geográficos de seguridad nacional, trasladándolos desde los ministerios de Defensa hacia los servidores privados de los gigantes tecnológicos transnacionales.

El mapeo pormenorizado y el escaneo de islas, costas, selvas y ciudades —bajo el eufemismo de la "democratización de la información"— no se corporiza en un beneficio de acceso universal sino todo lo contrario. Representa la entrega material de información estratégica nacional a favor de inversores privados y actores transnacionales o extrarregionales.

La cartografía territorial asimétrica disuelve la soberanía racional legal de los países de la periferia y permite que las potencias transnacionales capten y monitoreen en tiempo real las vulnerabilidades, las líneas de conectividad y las riquezas del subsuelo periférico, administrando la gobernabilidad del territorio desde una distancia calculada y a costo cero para el mando corporativo.

Esta transparencia desprotectora e inducida sobre el territorio periférico contrasta drásticamente con la opacidad hermética que las grandes corporaciones imponen sobre sus propios modelos de penetración cognitiva.

El margen latinoamericano es obligado a permanecer legible, expuesto y auditable para el algoritmo global, mientras que el diseño de la IA y las bases académicas permanecen ocultas detrás del secreto comercial.

Los mapas digitales contemporáneos no reflejan la geografía física del continente, sino que la regentean políticamente, trazando rutas logísticas artificiales y aislando regiones enteras en base a criterios estrictamente comerciales. La selva, el litoral y el tejido urbano periférico dejan de ser la sede “natural” de comunidades históricas originarias y pasan a convertirse en variables de flujo propias del mercado mundial, consolidando regímenes de soberanía compartida donde el Estado formal retiene la carga burocrática del orden público, con sus costos y conflictos, mientras el actor extrarregional usufructúa la riqueza cognitiva que proviene de los datos de la riqueza geográfica.

3. El rol del crimen organizado

El rol del crimen organizado en la apropiación de datos funciona como un intermediario operativo y brazo extractor que alimenta el mercado negro global y las estrategias híbridas de las grandes potencias. El crimen organizado transnacional está dejando en segundo plano los mercados físicos tradicionales (narcotráfico), dirigiéndose hacia el mercado digital donde se mercantilizan los datos.

Los grupos delictivos ejecutan cuatro actividades relacionadas con la disputa global por la soberanía de los datos:

1. El crimen como servicio (CaaS)

Las organizaciones criminales evaden el alto nivel de sofisticación técnica interna y subcontratan infraestructura digital a través del modelo Cybercrime-as-a-Service (CaaS). El despliegue masivo de ransomware y extorsiones basadas en el robo de datos (ejecutados por carteles digitales o franquicias como LockBit o ShinyHunters), extraen gigabytes de información crítica de corporaciones y gobiernos de la periferia y la semiperiferia. Estos datos se empaquetan y se venden al mejor postor en plataformas de la dark web (Microsoft, 2025).

2. Lavado de ingresos ilícitos provenientes del robo de datos

Los datos robados —secretos comerciales, código de software, modelos de IA, bases ciudadanas de datos— se transaccionan internacionalmente mediante

criptomonedas y canales financieros no centralizados. Así el crimen organizado monetiza los recursos estratégicos de un Estado y blanquea capitales de sus otras operaciones físicas transnacionales.

3. Actores proxy de las amenazas híbridas estatales

En la geopolítica actual, las fronteras entre el crimen organizado, el hacktivismo y las operaciones de inteligencia de las potencias centrales están difuminadas. Los Estados soberanos utilizan a grupos cibercriminales como actores proxy (corsarios digitales). Esto otorga a las potencias una ventaja estratégica doble:

- El Estado puede argumentar que el robo de información estratégica, de propiedad intelectual o de datos biométricos fue obra de delincuentes comunes, negando un ataque geopolítico coordinado.
- Los datos de infraestructura crítica digital robados por las mafias terminan nutriendo los aparatos de espionaje o desestabilización de las potencias competidoras.

4. Captura de datos para control territorial y desestabilización

A nivel local de América Latina) las mafias organizadas roban bases de datos estatales o de telecomunicaciones con objetivos políticos y de control. Utilizan la información filtrada para mapear instituciones, corromper o extorsionar a servidores públicos de alto nivel y desplegar campañas de desinformación para socavar la legitimidad. Al debilitar la soberanía del Estado sobre su propio territorio y sus datos, el crimen organizado facilita la penetración de intereses geopolíticos externos

El ejemplo más documentado de la utilización china del cibercrimen como actor proxy es el grupo APT41 (también conocido por firmas de ciberseguridad como Wicked Panda, Bronze Atlas o Winnti) (Resecurity, 2025).

Este grupo opera amparado por el Ministerio de Seguridad del Estado (MSS) ejecutando espionaje político y geopolítico para el gobierno en el horario laboral y ataques criminales de extorsión y robo de datos en beneficio propio por las noches.

4. La subjetividad contractualista y la expropiación

Esta dominación tecno-colonial-criminal se despliega con esplendor en los márgenes y fronteras urbanas del sistema, donde la ley del desarrollo desigual y combinado amalgama coacciones premodernas con tecnologías de última generación. Esta disímil amalgama supone una baja capacidad de retención soberana de los procesos de creación, producción y reproducción de la riqueza expresada en términos de *know how* avanzado. El acceso a las tecnologías de última generación es exógeno, en calidad de actores recipiendarios de flujos cognitivos importados.

Fuera de la matriz urbana, las numerosas comunidades originarias de la región sí detentan de facto la riqueza de los recursos estratégicos, aunque sea bajo títulos de propiedad precarios, propios de una cultura intrínsecamente no contractualista que fundamenta su legitimidad en el arraigo histórico y la memoria viva del territorio y no en las actas jurídicas de los tribunales capitalistas.

Las plataformas digitales usufructúan esta brecha metodológica entre información dada sin procesar e información recibida procesada y operan como el instrumento idóneo para moldear e imponer nuevas subjetividades artificiales sobre la propiedad de los recursos, construidas alrededor de la propiedad y el gerenciamiento de la información.

A través de la imposición de una nueva nomenclatura contractual de base digital, las corporaciones transnacionales desarticulan la cohesión comunitaria propia del margen sistémico, convirtiendo los saberes ancestrales en datos cuantificables y expropiables, forzando a los actores locales a subordinarse a un código lingüístico ajeno a fin de evitar un colapso civilizatorio que podría dejarlos completamente fuera del mapa de la existencia económica global.

Esta modelación coercitiva de la subjetividad periférica es el triunfo más invisible y letal de la nueva imperialidad cognitiva, dando contexto político a la conocida frase de que “el conocimiento es poder”. Al colonizar mental y operativamente la forma en que las poblaciones locales perciben, conciben y decodifican su propia riqueza y su relación con su propio territorio, las plataformas digitales anulan todo germen posible de pensar con términos propios alguna forma de resistencia soberana,

anclando la parálisis en la misma raíz psíquica del individuo. La captura del conocimiento supone una concomitante captura del lenguaje y de toda forma posiblemente independiente de comprensión de la naturaleza y el ambiente común. La cultura contractualista, introducida a través de la procedimentalidad corporativa, reduce la existencia social a transacciones comerciales atomizadas, disolviendo los lazos de solidaridad orgánica del cosmos periférico. Las comunidades originarias se ven obligadas a disputar la posesión de sus selvas y cuencas hídricas dentro de una conceptualización jurídica digitalizada diseñada ex profeso para asegurar su derrota.

El margen sistémico, urbano y no urbano, se transforma en un laboratorio de experimentación antropológica y económica, donde el factor delictivo local y el capital transnacional co-soberanizan los territorios enclávicos periféricos, utilizando el vocabulario algorítmico para universalizar el despojo y disfrazar la violencia estructural con el ropaje de la modernidad técnica.

5. La autoorganización urbana y el manejo de la micro información

Esta imposición totalizante derivada del control autoritario de la información produce que los fenómenos de resistencia y contra-hegemonía dentro de este desorden mundial contemporáneo solo pueden adquirir viabilidad cuando asumen esta misma física del flujo de información mediante un cambio de mano y de mando, conservando el formato y cambiando el dominio.

Las organizaciones sociales urbanas y las pertenencias comunitarias incrementan sus posibilidades de autoorganización real y supervivencia únicamente cuando manejan, controlan y comparten información estratégica generada por sus propios nodos y redes moleculares de inserción social. Los antiguos modos reivindicativos, aunque permanecen y mantienen vigencia, son escasos si no construyen y cuentan con mecanismos aptos para la penetración en la red. Los circuitos se retroalimentan, ya que no hay comunicación sin política y no hay política sin comunicación (Villa Guzmán y Emmerich, 2013). La simple penetración en la red no es un factor suficiente para disrumpir el entramado social coercitivo y las formas tradicionales de presentación de demandas tampoco.

Romper la escenografía enmascarada impuesta por el centro exige que el margen autogestione su propia legibilidad, su propio lenguaje y su propio discurso. La producción y gerenciamiento de datos propios sobre la microfísica territorial, la distribución de recursos viales y la economía del recurso fragmentario son los únicos insumos capaces de restar centralidad al comando corporativo, permitiendo a las comunidades organizadas trazar rumbos de autonomía relativa y defender su territorialidad frente al asedio de los órdenes híbridos y para-estatales que abrumen la periferia.

Pudiera parecer ilusoria y fantástica una consigna de reapropiación de la soberanía de datos mediante la autogestión de los recursos fragmentarios presentes en el propio territorio. En el proceso obran procesos contradictorios, un doble andarivel en el que se mueve la soberanía de datos:

- Uno es el carácter no contractualista de la soberanía territorial, que presiona por ser modificado y que figura como viejo instrumento de intervención colonizadora.
- El otro es el carácter territorial de la soberanía real, propio de una territorialidad definitoria de identidades, algo que no posee ni podrá poseer el capturador de datos.

La autoorganización urbana en el siglo XXI ya no depende de las antiguas consignas ideológicas del dualismo clasista tradicional. Ahora se define por la capacidad de construir infraestructuras de comunicación paralelas y autónomas. Cuando un nodo comunitario genera su propia cartografía social, decidiendo sobre su espacio y evadiendo sus flujos internos del control del algoritmo corporativo, implementa un acto de insurrección epistemológica.

La información generada desde el margen y el afuera actúa como un blindaje estratégico frente a las capacidades de control a distancia de las instituciones hegemónicas. El manejo de los datos permite a las organizaciones sociales anticipar los desplazamientos del capital transnacional, mitigar los riesgos de la violencia encubierta y estabilizar el entorno bajo una racionalidad propia. Puede llegar incluso a desfigurar los mecanismos de hiperrealidad conformados por el capital

transnacional y quitar los rasgos de evidencia que postula la resignificación fabricada por los exportadores de conocimiento.

La resistencia adquiere así una estructura científica. El caos inducido por la exclusión social y el arrinconamiento extractivo es reconvertido por la propia comunidad en un orden alternativo disonante ante el intento de control centralizado del Estado y las corporaciones.

Conclusión: la señal digital como medición de soberanía

La brecha digital contemporánea entre proveedores de datos y exportadores de conocimiento no es un problema técnico de conectividad o una simple carencia de infraestructura que pudiera resolverse con el voluntarismo inversionista del libre mercado, cosa de por sí cercana a lo imposible. Constituye en cambio una variable de asimetría estatal de nivel geopolítico. Es un problema territorial, de soberanía y de poder. En consecuencia, es un problema geopolítico.

Una baja señal de internet es, por definición ontológica, una soberanía de baja intensidad. Delimita la frontera entre las naciones soberanas que deciden sobre el algoritmo global y las entidades subordinadas del margen sistémico que padecen las estrategias del control transnacional que se ejerce sobre ellas.

Buscamos proveer el marco metodológico preciso y la densidad conceptual de la ciencia dura para resolver la "falla" epistemológica de nuestro tiempo, dotando al margen latinoamericano de la conceptualización analítica necesaria para pensarse a sí mismo de forma integral, deconstruyendo la ausencia ficticia del Estado y reclamando con suficiencia su derecho a la totalidad del porvenir histórico. Entendiendo que la propiedad de los datos y la construcción de conocimiento propio representan la soberanía del margen en el siglo XXI (Emmerich, 2024).

Bibliografía

- Castellanos, Rodrigo (2023). *Cables submarinos: China y Estados Unidos pelean por las arterias de internet*. El Orden Mundial. Recuperado el 23 de julio de 2026 en <https://elordenmundial.com/cables-submarinos-guerra-internet-estados-unidos-china/>

- CSIS (2026). *China's Localization Drive in Semiconductors Gains Impetus from Allied Chip Export Controls*. Recuperado el 23 de julio de 2026 en <https://www.csis.org/analysis/chinas-localization-drive-semiconductors-gains-impetus-allied-chip-export-controls>
- Emmerich, Norberto (2024). *Márgenes*. Editorial Biblos, Buenos Aires, Argentina.
- García-Herrero, Alicia (2023). *La bifurcación tecnológica*. Política Exterior. Recuperado el 23 de julio de 2026 en <https://www.politicaexterior.com/la-bifurcacion-tecnologica/>
- Microsoft (2025). *Cybercrime-as-a-Service, Explained*. Recuperado el 23 de julio de 2026 en <https://www.microsoft.com/en-us/corporate-responsibility//topics/cybersecurity/stories/what-is-caas/>
- Nye, J. S. (2021). *Soft power: the evolution of a concept*, Journal of Political Power, 14(1), 196-208.
- Orbe León, Jorge (2021). *Covid19 y la pandemia económica global*. Instituto de Altos Estudios Nacionales, Ecuador.
- Resecurity (2025). *APT 41: Threat Intelligence Report and Malware Analysis*. Recuperado el 23 de julio de 2026 en <https://www.resecurity.com/blog/article/apt-41-threat-intelligence-report-and-malware-analysis>
- Shen, Xinmei (2026). *"Skynet", China's massive video surveillance network*. Recuperado el 23 de julio de 2026 en <https://www.scmp.com/abacus/who-what/what/article/3028246/skynet-chinas-massive-video-surveillance-network>
- Villa Guzmán, Carlos Antonio y Emmerich, Norberto (2013). *La política de la comunicación. Por qué las sociedades son mediáticamente definidas y sus consecuencias*. Universidad de Guadalajara, México.
- Wallerstein, Immanuel (2005). *Análisis de sistemas-mundo. Una introducción*. Editorial Siglo XXI. México.
- ZNews (2026). *El presidente chino, Xi Jinping, asiste a la Conferencia Mundial de Inteligencia Artificial*. Recuperado el 23 de julio de 2026 en

<https://www.vietnam.vn/es/chu-tich-trung-quoc-tap-can-binh-du-hoi-nghi-ai-the-gioi>