ISSN 0719-4110

CIEE
CENTRO DE INVESTIGACIÓN Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL

CUADERNO DE TRABAJO Nº4-2024

NAVEGANDO LA SOBERANÍA DIGITALDEL CIBERESPACIO

Academia Nacional
de Estudios Políticos
y Estratégicos
www.anepe.cl

CUADERNOS DE TRABAJO es una publicación orientada a abordar temas vinculados a la Seguridad y Defensa a fin de contribuir a la formación de opinión en estas materias.

Los cuadernos están principalmente dirigidos a tomadores de decisiones y asesores del ámbito de la Defensa, altos oficiales de las Fuerzas Armadas, académicos y personas relacionadas con la comunidad de defensa en general.

Estos cuadernos son elaborados por investigadores, académicos y colaboradores del CIEE de la ANEPE, pero sus páginas se encuentran abiertas a todos quienes quieran contribuir al pensamiento y debate de estos temas.

Recordamos a los autores que el Cuaderno de Trabajo está comprometido con la publicación de artículos originales e inéditos que difundan conocimiento actualizado en materias de seguridad, defensa y ciencias sociales afines, con el fin de aportar y transferir, con el propósito fundamental de aportar al debate académico múltiples enfoques que enriquezcan el análisis, la reflexión y la interpretación en torno a los temas disciplinares propios de la seguridad, la defensa y las ciencias sociales.

Antes de imprimir este Cuaderno, piense en el medio ambiente.

CUADERNO DE TRABAJO DEL CENTRO DE INVESTIGACIONES Y ESTUDIOS ESTRATÉGICOS es una publicación electrónica del Centro de Investigaciones y Estudios Estratégicos de la Academia Nacional de Estudios Políticos y Estratégicos y está registrada bajo el **ISSN 0719-4110 Cuad. Trab., - Cent. Estud. Estratég.**
Dirección postal: Avda. Eliodoro Yáñez 2760, Providencia, Santiago, Chile.
Sitio Web www.anepe.cl. Teléfonos (+56 2) 2598 1000, correo electrónico ciee@anepe.cl

NAVEGANDO LA SOBERANÍA DIGITAL DEL CIBERESPACIO

Dr. Cristian Barría Huidobro♦

"La soberanía digital es la nueva frontera en el ciberespacio; un terreno donde la libertad y el control deben encontrar un equilibrio justo."

Shoshana Zuboff, autora de "El capitalismo de vigilancia"

RESUMEN

La soberanía digital se refiere al control que una nación ejerce sobre su espacio digital, crucial para proteger sus intereses en un mundo interconectado. Un ejemplo de esto es el Gran Cortafuegos de China, que representa la transición de fronteras físicas a digitales. La ausencia de límites físicos en el ciberespacio plantea desafíos singulares para los Estados que intentan regular el flujo de datos y salvaguardar sus ecosistemas digitales. Este concepto resalta la necesidad de que los países afirmen su derecho a gobernar el contenido y la infraestructura en línea, asegurando la seguridad y el cumplimiento de las leyes nacionales. Además, la influencia de las grandes empresas tecnológicas tiene implicaciones geopolíticas significativas. Estas empresas, mediante su dominio de las plataformas digitales y la infraestructura de datos, pueden dar forma al discurso público, influir en los resultados políticos y alterar dinámicas socioeconómicas a nivel global. Su poder complica el panorama de la soberanía digital, destacando la necesidad de marcos de gobernanza integrales que equilibren la innovación con la protección de la integridad digital tanto nacional como global.

Palabras clave: Soberanía digital, ciberespacio, ciberseguridad

ABSTRACT

Digital sovereignty refers to the control a nation exercises over its digital space, crucial for protecting its interests in an interconnected world. An example of this is China's Great Firewall, which represents the shift from physical to digital borders. The absence of physical boundaries in cyberspace presents unique challenges for states attempting to regulate data flow and safeguard their digital ecosystems. This concept highlights the need for countries to assert their right to govern online content and infrastructure, ensuring security and compliance with national laws. Furthermore, the influence of big tech companies has significant geopolitical implications. These companies, through

♦ Centro de Investigación en Ciberseguridad, CICS. Universidad Mayor, Chile ORCID: https://orcid.org/0000-0002-5840-7407

their dominance of digital platforms and data infrastructure, can shape public discourse, influence political outcomes, and alter socioeconomic dynamics on a global scale. Their power complicates the landscape of digital sovereignty, underscoring the need for comprehensive governance frameworks that balance innovation with the protection of both national and global digital integrity.

Keywords: Digital sovereignty, cyberspace, cybersecurity

INTRODUCCIÓN

El concepto de soberanía ha evolucionado con el pasar de los siglos, forjando el espectro político y las relaciones internacionales de la humanidad desde sus orígenes tribales hasta las grandes coaliciones de potencias mundiales de hoy[1]. La soberanía se refiere a la autoridad o poder supremo que un Estado tiene sobre su territorio, su población y sus procesos de toma de decisiones[2].

Históricamente, el concepto de soberanía se remonta a civilizaciones antiguas como Mesopotamia y Egipto, donde los gobernantes tenían poder absoluto sobre sus territorios. La idea de soberanía se desarrolló aún más durante la Edad Media, con el surgimiento del sis-

Figura 1: "Ratificación del Tratado de Münster", cuadro de Gerard ter Borch.

Fuente: The Religious Toleration and Peace (RETOPEA) project, https://retopea.eu/s/de/item/7657

1 PHILPOTT, D. Sovereignty: An introduction and brief history. Journal of international affairs, 1995, 353-368.
2 KUMAR, V. Explain the provisions of state: Condition of statehood, territory and underlying principles, sovereignty under international law - legal vidhiya. Legal Vidhiya, 2024. https://legalvidhiya.com/explain-the-provisions-of-state-condition-of-statehood-territory-and-underlying-principles-sovereignty-under-international-law/

tema feudal y el auge de las monarquías en Europa. El Tratado de Westfalia de 1648 a menudo se considera un momento decisivo en la historia de la soberanía, ya que estableció el principio de soberanía estatal y reconoció la independencia de los Estados de la interferencia externa. Esto sentó las bases para el sistema moderno de Estados-nación y el concepto de integridad territorial[3].

La soberanía es un principio fundamental del sistema estatal moderno, que otorga a los Estados la autoridad para gobernar sus territorios y tomar decisiones sin interferencia externa. Sin embargo, la soberanía también ha sido una fuente de conflicto y tensión, ya que los Estados a menudo chocan por cuestiones de integridad territorial, autodeterminación y derechos humanos. La tensión entre la soberanía estatal y la responsabilidad de proteger ha sido un debate clave en las relaciones internacionales, especialmente en casos de intervención humanitaria y transgresiones contra los derechos humanos.

Individuos influyentes han desempeñado un papel crucial en la configuración de la historia de la soberanía y han contribuido a este campo con sus ideas y acciones. Filósofos políticos como Jean Bodin[4], Thomas Hobbes[5] y John

Figura 2: Retrato de Hugo Grocio, por Michiel Jansz. van Mierevelt, 1631. El trabajo de Grocio sentó las bases de numerosas iniciativas legales internacionales, que hoy en día posibilitan la existencia de organizaciones como la ONU.

Fuente: Elaboración propia.

3 OSIANDER, A. Sovereignty, international relations, and the Westphalian myth. International organization, 2001, 55(2), 251-287.
4 BODIN, J. On sovereignty: four chapters from the six books of the commonwealth. 1992. Cambridge University Press.
5 HOBBES, T. Leviathan. 2002.

Locke[6] han explorado el concepto de soberanía en profundidad, proporcionando marcos teóricos para comprender la naturaleza de la autoridad política y el gobierno. La noción de Bodin de "soberanía como poder absoluto e indivisible" sentó las bases para las teorías modernas de la soberanía estatal, mientras que Hobbes y Locke contribuyeron al desarrollo de la teoría del contrato social y la idea de la soberanía popular.

En la era moderna, figuras como Hugo Grotius[7], Immanuel Kant[8] y Woodrow Wilson[9] han ampliado aún más el discurso sobre la soberanía y el derecho internacional. Grotius, conocido como el "padre del derecho internacional", enfatizó la importancia de las normas jurídicas y los tratados para regular las relaciones entre los Estados y garantizar la cooperación pacífica. La idea de paz perpetua de Kant y el concepto de una liga de naciones inspiraron la creación de las Naciones Unidas y la promoción de la gobernanza global. Los Catorce Puntos de Wilson y su visión de la autodeterminación influyeron en el acuerdo posterior a la Primera Guerra Mundial y el establecimiento de nuevos Estados-nación.

A pesar de sus importantes contribuciones a la teoría política y las relaciones internacionales, la soberanía también ha enfrentado críticas y desafíos en el mundo contemporáneo. La globalización, la interdependencia y el surgimiento de actores no estatales han erosionado la noción tradicional de soberanía estatal, lo que ha llevado a cuestionamientos sobre la relevancia y aplicabilidad de la soberanía en un mundo complejo e interconectado. Cuestiones como el cambio climático, el terrorismo transnacional y las pandemias han resaltado la necesidad de cooperación y acción colectiva más allá de las fronteras nacionales, desafiando la primacía de la soberanía estatal.

En la era digital moderna, donde la irrupción de internet, la inteligencia artificial y el ciberespacio en general han transformado el quehacer humano en sus diversas aristas, la soberanía también se ha enfrentado a nuevos desafíos que han motivado el surgimiento de otra concepción de este concepto: la soberanía digital o cibersoberanía.

"...la soberanía también se ha enfrentado a nuevos desafíos que han motivado el surgimiento de otra concepción de este concepto: la soberanía digital o cibersoberanía."

El concepto de cibersoberanía (i.e., soberanía en el ciberespacio) se refiere a la idea de que los países tienen la autoridad para gobernar Internet dentro de sus fronteras y controlar a qué contenido pueden acceder sus ciudadanos, incluyendo la capacidad estatal de regular el contenido en línea, supervisar los flujos de datos y hacer cumplir las leyes relacionadas con la ciberseguridad[10]. Este concepto ha cobrado cada vez mayor relevancia en la era digital actual, ya que cada vez más aspectos de nuestra vida diaria se realizan en

6 LOCKE, J. Two treatises of government. Cambridge university press, 1967.
7 GROTIUS, H. Hugo Grotius on the law of war and peace. Cambridge University Press, 2012.
8 PEACE, P. Immanuel Kant Perpetual Peace: A Philosophical Sketch.
9 WILSON, W. The Fourteen Points Address. The Record of American Diplomacy: Documents and Readings in the History of American Foreign Relations, 3rd ed.(New York: Alfred A. Knopf, 1954), 1918, 459-461.
10 SAAIDA, Mohammed. Digital Sovereignty. 2024,1-12.

línea. El debate en torno a la cibersoberanía gira en torno a cuestiones de privacidad, libertad de expresión, seguridad nacional y el equilibrio entre el control gubernamental y los derechos individuales en el ciberespacio.

ANTECEDENTES

El concepto de cibersoberanía tiene sus raíces en la noción tradicional de soberanía, que es la idea de que los Estados tienen la autoridad máxima dentro de sus territorios. En el pasado, esta autoridad se limitaba en gran medida al espacio físico, pero con el auge de Internet, los Estados han tenido que lidiar con la forma de extender su soberanía al ámbito virtual. El concepto de cibersoberanía surgió como respuesta a los desafíos que planteaba la naturaleza sin fronteras de Internet y la necesidad de que los Estados afirmaran su control sobre el ciberespacio.

No obstante, la idea de traer y ejercer soberanía en el mundo digital experimentó una destacada pero infructuosa resistencia por parte de los teóricos del ciberespacio: el año 1996 durante el Foro Económico Mundial en Davos (Suiza), el poeta, activista político y ciberlibertario John Perry Barlow publicó la "Declaración de Independencia del Ciberespacio"[11], manifestó que expresaba un firme rechazo a la interferencia estatal en el dominio digital, protegiendo su libertad e independencia. Sin embargo, la relevancia del ciberespacio anularía toda opción de este conjunto de ideales, impulsando a países, empresas y agrupaciones a buscar fórmulas para adaptar su soberanía al nuevo entorno cibernético.

Es en ese entonces cuando los teóricos dejan de preguntarse si la web podía ser gobernada, dando paso a un problema mayor, a saber, cómo lograrlo. Dado que se produce una tensión significativa entre la soberanía estatal, basada en los límites territoriales, y el espacio no territorial creado por un espacio no territorial ni demarcado (como el ciberespacio), la forma tradicional de ejercer soberanía se ve afectada. Por lo tanto, el entendimiento y ejercicio de la cibersoberanía presenta matices heredados de la comprensión que cada Estado tiene respecto de su propia soberanía tradicional. Veremos a continuación algunos casos relevantes.

"Dado que se produce una tensión significativa entre la soberanía estatal, basada en los límites territoriales, y el espacio no territorial creado por un espacio no territorial ni demarcado (como el ciberespacio), la forma tradicional de ejercer soberanía se ve afectada."

China

El enfoque de China hacia la cibersoberanía se centra en consolidar el control sobre su panorama digital para salvaguardar los intereses nacionales, mantener la estabilidad política y fomentar el crecimiento económico[12]. Un elemento central de este enfoque es el concepto de Gran Cortafuegos, un amplio sistema de controles de Internet y mecanismos de censura que regulan el flujo de información dentro y a través de las fronteras de China. Esta barrera

11 BARLOW, J. P. (1996). Cyberspace Independence Declaration http://www. eff. org/pub/Publications. John_Perry_Barlow/barlow_0296. declaration.

12 WANG, A. (2020). Cyber Sovereignty at Its Boldest: A Chinese Perspective. Ohio St. Tech. LJ, 16, 395.

digital sirve como contraparte moderna de la histórica Gran Muralla, diseñada para proteger la integridad de la nación en un ciberespacio sin fronteras.

El Gran Cortafuegos es un componente crítico de la estrategia de cibersoberanía de China, que permite al gobierno filtrar y monitorear el contenido en línea. Al bloquear el acceso a sitios web extranjeros y controlar la difusión de información, el gobierno chino puede suprimir la disidencia, impedir la difusión de material políticamente sensible y mantener una narrativa alineada con sus políticas. Este control se extiende a las plataformas de redes sociales, motores de búsqueda y otras herramientas de comunicación digital, donde el contenido es rigurosamente monitoreado y censurado.

Además de la censura, la cibersoberanía de China abarca amplias prácticas de vigilancia. El gobierno emplea tecnologías avanzadas, incluida la inteligencia artificial y el análisis de big data, para monitorear las actividades en línea de los ciudadanos. Este aparato de vigilancia está integrado en el sistema de crédito social, donde se rastrea y califica el comportamiento de los individuos, lo que influye en su acceso a servicios y oportunidades. Estas medidas refuerzan el control estatal y promueven un clima de autocensura entre los ciudadanos.

China también prioriza el desarrollo de tecnología autóctona para reducir la dependencia de empresas tecnológicas extranjeras y reforzar su cibersoberanía. A través de iniciativas como el plan *Made in China 2025*, el gobierno pretende lograr la autosuficiencia tecnológica en sectores críticos, incluidos los semiconductores, la inteligencia artificial y las telecomunicaciones. Este impulso hacia la innovación se ejemplifica con el ascenso de gigantes tecnológicos chinos como Huawei, Tencent y Alibaba, que desempeñan papeles fundamentales en el avance de la infraestructura digital y la influencia global del país.

A nivel internacional, China aboga por un modelo de cibersoberanía que enfatice el derecho de los Estados a controlar sus propios dominios digitales sin interferencia externa. Esta postura contrasta con los modelos de gobernanza de Internet más abiertos y globales promovidos por los países occidentales. En foros como las Naciones Unidas, China impulsa normas y políticas que legitiman el control estatal sobre Internet, lo que refleja su creencia en la primacía de la soberanía nacional en la era digital.

“China aboga por un modelo de cibersoberanía que enfatice el derecho de los Estados a controlar sus propios dominios digitales sin interferencia externa.”

Al combinar censura, vigilancia, innovación tecnológica y defensa internacional, China busca dar forma a un dominio cibernético que se alinee con sus intereses nacionales y refuerce su visión de control estatal de su propio ciberespacio, convirtiéndose en uno de los principales defensores de este tipo de estrategias en la actualidad.

Rusia

Similar al caso chino, el enfoque de Rusia hacia la cibersoberanía se caracteriza por buscar el aseguramiento de su dominio digital, manteniendo el control político y afirmando su influencia tanto a nivel nacional como internacional. Un elemento central de esta estrategia es el concepto de “Internet soberana”, que prevé una infraestructura de Internet nacional capaz de operar independientemente de la Internet global. Esta iniciativa está diseñada para pro-

teger a Rusia de amenazas cibernéticas externas, mejorar las capacidades de vigilancia estatal y garantizar el control sobre el entorno de información dentro de sus fronteras[13].

La ley de "Internet soberana", promulgada en 2019, exige la creación de un Sistema de Nombres de Dominio (DNS) nacional y la instalación de tecnología de inspección profunda de paquetes (DPI). Esta tecnología permite al gobierno ruso filtrar y monitorear el tráfico de Internet, bloquear el acceso a contenido no deseado y aislar la Internet rusa (Runet) de la red global durante emergencias. El desarrollo de una Internet soberana refleja el deseo de Rusia de minimizar la dependencia de la infraestructura de Internet extranjera y reducir la vulnerabilidad a los ciberataques y sanciones externos.

El enfoque de Rusia hacia la cibersoberanía también está marcado por estrictas medidas de censura y vigilancia en Internet. El gobierno emplea una variedad de tácticas para controlar el contenido en línea, incluido el bloqueo del acceso a sitios web extranjeros, la restricción de las plataformas de redes sociales y la regulación de las fuentes de noticias en línea. El Servicio Federal de Supervisión de Comunicaciones, Tecnología de la Información y Medios de Comunicación (Roskomnadzor) desempeña un papel clave en el cumplimiento de estas regulaciones, imponiendo frecuentemente multas y bloqueando órdenes a entidades que no las cumplen. Casos de alto perfil, como el bloqueo de LinkedIn y Telegram, ilustran el compromiso del gobierno de controlar la narrativa digital.

La vigilancia es otro componente crítico de la estrategia de cibersoberanía de Rusia. El Sistema de Actividades de Investigación Operativa (SORM) permite un seguimiento exhaustivo de las comunicaciones en línea, lo que permite a las agencias de seguridad interceptar y analizar el tráfico de Internet. Este sistema está integrado en las redes de todos los proveedores de telecomunicaciones, asegurando capacidades integrales de vigilancia estatal. El gobierno también aprovecha tecnologías avanzadas, como la inteligencia artificial y el análisis de datos, para mejorar sus operaciones de vigilancia y mantener un estricto control sobre las actividades digitales de sus ciudadanos.

"El enfoque de Rusia hacia la cibersoberanía refleja sus esfuerzos por fortalecer su dominio digital, proteger sus intereses nacionales y afirmar su influencia a nivel mundial."

Además de las medidas internas, Rusia promueve activamente su visión de la cibersoberanía en el escenario internacional. En foros como las Naciones Unidas, Rusia aboga por el principio de soberanía estatal en el ciberespacio, enfatizando los derechos de las naciones a controlar sus propios entornos digitales sin interferencia externa. Esta postura se alinea con la estrategia geopolítica más amplia de Rusia, que busca contrarrestar la influencia occidental y promover un orden mundial multipolar.

El enfoque de Rusia hacia la cibersoberanía refleja sus esfuerzos por fortalecer su dominio digital, proteger sus intereses nacionales y afirmar su influencia a nivel mundial. Al implementar una censura estricta, medidas de vigilancia y abogar por una gobernanza de Internet cen-

13 SHERMAN, J. Reassessing RuNet: Russian internet isolation and implications for Russian cyber behavior. JSTOR Security Studies Collection, 2022.

trada en el Estado, Rusia pretende mantener la estabilidad política, mejorar sus defensas cibernéticas y dar forma al futuro de las normas cibernéticas globales de acuerdo con sus objetivos estratégicos. Esta estrategia multifacética subraya el compromiso de Rusia de asegurar su soberanía en el panorama digital en rápida evolución.

Estados Unidos

El enfoque de Estados Unidos hacia la ciber soberanía se basa en un equilibrio entre garantizar la seguridad nacional, promover la prosperidad económica y defender valores democráticos como la libertad de expresión y los principios de una Internet abierta[14]. A diferencia de modelos más restrictivos, Estados Unidos defiende un ciberespacio libre y abierto, abogando por una mínima intervención gubernamental y máximas libertades individuales y corporativas dentro del dominio digital. Este enfoque está influenciado por los ideales fundamentales de libertad y libre empresa del país, lo que posiciona a Estados Unidos como líder mundial en gobernanza e innovación de Internet.

"El enfoque de Estados Unidos hacia la cibersoberanía enfatiza una Internet libre y abierta, fuertes medidas de seguridad nacional, innovación económica y la promoción de valores democráticos."

La seguridad nacional es una preocupación primordial en el enfoque estadounidense de la cibersoberanía. El gobierno ha implementado un marco sólido para proteger su infraestructura digital de las amenazas cibernéticas. Agencias clave como el Departamento de Seguridad Nacional (DHS), la Oficina Federal de Investigaciones (FBI) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) trabajan en conjunto para identificar, prevenir y responder a los ciberataques. Estados Unidos también participa en colaboraciones internacionales para reforzar la ciberseguridad global, participando en iniciativas como el Llamado de París para la confianza y la seguridad en el ciberespacio.

Las consideraciones económicas son igualmente vitales en la estrategia estadounidense. Estados Unidos apoya una próspera industria tecnológica, hogar de algunas de las empresas tecnológicas más grandes e influyentes del mundo, como Google, Apple, Microsoft y Facebook. Estas empresas impulsan la innovación, el crecimiento económico y el desarrollo de infraestructura digital global. El enfoque regulatorio del gobierno de Estados Unidos tiene como objetivo fomentar la innovación y, al mismo tiempo, abordar preocupaciones como la privacidad de los datos, las cuestiones antimonopolio y la difusión de información errónea. Legislaciones históricas, como la Ley de Privacidad del Consumidor de California (CCPA) y los debates en curso sobre las leyes federales de privacidad de datos, ejemplifican el compromiso de Estados Unidos de equilibrar el crecimiento económico con la protección del consumidor.

Los valores democráticos sustentan el enfoque estadounidense hacia la cibersoberanía. Estados Unidos aboga por una Internet abierta, interoperable, segura y confiable. Se opone a la censura estatal y promueve la libertad glo-

14 GOEl, S. National cyber security strategy and the emergence of strong digital borders. Connections, 2020 19(1), 73-86.

bal en Internet, apoyando iniciativas que protegen la libertad de expresión y el acceso a la información. El gobierno de Estados Unidos frecuentemente critica e impone sanciones a regímenes que practican una extensa censura y vigilancia en Internet, posicionándose como un defensor de los derechos digitales globales.

La influencia de las grandes empresas tecnológicas juega un papel importante en la ciberseguridad estadounidense. Estas empresas no solo dan forma a la política interna, sino que también tienen un impacto geopolítico significativo. Sus políticas sobre gestión de datos, moderación de contenidos y operaciones de mercado influyen en las normas y prácticas digitales globales. El gobierno de Estados Unidos a menudo se encuentra navegando por la compleja interacción entre estos gigantes corporativos y su marco regulatorio, con el objetivo de garantizar que sus operaciones se alineen con la seguridad nacional y el interés público.

El enfoque de Estados Unidos hacia la ciberseguridad enfatiza una Internet libre y abierta, fuertes medidas de seguridad nacional, innovación económica y la promoción de valores democráticos. Esta estrategia multifacética refleja el compromiso de Estados Unidos de liderar la gobernanza global de Internet y al mismo tiempo equilibrar los intereses de la seguridad, el crecimiento económico y las libertades individuales en la era digital.

ANÁLISIS

Comparativa entre enfoques estatales

Los tres ejemplos previamente descritos (China, Rusia y EE. UU.) reconocen la importancia de proteger sus espacios digitales contra amenazas externas y garantizar la estabilidad de su infraestructura cibernética. Los ciberataques, las filtraciones de datos y el espionaje digital plantean riesgos importantes para la seguridad nacional, la estabilidad económica y la confianza pública. En consecuencia, China, Rusia y Estados Unidos han invertido mucho en medidas de ciberseguridad, incluidos sistemas de vigilancia avanzados, marcos regulatorios y colaboraciones internacionales.

Otro punto común es la influencia de las grandes empresas tecnológicas en las políticas cibernéticas nacionales y globales. En los tres países, estas corporaciones desempeñan papeles cruciales en la configuración de los ecosistemas digitales. Ya sea a través de la innovación tecnológica, la gestión de datos u operaciones de mercado, las acciones y políticas de los gigantes tecnológicos tienen un impacto significativo en la forma en que se ejerce y mantiene la ciberseguridad.

Si bien China, Rusia y Estados Unidos dan prioridad a la ciberseguridad y la influencia de las empresas tecnológicas, sus enfoques divergen significativamente. Las estrategias de China y Rusia están marcadas por un control y una vigilancia estrictos, con el objetivo de mantener la estabilidad política y el control sobre las narrativas digitales. Ambos países priorizan la autosuficiencia tecnológica y el control estatal sobre los contenidos e infraestructuras digitales.

Estados Unidos, sin embargo, promueve una Internet abierta y libre, enfatizando las libertades individuales y una mínima interferencia gubernamental. Si bien se prioriza la seguridad y la innovación económica, el enfoque estadounidense se alinea con los valores democráticos, abogando por la libertad global en Internet y oponiéndose a la censura estatal generalizada.

Las corporaciones y la ciberseguridad

Las grandes empresas tecnológicas desempe-

ñan un papel fundamental en la configuración del panorama de la cibersoberanía, ya que sus innovaciones tecnológicas, sus prácticas de gestión de datos y el alcance global que poseen, influyen significativamente en las políticas digitales nacionales e internacionales (y viceversa). La influencia de estas empresas varía según los diferentes contextos geopolíticos, y del mismo modo que la noción de cibersoberanía es interpretado de forma diferente por las grandes potencias mundiales, la manera de interactuar con las grandes empresas tecnológicas locales (y aprovechar sus potenciales) presenta sus propios matices.

China

El gobierno chino mantiene un control estricto sobre la infraestructura y el contenido digital, utilizando gigantes tecnológicos nacionales para hacer cumplir sus políticas y ampliar su influencia. Por esto, las grandes empresas tecnológicas son parte integral de la estrategia estatal de ese país.

- **Huawei:** Proveedor mundial de equipos de telecomunicaciones y electrónica de consumo. Las tecnologías avanzadas y el amplio alcance de la empresa la han convertido en un actor clave en el desarrollo de la infraestructura digital de China. La participación de Huawei en la construcción de redes 5G tanto a nivel nacional como internacional ha generado preocupaciones sobre la seguridad nacional y la privacidad de los datos entre las naciones occidentales. El gobierno chino aprovecha las capacidades tecnológicas de Huawei para mejorar sus mecanismos de vigilancia y control, asegurando que su infraestructura digital se alinee con las políticas estatales.

- **Tencent:** Compañía con diversas empresas subsidiarias que provee servicios de internet, publicidad e inteligencia artificial. La popular plataforma de redes sociales de la compañía, WeChat, sirve como una herramienta crucial para la vigilancia y censura estatales. La amplia base de usuarios y la multifuncionalidad de WeChat (que abarca mensajería, pagos y difusión de noticias) permiten al gobierno monitorear y controlar las actividades en línea de manera efectiva. El cumplimiento por parte de Tencent de las regulaciones gubernamentales garantiza que el contenido considerado políticamente sensible sea rápidamente censurado, lo que refuerza el control del Estado sobre las narrativas digitales.

Rusia

El enfoque de Rusia hacia la cibersoberanía implica aprovechar las empresas tecnológicas nacionales para imponer el control estatal y desarrollar una infraestructura digital autosuficiente. El énfasis del gobierno en crear una “Internet soberana” refleja su deseo de minimizar la influencia extranjera y mejorar sus capacidades regulatorias.

- **Yandex:** Empresa también conocida informalmente como “el Google de Rusia”, es el principal motor de búsqueda y proveedor de servicios de Internet del país. La empresa desempeña un papel fundamental en los esfuerzos de soberanía cibernética de Rusia al garantizar que sus plataformas cumplan con las regulaciones estatales. Los algoritmos de búsqueda y las prácticas de moderación de contenido de Yandex están alineados con las políticas gubernamentales, lo que permite filtrar información políticamente sensible y promover narrativas aprobadas por el Estado. Además, las prácticas de gestión y almacenamiento de datos de Yandex están sujetas a las leyes rusas

de localización de datos, que exigen que los datos sobre los ciudadanos rusos se almacenen dentro del país.

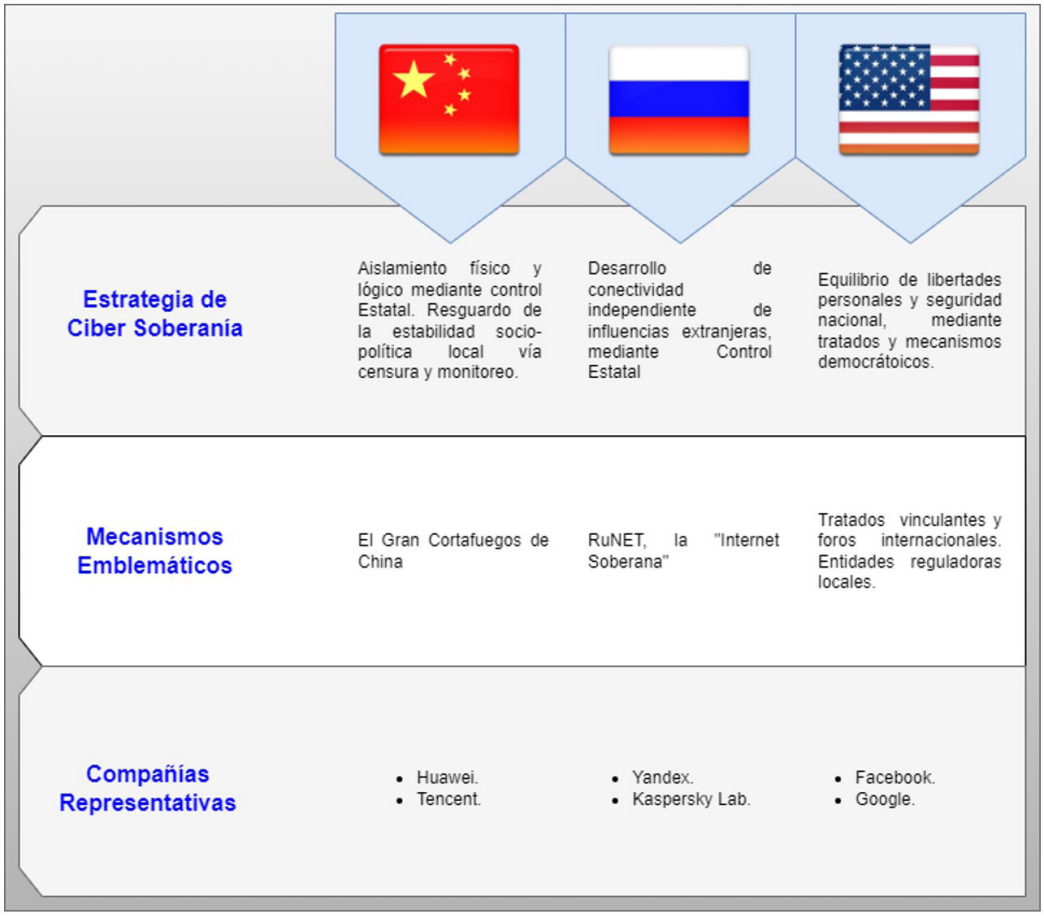
- **Kaspersky Lab:** Empresa global de ciberseguridad con sede en Moscú. La experiencia de la empresa en soluciones de ciberseguridad mejora la capacidad del gobierno para proteger su infraestructura digital de amenazas externas. Sin embargo, Kaspersky Lab ha enfrentado el escrutinio de los gobiernos occidentales por preocupaciones sobre sus posibles vínculos con las agencias de inteligencia rusas. A pesar de estas preocupaciones, la prominencia de la empresa en la industria de la ciberseguridad subraya el enfoque de Rusia en desarrollar capacidades nacionales para salvaguardar su dominio cibernético.

Estados Unidos

Por su parte, Estados Unidos adopta un enfoque más liberal en estos temas, enfatizando el papel de las grandes empresas tecnológicas en el impulso de la innovación y el crecimiento económico. Sin embargo, la influencia de estas empresas también plantea desafíos relacionados con la privacidad de los datos, la competencia en el mercado y la difusión de información errónea.

- **Google:** Líder mundial en tecnología y servicios de Internet, desempeña un papel importante en la configuración del panorama

Figura 3: Cibersoberanía, esquema comparativo entre China, Rusia y Estados Unidos.



Fuente: Elaboración propia.

digital de Estados Unidos y del mundo. El dominio de la empresa en búsquedas, publicidad y computación en la nube la ha convertido en un actor central en la industria tecnológica estadounidense. Los reguladores y formuladores de políticas examinan de cerca las prácticas de gestión de datos, las políticas de moderación de contenido y el comportamiento del mercado de Google. Cuestiones como las investigaciones antimonopolio, las preocupaciones sobre la privacidad de los datos y la difusión de información errónea en plataformas como YouTube resaltan la compleja interacción entre las operaciones de Google y la soberanía cibernética de Estados Unidos.

- **Facebook:** Actualmente transformado en subsidiaria de Meta, es posiblemente la plataforma de redes sociales más grande del mundo. El papel de la empresa a la hora de dar forma al discurso público, facilitar las conexiones sociales e impulsar la publicidad digital subraya su importante impacto en la sociedad estadounidense. Sin embargo, la participación de Facebook en controversias como el escándalo de Cambridge Analytica y su manejo del contenido político y la desinformación han provocado llamados a una mayor supervisión regulatoria. Los esfuerzos del gobierno de Estados Unidos para abordar estos desafíos reflejan la necesidad de equilibrar la innovación con la protección de los valores democráticos y la seguridad nacional.

En términos comparativos, China y Rusia están más cerca la una de la otra que Estados Unidos de cualquiera de esas dos potencias. Hay claramente dos versiones en disputa, una más abierta y otra más cerrada, basada en el control y la censura.

En China, empresas tecnológicas como Huawei y Tencent están profundamente integradas en la estrategia de cibersoberanía del Estado, apoyando los esfuerzos del gobierno para controlar el contenido y la infraestructura digitales. El cumplimiento de regulaciones estrictas por parte de estas empresas garantiza que sus operaciones se alineen con las políticas estatales, lo que refuerza el control centralizado de China sobre su dominio digital. De manera similar, el enfoque de Rusia implica aprovechar las empresas tecnológicas nacionales para imponer el control estatal y desarrollar una infraestructura digital autosuficiente. Empresas como Yandex y Kaspersky Lab desempeñan un papel crucial a la hora de alinear sus prácticas con las regulaciones gubernamentales y mejorar las capacidades de ciberseguridad de Rusia.

En contraste, el enfoque de Estados Unidos enfatiza un entorno digital más abierto y liberal, donde las grandes empresas tecnológicas impulsan la innovación y el crecimiento económico. Sin embargo, la influencia de empresas como Google y Facebook también plantea desafíos relacionados con la privacidad de los datos, la competencia en el mercado y la difusión de información errónea. Los esfuerzos regulatorios del gobierno de Estados Unidos reflejan la necesidad de equilibrar estas preocupaciones con la promoción de los valores democráticos y la seguridad nacional.

DISCUSIÓN

Si bien en el presente documento se ha tratado a la soberanía tradicional como un concepto esencialmente uniforme, cabe destacar que teóricos han propuesto diferentes tipos de soberanía, aspecto relevante al momento de analizar su equivalencia en el ciberespacio.

En este sentido destaca el trabajo de Stephen Krasner, quien identifica cuatro tipos de soberanía[15]:

- **Soberanía interna (o doméstica):** se refiere a las estructuras de autoridad dentro de un Estado y la capacidad de estas estructuras para regular eficazmente las actividades dentro de sus fronteras.
- **Soberanía de interdependencia:** este tipo aborda la capacidad de los Estados para controlar los movimientos transfronterizos y el impacto de la globalización. Implica gestionar el flujo de bienes, personas, información y capital a través de las fronteras nacionales.
- **Soberanía jurídica internacional:** Se refiere al reconocimiento de un estado por otros Estados y organizaciones internacionales. Implica el reconocimiento formal y la aceptación de la existencia de un Estado y su derecho a entablar relaciones internacionales. La soberanía legal internacional tiene que ver con el estatus legal de un Estado y su capacidad para celebrar acuerdos y tratados con otros Estados.
- **Soberanía "Westfaliana":** lleva el nombre de la Paz de Westfalia (1648), que estableció los principios de integridad territorial y no interferencia. Se centra en la exclusión de actores externos a las estructuras de autoridad interna de un Estado. Enfatiza el principio de que los Estados no deben intervenir en los asuntos internos de otros Estados, asegurando la independencia política y la autodeterminación.

Resulta interesante observar que la noción de cibersoberanía permea a los cuatro tipos de soberanía de Krasner, por lo que un mismo enfoque estatal de cibersoberanía puede tener implicaciones para cada uno de los tipos descritos.

En el caso de China, su ejercicio de la soberanía doméstica se apoya en el control extensivo de los contenidos digitales e infraestructura, siendo el Gran Muro de Fuego su ejemplo más representativo. Este tipo de medidas permiten al gobierno regular y monitorear la actividad digital dentro de sus fronteras, apalancando las capacidades técnicas y tecnológicas de empresas como Huawei y Tencent. Así, China logra establecer y hacer cumplir las normas de censura y vigilancia vigentes, asegurando que su espacio digital se mantenga alineado con las políticas de Estado.

Este control exhaustivo del nivel doméstico digital -en conjunto con el énfasis chino en la autosuficiencia tecnológica- obliga a este país a aplicar medidas a nivel transfronterizo. Desde la perspectiva de la soberanía de interdependencia, China ejerce un fuerte control en el flujo de datos que entran y salen del país, limitando la influencia extranjera en la opinión pública local. Esto se complementa con planes estatales de desarrollo tecnológico local, desarrollando mayores capacidades de independencia tecnológica, entregando a China una mayor capacidad de negociación comercial internacional, al no tener que depender de otros proveedores, a diferencia de muchos otros países.

En lo que respecta a soberanía legal internacional, China busca el reconocimiento de su modelo de cibersoberanía en foros internacionales, abogando por el principio de que los Estados deberían tener derecho a gobernar sus espacios digitales sin interferencias externas.

15 KRASNER, S. D. Sovereignty: organized hypocrisy. Princeton university press, 1999.

Si bien en un nivel más general este principio es aceptado por muchos países, bajo el supuesto de que debe respetarse la autodeterminación de cada nación (aspecto fuertemente alineado con la soberanía Westfaliana), las medidas específicas que China emplea para lograr sus objetivos tienden a generar resistencia en el mundo occidental, al considerarse muchas veces que el Estado chino transgrede la privacidad personal de sus ciudadanos.

Por su parte, Rusia también apunta a lograr un fuerte control de su soberanía doméstica, valiéndose de medidas a veces bastante literales, como la ya mencionada "internet soberana", complementando iniciativas como el DNS nacional y el empleo de tecnologías DPI. Y así como el Gran Cortafuegos chino cumple un rol a nivel doméstico y de interdependencia, la Internet soberana rusa además del control local, es parte fundamental de los esfuerzos estatales para lograr la autosuficiencia digital y minimizar la influencia extranjera (especialmente la occidental).

Rusia aboga por los principios de soberanía estatal digital y legal, formando parte de diferentes organizaciones internacionales y promoviendo normativas que legitimasen el control estatal sobre los dominios digitales. El enfoque de cibersoberanía de Rusia está profundamente arraigado en la soberanía Westfaliana. El énfasis en la creación de una Internet soberana y el amplio control estatal sobre las actividades digitales subrayan el principio de no interferencia y el derecho a gobernar su propio espacio digital independientemente de influencias externas.

Para Estados Unidos, el desafío doméstico se centra en el complejo balance entre la seguridad nacional y las libertades individuales, desplegando las competencias de diversas agencias estatales para desarrollar e implementar medidas que resguarden la infraestructura digital nacional, al tiempo que respondan a las necesidades civiles de privacidad, libre competencia e innovación. En este complejo escenario de intereses posiblemente contrapuestos, Estados Unidos se apoya también en la labor de las grandes empresas tecnológicas para crear soluciones y servicios útiles para la ciudadanía pero que se apeguen a las normativas locales.

En la arista de la interdependencia, Estados Unidos marca otra gran diferencia con China y Rusia, abrazando la globalización y navegando activamente los desafíos de una internet libre y sin fronteras. Las empresas tecnológicas norteamericanas ejercen una fuerte influencia en el escenario digital internacional, propiciando colaboraciones en materia de ciberseguridad, protección de datos personales y libre mercado. No obstante, estas firmas y sus redes son objeto constante de críticas por temas de privacidad y distribución de desinformación.

En lo legal, el gobierno estadounidense participa activamente en diferentes instancias internacionales y adscribe a tratados en materia de libertades digitales y protección de la privacidad, tal como sus empresas tecnológicas, permitiendo así una colaboración mucho más extensa que China y Rusia.

Bajo el prisma Westfaliano, Estados Unidos promueve un enfoque mucho más liberal a la cibersoberanía, a pesar de mantener su compromiso con el principio de no intervención en los asuntos internos de otros países. Sin embargo, su apoyo a una internet global y libre implica desafíos más complejos para poder respetar dicho principio. Hoy en día es bastante simple generar y distribuir información falsa que pueda afectar a la opinión pública de un país que

pudiera estar pasando por un momento político delicado, ilustrando así la necesidad de seguir investigando mecanismos que mantengan el equilibrio occidental entre libertad y seguridad.

CONCLUSIONES

El mundo moderno -hiperconectado y digital- presenta una serie de cambios de paradigma para variadas nociones humanas, incluyendo la soberanía. Analizando el ejemplo de tres potencias mundiales podemos observar que contrastan estrategias diferentes ante un desafío común: resguardar los intereses nacionales en el ciberespacio.

La discordancia entre estas estrategias es reflejo de la visión política y cultural que dichos Estados poseen respecto de su propia soberanía nacional y del peso que les asignan a las libertades personales, en una balanza que no siempre está equilibrada.

En esta compleja apuesta, se integran no solo los límites legales y diplomáticos propios de un mundo globalizado, sino que también entra en juego el mundo privado y comercial, manifestado en la influencia (accidental o planificada) que grandes compañías tecnológicas tienen sobre el quehacer civil local e internacional y, por lo tanto, convirtiéndose en actores relevantes para los intereses soberanos de sus países de origen.

Queda por ver el nivel de efectividad que cada apuesta estratégica arroja en el mediano y largo plazo, por lo cierto es que este no es sino uno de varios desafíos cambiantes que copará la agenda global en los próximos años, posiblemente transformando nuestro entendimiento de las fronteras y de la soberanía tanto física como digital.

BIBLIOGRAFÍA

BARLOW, J. P. (1996). Cyberspace Independence Declaration. http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296. Declaration.

BODIN, J. (1992). On sovereignty: Four chapters from the six books of the commonwealth. Cambridge University Press.

GOEL, S. (2020). National cyber security strategy and the emergence of strong digital borders. Connections, 19(1), 73-86.

GROTIUS, H. (2012). Hugo Grotius on the law of war and peace. Cambridge University Press.

HOBBES, T. (2022). Leviathan.

KANT, I. Perpetual Peace: A Philosophical Sketch.

KRASNER, S. D. (1999). Sovereignty: Organized hypocrisy. Princeton University Press.

KUMAR, V. (2024, March 15). Explain the provisions of state: Condition of statehood, territory and underlying principles, sovereignty under international law - legal vidhiya. Legal Vidhiya. https://legalvidhiya.com/explain-the-provisions-of-state-condition-of-statehood-territory-and-underlying-prin-

ciples-sovereignty-under-international-law/

LOCKE, J. (1967). Two treatises of government. Cambridge University Press.

OSIANDER, A. (2001). Sovereignty, international relations, and the Westphalian myth. International organization, 55(2), 251-287.

PHILPOTT, D. (1995). Sovereignty: An introduction and brief history. Journal of International Affairs, 353-368.

SAAIDA, Mohammed. (2024). Digital Sovereignty. 6. 1-12.

SHERMAN, J. (2022). Reassessing RuNet: Russian internet isolation and implications for Russian cyber behavior. JSTOR Security Studies Collection.

WILSON, W. (1918). The Fourteen Points Address. The Record of American Diplomacy: Documents and Readings in the History of American Foreign Relations, 3rd ed. (New York: Alfred A. Knopf, 1954), 459-461.


CENTRO DE INVESTIGACIÓN Y ESTUDIOS ESTRATÉGICOS
ANEPE.CL