Licenciatura en Relaciones Internacionales

Tesina de Grado

Disputa global por el poder digital entre los Estados y las grandes empresas tecnológicas a partir de la pandemia COVID-19 (2020-2025)

Tesista

Julieta María Oldani

Directora

Paula Demarchi

20 de julio de 2026

Rosario, Santa Fe, Argentina

julioldani53@gmail.com

Agradecimientos

A mi mamá y a mi papá, por su inmenso amor y por hacer posible que hoy esté acá. Este logro también es suyo.

A mi hermana, Luli, por ser siempre mi lugar seguro.

A mis amigas, por caminar a mi lado durante todos estos años.

A mi novio, Mariano, por su paciencia y por confiar en mí incluso cuando yo dudaba.

A mi gatita Alaska, mi compañera incondicional.

A los profesores de la Facultad de Ciencia Política y Relaciones Internacionales, por sus enseñanzas y por transmitirme la importancia de la perseverancia, la responsabilidad y el compromiso. A Paula Demarchi, mi tutora, por su guía, sus consejos y su acompañamiento constante durante todo el proceso de investigación.

A la universidad pública, gratuita y de calidad, por brindarme la oportunidad de formarme profesional y personalmente.

¡Muchas gracias!

Resumen

La presente tesina analiza la reconfiguración de la disputa por el poder digital en las Relaciones Internacionales a partir de la pandemia de COVID-19, durante el período 2020-2025. Se parte de la premisa de que la aceleración de la digitalización profundizó la dependencia de los Estados y las sociedades respecto de las plataformas digitales, fortaleciendo la capacidad de las grandes empresas tecnológicas para incidir en procesos políticos, económicos, sociales y comunicacionales. La investigación examina la transformación del concepto de poder en el escenario digital, la centralidad estratégica del ciberespacio, la emergencia de la ciberseguridad en la agenda estatal y los principales marcos regulatorios adoptados por Estados Unidos, la Unión Europea, China y Brasil. Asimismo, se abordan los casos de Estados Unidos frente a TikTok y Brasil frente a X como expresiones concretas de la disputa por la autoridad digital. El estudio sostiene que, aunque ambos conflictos responden a contextos, fundamentos y herramientas distintas, revelan una misma tendencia: los Estados buscan reafirmar su soberanía y su capacidad de decisión frente a actores digitales transnacionales que controlan datos, algoritmos, infraestructuras y espacios centrales de circulación de información. La tesina concluye que la soberanía digital constituye una dimensión clave de la política internacional contemporánea, atravesada por tensiones entre seguridad, libertad de expresión, regulación, derechos y gobernanza global.

Palabras clave: poder digital – soberanía digital – plataformas digitales – ciberseguridad – Estados Unidos – China – TikTok – Brasil – X.

Índice

Introducción 5
Capítulo 1: La transformación del poder en el escenario digital internacional 13
1.1. La evolución del concepto de poder en las Relaciones Internacionales 13
1.2. El ciberespacio como nuevo escenario de poder 16
1.3. De empresas tecnológicas a actores globales 20
1.4. Cuando el poder se desplaza: Estados, empresas tecnológicas y autoridad en disputa 23
Capítulo 2: Después de la pandemia: dependencia digital, ciberseguridad y nuevas reglas para el ciberespacio 29
2.1. El COVID-19 como catalizador de la dependencia digital a nivel mundial 29
2.2. La ciberseguridad en el centro de la agenda estatal 33
2.3. Las nuevas reglas del entorno digital: respuestas estatales y regionales 34
2.3.1. EE. UU. 35
2.3.2. Unión Europea 39
2.3.3. China 44
2.3.4. Brasil 48
2.4. Gobernar un espacio sin fronteras: cooperación, fragmentación y límites de la gobernanza global 51
Capítulo 3: La soberanía digital puesta a prueba: los casos de TikTok en EE. UU. y X en Brasil 57
3.1. EE. UU. vs. TikTok: la disputa por una plataforma estratégica 58
3.1.1. Del crecimiento de TikTok a la presión por la desinversión 58
3.1.2. Lo que revela el caso TikTok 65
3.2. Brasil vs. X: el límite entre libertad de expresión y autoridad estatal 67
3.2.1. De la desinformación electoral al bloqueo de la plataforma 67
3.2.2. Lo que revela el caso X 73
3.3. Cierre comparativo: dos casos, una misma disputa por la autoridad digital 75
Conclusión 77
Referencias bibliográficas 81
Anexo I: Lista de abreviaciones y siglas 90
Anexo II: Principales tecnologías digitales asociadas a la Cuarta Revolución Industrial 91

Introducción

A lo largo de la historia, las disputas por el poder han definido el curso de las Relaciones Internacionales. Desde la dimensión militar hasta la económica, los Estados han competido constantemente por establecer, preservar o ampliar su influencia dentro del sistema internacional. Sin embargo, en el siglo XXI ha emergido una nueva dimensión estratégica: el poder digital. Este poder, basado en el control de las tecnologías de la información (TIC), los datos, las plataformas digitales y las infraestructuras de conectividad, se ha convertido en un componente central de la política internacional contemporánea. En un escenario cada vez más atravesado por la digitalización, la capacidad de un Estado para influir, regular o restringir el acceso y uso de estos recursos digitales incide de manera creciente en su posicionamiento internacional, en su seguridad y en el ejercicio efectivo de su soberanía.

En este contexto, las grandes empresas tecnológicas, también conocidas como *Big Tech*, han adquirido una relevancia inédita. Compañías como Google, Amazon, Meta, ByteDance o X Corp. han dejado de ser simples proveedoras de herramientas tecnológicas para convertirse en actores internacionales con una significativa capacidad de influencia frente a los actores tradicionales del sistema internacional. Las plataformas digitales controladas por estas empresas no solo intermedian la comunicación y el acceso a la información, sino que también acumulan cantidades masivas de datos, organizan flujos de interacción social y poseen el potencial de incidir sobre procesos políticos, económicos y sociales dentro de los Estados. De este modo, su poder no se limita al plano tecnológico o comercial, sino que adquiere implicancias directas para la soberanía digital, la ciberseguridad, la protección de datos y la disputa por las narrativas políticas.

Estas tensiones se hicieron más evidentes a partir de la pandemia de COVID-19. Durante los años 2020 y 2021, las tecnologías digitales se volvieron esenciales para

garantizar la continuidad de la vida social, económica, educativa, laboral y política. La expansión del trabajo remoto, la educación virtual, el comercio electrónico, la comunicación digital y el consumo de información en línea profundizó la dependencia de los Estados y de las sociedades respecto de las plataformas digitales. Al mismo tiempo, los gobiernos comenzaron a prestar mayor atención a fenómenos como la desinformación, la manipulación algorítmica, la influencia extranjera en procesos políticos internos y la pérdida de control sobre los datos de sus ciudadanos. Esta nueva sensibilidad estatal frente al espacio digital dio lugar a respuestas más enérgicas y sistemáticas, expresadas en regulaciones, restricciones, litigios judiciales, sanciones económicas y, en algunos casos, prohibición o suspensión del funcionamiento de determinadas aplicaciones dentro de territorios nacionales.

En este marco, durante el período analizado se destacan dos conflictos especialmente relevantes: el caso de Estados Unidos (EE. UU.) frente a TikTok y el enfrentamiento entre Brasil y X. El primero se inscribe en el contexto de la rivalidad tecnológica y geopolítica entre EE. UU. y China, y pone de relieve las tensiones en torno al control de los datos personales, la ciberseguridad y la posible injerencia extranjera. Desde la administración de Donald Trump, el gobierno estadounidense ha sostenido que TikTok, al ser propiedad de la empresa china ByteDance, podía representar una amenaza para la seguridad nacional. Este caso permite observar cómo una plataforma digital puede ser interpretada por un Estado como un recurso estratégico vinculado a una potencia rival.

El segundo caso refleja una dinámica distinta, aunque igualmente reveladora. En Brasil, las tensiones entre el Estado y X se vincularon principalmente con la moderación de contenidos, la difusión de desinformación, los discursos de odio y los ataques a las instituciones democráticas, especialmente en el contexto posterior a las elecciones presidenciales y al intento de golpe de Estado del 8 de enero de 2023. Este conflicto expresa con mayor claridad la disputa entre la autoridad judicial de un Estado democrático y una

compañía transnacional que desafía el cumplimiento de decisiones jurisdiccionales nacionales.

A la luz de lo expuesto, la presente tesina se propone abordar el siguiente problema de investigación: ¿cómo se ha reconfigurado la disputa por el poder en el ámbito digital entre los Estados y las grandes empresas tecnológicas a partir de la pandemia de COVID-19, durante el período 2020-2025? ¿Qué estrategias han adoptado los Estados para reafirmar su soberanía en este contexto?

A fin de responder estos interrogantes, el objetivo general de este trabajo consiste en analizar cómo se ha reconfigurado el poder digital en las Relaciones Internacionales a partir de la pandemia de COVID-19, examinando las medidas adoptadas por los Estados frente a la influencia de las grandes empresas tecnológicas y sus implicancias para la soberanía estatal y la gobernanza del espacio digital. Para ello, el trabajo se orienta en función de tres objetivos específicos: en primer lugar, analizar la transformación del concepto de poder en las Relaciones Internacionales en el contexto de la digitalización; en segundo lugar, examinar cómo la pandemia profundizó la centralidad de las grandes empresas tecnológicas; y en tercer lugar, analizar las estrategias adoptadas por EE. UU. frente a TikTok y por Brasil frente a X como casos ilustrativos de la disputa global por el poder digital y de los intentos estatales por reafirmar su autoridad en el espacio digital.

La relevancia de esta investigación para la disciplina de las Relaciones Internacionales radica en que aborda una dimensión emergente y aún en proceso de conceptualización: el poder digital. Tradicionalmente, el análisis del poder internacional se ha concentrado en sus expresiones militares, económicas, diplomáticas o territoriales. No obstante, la creciente importancia de las tecnologías digitales en la vida social y política obliga a repensar cómo se ejerce, se disputa y se regula el poder en el siglo XXI. El entorno digital no constituye un espacio neutral ni meramente técnico, sino un ámbito atravesado por

intereses estratégicos, rivalidades geopolíticas, disputas normativas y tensiones entre actores estatales y no estatales. Sobre esta base, el presente análisis contribuye a enriquecer el debate académico al examinar cómo los Estados interactúan, negocian y confrontan con actores privados que operan transnacionalmente y que poseen una capacidad de influencia difícil de encuadrar dentro de las categorías tradicionales de las Relaciones Internacionales. En virtud de un análisis preliminar del tema elegido, se presenta a continuación un breve estado del arte y un marco conceptual, que serán desarrollados con mayor detalle a lo largo del primer y segundo capítulo del trabajo.

En cuanto al estado del arte, tal como se mencionó anteriormente, el estudio del poder ha ocupado un lugar central en la disciplina de las Relaciones Internacionales, aunque su significado ha sido históricamente objeto de debate y reformulación. En este recorrido, los aportes de Morgenthau (1948) y Waltz (1979) se inscriben dentro de las perspectivas realistas y neorrealistas, centradas en la seguridad, la supervivencia y la distribución de capacidades en un sistema internacional anárquico. A su vez, Keohane (1984), Strange (1988) y Wendt (1999) ampliaron el debate al incorporar dimensiones vinculadas con la cooperación, las instituciones, las normas, las ideas, la legitimidad y las estructuras que condicionan la interacción entre los actores internacionales.

En los últimos años, la literatura especializada comenzó a prestar mayor atención a los efectos de la digitalización sobre estas formas tradicionales de poder. En esta línea, Nye (2011) y Noël (2019) contribuyen a situar el poder digital como una dimensión relevante de la política internacional contemporánea, mientras que Mayer-Schönberger y Cukier (2013) destacan la centralidad de los datos como recurso económico y estratégico. Estos enfoques son complementados por los aportes de Malacalza (2025), quien incorpora la dimensión algorítmica como parte de las nuevas formas de poder asociadas a la transformación digital.

Otro eje relevante del debate académico se vincula con la emergencia de las grandes empresas tecnológicas como actores internacionales que, a través de sus plataformas digitales, presentan una significativa capacidad de intermediación, regulación e incidencia transnacional. El rol de dichas plataformas en el escenario internacional es abordado en los trabajos de Srnicek (2017), Van Dijck et al. (2018), Gillespie (2018) y Törnberg (2024). Asimismo, los aportes de Bremmer (2021), Mukherjee (2025) y Malacalza (2025) permiten situar estas transformaciones dentro de un escenario más amplio de competencia tecnológica, tecnopolaridad y disputa geopolítica por el control de recursos digitales estratégicos.

Finalmente, estos trabajos se complementan con los estudios sobre ciberseguridad, regulación y gobernanza global del ciberespacio llevados a cabo por Kello (2013), Johanson y Chong (2024) y Henen (2025). Asimismo, Mukherjee (2025) contribuye al análisis de los marcos regulatorios como respuestas estatales frente a la competencia digital, mientras que Chang y Grabosky (2026), Raymond y DeNardis (2015), DeNardis (2014) y Nye (2014) permiten comprender la gobernanza del ciberespacio como un campo transnacional, fragmentado y atravesado por la participación de múltiples actores.

Por su parte, el marco conceptual de esta tesina se apoya sobre una noción amplia del poder en las Relaciones Internacionales. En primer lugar, se recuperan los aportes de Nye (2011), quien desarrolla el concepto de poder digital o ciberpoder, posteriormente profundizado por Noël (2019), el cual es entendido como la capacidad de obtener resultados mediante el uso estratégico de los recursos de información interconectados electrónicamente del ciberespacio. A su vez, Malacalza (2025) introduce la noción de poder algorítmico para comprender la capacidad de los sistemas automatizados de moldear percepciones, decisiones y comportamientos, con implicancias cognitivas, geoeconómicas y geopolíticas. Estos conceptos se vinculan íntimamente con la noción de soberanía digital, entendida por Shoker (2022) como el dominio absoluto por parte del Estado sobre todos sus activos digitales,

incluyendo toda la cadena de valor: datos, infraestructura, operaciones, cadena de suministro y conocimiento.

En segundo lugar, el análisis incorpora la dimensión geopolítica de la transformación digital. Siguiendo a Mukherjee (2025), la competencia tecnológica puede entenderse como la disputa entre actores estatales y privados por el control de tecnologías estratégicas, datos, sistemas digitales, algoritmos y capacidades de innovación. Esta lectura se complementa con la noción de tecnopolaridad desarrollada por Bremmer (2021), que permite comprender un escenario en el cual las grandes empresas tecnológicas no actúan únicamente como instrumentos de los Estados, sino también como actores con capacidad propia para ejercer influencia geopolítica, definir reglas de interacción y condicionar el funcionamiento del espacio digital. En este marco, los aportes de Strange (1988) sobre la difusión de la autoridad estatal resultan centrales para analizar cómo ciertas funciones históricamente asociadas al Estado se desplazan o fragmentan hacia otros niveles y actores, entre ellos, las empresas tecnológicas que operan plataformas digitales. En este sentido, Srnicek (2017), Van Dijck et al. (2018), Gillespie (2018) y Törnberg (2024) definen a las plataformas digitales como infraestructuras privadas de intermediación, regulación y control de datos.

Por último, se retoman los conceptos de ciberseguridad y gobernanza global del ciberespacio. Siguiendo a Kello (2013), la ciberseguridad es entendida no solo como el conjunto de medidas destinadas a proteger sistemas informáticos y datos frente a acciones hostiles, sino también como una dimensión vinculada al control gubernamental de los flujos de información en la sociedad. Por su parte, la gobernanza global del ciberespacio es abordada a partir de los aportes de Raymond y DeNardis (2015), quienes destacan su carácter multiactor, y de Nye (2014), quien la concibe como un complejo de regímenes compuesto por normas e instituciones parcialmente articuladas.

Con el propósito de brindar una respuesta tentativa a las preguntas de investigación, la hipótesis que guía este trabajo sostiene que la pandemia de COVID-19 intensificó la disputa global por el poder digital, configurando un escenario en el que los Estados comenzaron a percibir nuevos desafíos a su seguridad, soberanía y gobernanza estatal frente a la creciente influencia de las grandes empresas tecnológicas. Este contexto, sumado a la competencia tecnológica entre las principales potencias, ha impulsado a los Estados a adoptar diversas estrategias regulatorias, judiciales y discursivas destinadas a reafirmar su autoridad y recuperar márgenes de control sobre el espacio digital.

Desde el punto de vista metodológico, el trabajo adopta un diseño descriptivo y analítico, con un enfoque cualitativo. Asimismo, el recorte temporal se delimita entre 2020 y 2025. El año 2020 constituye un punto de inflexión debido a la pandemia de COVID-19, que profundizó la centralidad del ciberespacio en la vida política, social y económica, al tiempo que visibilizó las asimetrías de poder entre Estados y las corporaciones tecnológicas. El cierre en 2025 permite trabajar con un período delimitado y observar la evolución de conflictos que se desarrollaron a lo largo de esos años.

En cuanto al recorte espacial y empírico, la investigación recurre a los conflictos entre EE. UU. y TikTok, por un lado, y Brasil y X, por el otro, como casos ilustrativos para complementar el análisis desarrollado. La selección de estos casos se justifica por la repercusión pública que ambos han adquirido, así como también por su actualidad y su capacidad para evidenciar diferentes formas de respuesta estatal frente al desafío que les presentan las plataformas digitales.

Para la recolección de datos se recurre tanto a fuentes primarias —fallos judiciales, documentos oficiales, leyes, comunicados gubernamentales, declaraciones públicas y publicaciones oficiales en redes sociales—, así como a fuentes secundarias —libros, artículos académicos, informes especializados y notas periodísticas—. En cuanto al análisis de la

información, se emplea el análisis documental y de contenido, con el objetivo de examinar las fuentes seleccionadas e interpretar los diferentes enfoques estatales.

La tesina se estructura en tres capítulos, organizados en función de los objetivos específicos de la investigación. El capítulo 1 desarrolla la transformación del poder en el escenario internacional, con especial énfasis en la noción de poder digital y su vinculación con la soberanía estatal y la gobernanza digital. El capítulo 2 aborda la profundización de la dependencia digital a partir de la pandemia de COVID-19, el fortalecimiento de la capacidad de influencia de las empresas tecnológicas transnacionales y la emergencia de la ciberseguridad como eje prioritario en la agenda estatal. El capítulo 3 analiza los conflictos EE. UU. vs. TikTok, y Brasil vs. X, e incorpora una breve comparación entre ambos casos. Por último, se presentan las conclusiones, en las que se sintetizan los principales hallazgos en relación con la problemática abordada.

Capítulo 1: La transformación del poder en el escenario digital internacional

El concepto de poder ha ocupado un lugar central en el campo de las Relaciones Internacionales, aunque su significado ha sido históricamente objeto de debate y reformulación. Desde las concepciones tradicionales centradas en las capacidades materiales y la coerción, hasta enfoques que incorporan dimensiones normativas, simbólicas y estructurales, el poder ha sido redefinido en función de las transformaciones del sistema internacional. Por esta razón, las distintas corrientes teóricas han contribuido a ampliar su alcance analítico, permitiendo comprenderlo no solo como la capacidad de imponer la voluntad propia, sino también como la habilidad de influir, estructurar contextos y moldear percepciones.

En este marco, en el presente capítulo se analiza cómo la expansión de las tecnologías digitales ha profundizado esta evolución, dando lugar a nuevas formas de ejercicio del poder asociadas al control de la información y los datos. La configuración del ciberespacio como un dominio de interacción global, junto con la emergencia de plataformas digitales capaces de mediar, organizar y regular múltiples esferas de la vida social, ha reconfigurado las dinámicas tradicionales entre actores estatales y no estatales. En este contexto, el poder digital se consolida como un recurso estratégico clave, al tiempo que contribuye a difuminar las fronteras entre lo público y lo privado, y a tensionar la centralidad del Estado en la gobernanza mundial.

1.1. La evolución del concepto de poder en las Relaciones Internacionales

El concepto de poder ha ocupado un lugar central en el campo de las Relaciones Internacionales. Sin embargo, hoy en día, este concepto carece de una definición universalmente aceptada y continúa siendo objeto de debate dentro de la disciplina. Las distintas corrientes teóricas han desarrollado interpretaciones diversas sobre la naturaleza del

sistema internacional y el comportamiento de sus actores. En el marco del realismo, el poder se concibe principalmente en términos de capacidades materiales, particularmente el poder militar. Autores como Hans Morgenthau (1948) sostienen que la política internacional es una lucha por el poder, entendido como la capacidad de controlar las acciones de otros Estados. En esta misma línea, el neorrealismo estructural de Kenneth Waltz (1979) enfatiza la distribución de capacidades en el sistema internacional como factor determinante del comportamiento estatal. Desde esta perspectiva, el poder se vincula estrechamente con la supervivencia y la seguridad en un entorno anárquico.

En contraste, las perspectivas liberales amplían la noción de poder al incorporar dimensiones no coercitivas y al reconocer la importancia de la cooperación internacional. En esta dirección, Robert Keohane (1984) destaca el rol de las instituciones en la facilitación de la cooperación entre Estados, incluso en ausencia de una autoridad central. Asimismo, los aportes de Joseph Nye (2011) resultan especialmente relevantes para el presente trabajo, en tanto define al poder como "la capacidad de actuar, y en situaciones sociales, influir en los demás para conseguir los resultados deseados" (Nye, 2011, p. 4).

A su vez, Nye distingue entre diferentes formas de ejercicio del poder. Por un lado, el poder duro refiere a la capacidad de influir en el comportamiento de otros actores mediante mecanismos coercitivos, tales como el uso de la fuerza, las sanciones económicas o la imposición de agendas. Por otro lado, el poder blando se vincula con la capacidad de obtener resultados a través de la atracción, la persuasión y la cooptación, apoyándose en recursos intangibles como la cultura, los valores, las instituciones y la legitimidad percibida. Bajo esta lógica, mientras el poder duro se asocia principalmente a recursos materiales, el poder blando depende en gran medida de la percepción de los actores destinatarios, lo que otorga un rol central a las ideas y a los procesos de construcción de legitimidad.

Adicionalmente, Nye introduce el concepto de poder inteligente, entendido como “la capacidad de combinar recursos de poder duro y blando en estrategias efectivas” (Nye, 2011, p. 16). Desde esta perspectiva, no basta con disponer de amplios recursos de poder, sino que resulta fundamental la habilidad para articularlos de forma coherente en función del contexto. De este modo, el poder inteligente implica no solo el reconocimiento de la diversidad de recursos disponibles, sino también la capacidad de adaptarlos a escenarios cambiantes y complejos, como los que caracterizan a la política internacional contemporánea.

Por su parte, el constructivismo propone una concepción del poder como fenómeno socialmente construido, en el cual las ideas, normas e identidades desempeñan un papel fundamental. En este marco, Alexander Wendt (1999) sostiene que las estructuras internacionales no son únicamente materiales, sino también intersubjetivas, lo que implica que el significado del poder depende de los contextos sociales en los que se inscribe. Desde este enfoque, el poder incluye la capacidad de definir y moldear normas, valores y percepciones, influyendo así en el comportamiento de los actores internacionales.

Asimismo, los aportes de Susan Strange (1988) desde la Economía Política Internacional introducen una dimensión estructural del poder. La autora distingue entre poder relacional y poder estructural, destacando que este último:

> Implica la facultad de establecer la agenda de debate o de diseñar (...) los regímenes internacionales de normas y costumbres que supuestamente rigen las relaciones económicas internacionales. (...) Confiere la facultad de decidir cómo deben hacerse las cosas, la facultad de configurar los marcos dentro de los cuales los Estados se relacionan entre sí, con las personas o con las empresas. (Strange, 1988, p. 25).

Este poder estructural puede encontrarse en cuatro estructuras, distintas pero relacionadas entre sí: seguridad, producción, finanzas y conocimiento. Este enfoque resulta

esencial para analizar los contextos contemporáneos en los que actores no estatales adquieren un rol significativo en la configuración de reglas, normas y mercados a nivel internacional.

1.2. El ciberespacio como nuevo escenario de poder

A la luz de estas conceptualizaciones, resulta necesario ubicar el análisis del poder en el marco de las transformaciones estructurales impulsadas por la Cuarta Revolución Industrial. Este fenómeno no se limita al avance de tecnologías digitales, sino que constituye un nuevo paradigma que reconfigura las relaciones políticas, económicas, sociales y ambientales en todo el mundo. Se caracteriza por la aceleración del cambio tecnológico y la expansión de la economía digital, impulsadas por la interconectividad, el capitalismo de plataformas y la creciente velocidad en la circulación de datos. En este marco emergen y se articulan desarrollos tecnológicos avanzados como la computación en la nube, las redes 5G, la inteligencia artificial (IA), el análisis de macrodatos, la internet de las cosas (IoT, por sus siglas en inglés), la robótica, entre otros. Si bien este proceso es liderado por economías tradicionales como EE. UU. y Alemania, también encuentra un fuerte dinamismo en países asiáticos, principalmente China, donde se concentran crecientes inversiones en sectores tecnológicos estratégicos (Malacalza, 2021).

Más que la aparición de tecnologías completamente nuevas, lo distintivo de esta revolución radica en la escala, la velocidad y la convergencia de innovaciones preexistentes. Ejemplo de ello es el IoT, cuyo desarrollo se remonta a décadas atrás, pero que hoy adquiere relevancia por la masificación de dispositivos conectados y la aceleración de las redes. En conjunto, estas transformaciones han dado lugar a un acelerado proceso de digitalización que ha reconfigurado de manera profunda las lógicas de producción, comunicación e interacción social (Malacalza, 2021). En este contexto, el desarrollo del ciberespacio introduce una dimensión novedosa en el análisis del poder. Aunque el uso de la información como recurso

no es nuevo, la emergencia del ciberespacio como dominio operativo representa una transformación cualitativa en las condiciones de su producción, circulación y control, alterando las formas en que el poder se estructura y se proyecta en la política internacional. En este sentido, el ciberespacio es un régimen híbrido creado por el ser humano que combina propiedades físicas y virtuales. Siguiendo a Jean-Christophe Noël (2019), está compuesto por tres capas:

> La primera es tangible (*hardware*) e incluye toda la infraestructura física necesaria para transmitir datos de un punto de la red a otro. En concreto, incluye cables submarinos, servidores, ordenadores y objetos conectados. La segunda capa es intangible y corresponde a las aplicaciones necesarias para procesar la información (*software*). Está compuesta por software y sistemas operativos. La última capa se denomina capa cognitiva. Se refiere al contenido de la información almacenada e intercambiada en la red. (Noël, 2019, p. 17).

De esta manera, si bien el ciberespacio parece no tener fronteras, en realidad "está delimitado por las infraestructuras físicas que facilitan la transferencia de datos e información. Dichas infraestructuras son mayoritariamente propiedad del sector privado y se ubican en el territorio soberano de los Estados" (Makovetka et al., 2024, p. 8).

El dominio cibernético es único porque es artificial, novedoso y está sujeto a cambios tecnológicos aún más rápidos que otros dominios (Nye, 2010). En otras palabras, es un entorno dinámico que evoluciona y cambia constantemente.

> El ciberespacio alberga procesos fundamentales para la sociedad, la economía y la gobernanza modernas, como el comercio electrónico, la comunicación digital, las redes sociales y el acceso a la información y los servicios. También se ha convertido en escenario de nuevas formas de delincuencia, como los ciberataques, el

> ciberespionaje, la ciberguerra y otras ciberamenazas, que plantean nuevos desafíos legales y de seguridad para la sociedad. (Makovetka et al., 2024, p. 7).

En este sentido, resulta relevante mencionar el proceso de "datificación", entendido como aquel mediante el cual distintos aspectos de la realidad, incluso aquellos que tradicionalmente no se concebían como información, como la ubicación de una persona o su comportamiento en línea, son transformados en datos cuantificables. En la era digital, este fenómeno ha redefinido el valor de los datos: ya no funcionan únicamente como soporte de transacciones, sino que, en muchos casos, se convierten en el objeto central de intercambio (Mayer-Schönberger y Cukier, 2013).

A diferencia de los bienes materiales, los datos poseen características particulares que potencian su valor económico y estratégico. Son un bien no rival, es decir, pueden ser utilizados por múltiples actores sin agotarse, y su valor no disminuye con el uso, sino que, por el contrario, reside en su capacidad de ser reutilizados de manera prácticamente ilimitada. Por ello, su verdadero potencial no radica solo en su acumulación, sino en su procesamiento y explotación (Mayer-Schönberger y Cukier, 2013).

En el ecosistema digital, las plataformas desempeñan un papel central en este proceso. A través de la interacción cotidiana de los usuarios (como clics, búsquedas o movimientos en línea) se generan y recopilan grandes volúmenes de datos que incluyen desde información técnica hasta detalles sobre intereses, preferencias y comportamientos (Van Dijck et al., 2018). Estos datos no solo se almacenan y analizan, sino que también circulan constantemente entre plataformas mediante interfaces de programación (API, por sus siglas en inglés), lo que permite su uso por terceros para desarrollar nuevos servicios y aplicaciones.

En este marco, el desarrollo de estas aplicaciones no solo configura un nuevo ámbito en el que se despliegan y disputan recursos de poder, sino que también transforma las condiciones tradicionales de su ejercicio. En términos generales, podemos entender al

ciberpoder como “la capacidad de obtener resultados deseados mediante el uso de los recursos de información interconectados electrónicamente del ciberespacio” (Nye, 2010, p. 3). Puede utilizarse para generar resultados deseados dentro del ciberespacio, como también en otros dominios fuera de él. En el marco de la política internacional, podemos referirnos al ciberpoder como “la capacidad de cualquier actor para explotar los datos digitales con el fin de ayudar a cambiar el comportamiento de otros actores en el escenario internacional y lograr sus propios fines” (Noël, 2019, p. 13).

El poder digital constituye un recurso estratégico de gran valor para quienes logran aprovecharlo. No solo puede emplearse en actividades convencionales como el espionaje, el sabotaje o la subversión, sino que además desempeña un papel relevante en el ámbito militar, al incidir en los niveles táctico, operacional y estratégico de las operaciones (Noël, 2019). En este sentido, lo que distingue al mundo virtual es que los actores son diversos, el costo de entrada es bajo debido al anonimato, la distancia física es irrelevante y llevar a cabo un ataque virtual es posible con tan solo un clic. Asimismo, la velocidad del internet implica que todos los gobiernos tienen menos control sobre sus agendas, al tiempo que la política se vuelve más volátil y menos confinada a los límites nacionales (Nye, 2010).

Como una derivación del poder digital, Bernabé Malacalza (2025) propone el concepto de megapoder algorítmico, de particular relevancia para el presente análisis. Este tipo de poder configura el orden mundial al moldear percepciones, decisiones y comportamientos. Los algoritmos avanzados de IA operan como un “cerebro sintético”, a saber, procesan datos para generar resultados y brindan las instrucciones que permiten a los sistemas aprender, razonar y tomar decisiones. El poder algorítmico no reside solo en el control de datos o la eficiencia de los modelos, sino en su capacidad para reconfigurar jerarquías globales: desde la supremacía tecnológica hasta la militarización de la inteligencia. No obstante, también implican riesgos significativos. Desde la vigilancia masiva hasta la

manipulación informativa, los algoritmos pueden ser utilizados como herramientas de presión geopolítica, afectando incluso la integridad de los procesos democráticos. Así, su uso (o abuso) redefine las fronteras entre lo civil y lo militar, entre la libertad y el control, entre la democracia y su simulacro.

Concebido como una forma de influencia, el poder algorítmico se define como la capacidad de los Estados y de las grandes corporaciones tecnológicas para incidir sobre sociedades y mercados mediante el control de sistemas automatizados. Este poder se despliega en tres dimensiones interrelacionadas: la cognitiva, al modelar percepciones; la geoeconómica, al concentrar riqueza; y la geopolítica, al generar dependencias tecnológicas. Su carácter de "megapoder" radica en que el control de los algoritmos permite incidir tanto en la vida cotidiana (como el consumo digital), como en ámbitos estratégicos, incluyendo el funcionamiento de infraestructuras críticas, la seguridad nacional y los flujos financieros. En este escenario, la competencia entre potencias como EE. UU. y China por el dominio algorítmico refleja su potencial como recurso estratégico clave en la disputa por la hegemonía internacional (Malacalza, 2025).

1.3. De empresas tecnológicas a actores globales

En las últimas décadas, las plataformas digitales emergieron como un nuevo modelo de negocio caracterizado por su capacidad para extraer, procesar y controlar grandes volúmenes de datos. A diferencia de los modelos tradicionales, no crean un mercado desde cero, sino que ofrecen el ecosistema necesario para mediar entre distintos grupos de usuarios. Esta función de intermediación constituye la base de su ventaja competitiva: al facilitar la interacción entre dos o más partes, las plataformas se consolidan como espacios digitales que articulan y organizan dichas relaciones (Srnicek, 2017).

Las plataformas no solo representan una innovación organizativa, sino también una respuesta del capitalismo a los desafíos de la digitalización. Como plantea Törnberg (2024), se trata de estructuras digitales que organizan las interacciones entre usuarios dentro de entornos que ellas mismas controlan. De este modo, su estrategia comercial| no se limita a facilitar intercambios, sino que consiste en apropiarse del mercado en el que operan, regulando su funcionamiento y obteniendo beneficios a partir de ese control. En este marco, los proveedores de servicios digitales emergen como una nueva forma de "Estados empresariales": empresas con capacidad de controlar no solo el comercio, sino también las normas, el espacio y los márgenes de acción de otros actores; en otras palabras, de regular la vida social.

Existe una creencia generalizada de que los servicios que ofrecen este tipo de aplicaciones son gratuitos, simplemente porque no implican un pago directo por parte del usuario. Sin embargo, esta idea resulta engañosa. Como señalan Van Dijck et al. (2018), las plataformas pueden adoptar diversos modelos de negocio para generar valor, incluyendo la venta de publicidad, la implementación de suscripciones o tarifas, así como la comercialización de datos a otras empresas e incluso a gobiernos interesados en su uso para la elaboración de perfiles. Esta lógica se vuelve especialmente visible al analizar la estructura del ecosistema de plataformas, en el que es posible distinguir entre plataformas de infraestructura y plataformas sectoriales.

Las plataformas de infraestructura, en su mayoría controladas por las llamadas "*Big Five*" (Alphabet, Meta, Microsoft, Amazon y Apple), constituyen el núcleo del sistema, en tanto funcionan como la base sobre la cual se desarrollan otras plataformas. Estas operan como verdaderos intermediarios o "guardianes" de los flujos de datos, ya que gestionan su almacenamiento, procesamiento y circulación. Entre sus servicios se incluyen motores de

búsqueda, computación en la nube, redes sociales, sistemas de pago, tiendas de aplicaciones, servicios de mensajería, publicidad digital y análisis de datos, entre otros.

Aunque en teoría este ecosistema permite la entrada de nuevos actores, en la práctica la fuerte expansión de las plataformas de infraestructura ha reducido significativamente la competencia, consolidando un núcleo altamente concentrado. Estas grandes empresas se benefician de la integración de millones de sitios web y aplicaciones con sus servicios, lo que les permite recolectar datos a gran escala y reforzar su posición dominante. Además, han extendido su presencia hacia múltiples sectores mediante adquisiciones, alianzas estratégicas y el desarrollo de nuevas plataformas, e incluso han comenzado a incursionar en actividades tradicionales. Debido a su centralidad, algunos autores consideran este tipo de plataformas como "superplataformas" o infraestructuras casi públicas, indispensables para el funcionamiento de la economía digital.

Por su parte, las plataformas sectoriales operan en ámbitos específicos como el comercio, el transporte o la salud, y ofrecen servicios digitales orientados a esas áreas. Muchas de ellas funcionan principalmente como intermediarias que conectan a usuarios con proveedores, facilitando intercambios dentro de un sector determinado. Dentro de este grupo podemos encontrar a Uber, Airbnb, Booking, entre otras.

Ahora bien, aunque no es la primera vez que corporaciones privadas desempeñan un papel importante en la política internacional, los gigantes del pasado jamás podrían igualar la omnipresente presencia global de las empresas tecnológicas actuales. Como se mencionó anteriormente y siguiendo el análisis Bremmer (2021), estas cuentan con dos ventajas cruciales que les han permitido forjar una influencia geopolítica independiente. En primer lugar, no operan ni ejercen su poder exclusivamente en el espacio físico, sino que han creado una nueva dimensión geopolítica (el espacio digital) sobre la que ejercen una influencia primordial. La segunda diferencia entre estas empresas tecnológicas y sus formidables

predecesoras radica en que, cada vez más, ofrecen una gama completa de bienes y servicios, tanto digitales como del mundo real, necesarios para el funcionamiento de una sociedad moderna. En consecuencia, los Estados que no pueden ofrecer dichos bienes por su cuenta corren el riesgo de perjudicarse a sí mismos si sus medidas obligan a las empresas a cesar sus operaciones.

1.4. Cuando el poder se desplaza: Estados, empresas tecnológicas y autoridad en disputa

Se podría afirmar que el poder digital, en virtud de sus características particulares, reconfigura tanto las relaciones interestatales como, de manera más profunda, los vínculos entre actores estatales y no estatales. En este sentido, el ciberespacio tiende a erosionar las asimetrías convencionales, ampliando la capacidad de actores no estatales (incluso de menor escala) para proyectar influencia. En consecuencia, a diferencia de dominios tradicionales como el marítimo o el aéreo, el control por parte de las grandes potencias resulta más limitado.

Asimismo, la emergencia del poder digital trae consigo una profundización del cuestionamiento de la centralidad del Estado que se viene desarrollando desde décadas anteriores. En este escenario, los aportes de Susan Strange y Joseph Nye constituyen herramientas analíticas clave para comprender estas transformaciones desde perspectivas complementarias. Mientras Strange (1996) se centra en la difusión de la autoridad, es decir, el proceso de fragmentación o desplazamiento de la autoridad estatal hacia otros niveles y actores; Nye (2011) pone el foco en la difusión del poder, entendida como la creciente distribución de capacidades entre una pluralidad de actores estatales y no estatales a nivel internacional.

En primer lugar, Susan Strange (1996) plantea que la autoridad estatal está experimentando un período de difusión, tras siglos de creciente centralización en la institución del Estado. Las fronteras territoriales ya no delimitan con precisión el alcance de la autoridad política sobre la economía y la sociedad, lo que se traduce en una pérdida relativa de capacidad estatal para desempeñar sus funciones básicas, entre las cuales se encuentran la creación, el almacenamiento y la comunicación del conocimiento y la información.

En este sentido, la autoridad estatal tiene "escapes" en múltiples direcciones: hacia arriba (frente a instituciones internacionales), hacia los lados (frente a otros Estados y diversos actores privados como las empresas transnacionales), y hacia abajo (frente a autoridades locales y regionales). Incluso, la autora advierte que existen algunas responsabilidades importantes de la autoridad estatal que nadie está en posición de ejecutar completamente. Esto no significa que los Estados sean obsoletos, por el contrario, aun colectivamente son las fuentes más influyentes. Sin embargo, se están convirtiendo cada vez más en instituciones "huecas" (Strange, 1996).

En paralelo, Strange (1996) destaca que la naturaleza de la competencia interestatal también ha mutado: en el pasado, los Estados competían los unos con otros por el control sobre el territorio y sobre los recursos generadores de riqueza dentro de éste. Ahora están compitiendo cada vez más por porciones de mercado en la economía mundial. Como consecuencia, la política industrial y la comercial se han vuelto más importantes que la defensa y la política exterior. Se podría afirmar, entonces, que el poder digital está cambiando las formas de competencia entre los actores del sistema internacional, como lo hizo con la competencia económica hace décadas atrás.

En diálogo con estos aportes, Joseph Nye (2011) sostiene que las transformaciones cibernéticas han favorecido la emergencia de estructuras en red que desafían las jerarquías

tradicionales, generando un cambio profundo en la naturaleza del poder y aumentando su difusión. Si bien los Estados seguirán siendo el actor dominante en el escenario mundial, lo encontrarán mucho más concurrido y difícil de controlar. Esto se debe a que la mayor parte de la población mundial tiene acceso al poder que emana de la información. En efecto, Nye advierte que, a medida que se desarrollen comunidades virtuales en internet, estas trascenderán las jurisdicciones territoriales y desarrollarán sus propios modelos de gobernanza. Los Estados perderán gran parte de su papel central en la vida de las personas y la gente vivirá mediante múltiples contratos voluntarios, pudiendo entrar y salir de comunidades virtuales con un simple clic.

Dicho de otro modo, la creciente participación de actores diversos y la dificultad para controlar los flujos de información configuran un escenario en el cual las capacidades de poder se encuentran más ampliamente distribuidas. Muchos de estos nuevos actores transnacionales afirman actuar como una "conciencia global", representando intereses públicos generales que trascienden el ámbito de los Estados nacionales. Si bien no son elegidos democráticamente, estos actores suelen contribuir al desarrollo de nuevas normas presionando directamente a gobiernos para que modifiquen políticas, e indirectamente alterando la percepción pública sobre la legitimidad y las funciones que deberían desempeñar. En términos de recursos de poder, estos actores rara vez poseen un gran poder coercitivo, pero la revolución tecnológica ha potenciado enormemente su poder blando (Nye, 2011).

Dentro de este escenario, la noción de "plataformización" resulta central para comprender las transformaciones contemporáneas en las relaciones de poder. Lejos de ser espacios neutrales, las plataformas digitales constituyen estructuras de mediación profundamente políticas. Como señala Srnicek (2017), su posición de intermediarias les

otorga acceso privilegiado a grandes volúmenes de datos y les permite ejercer un control significativo sobre el mercado y las dinámicas sociales.

> El ecosistema de plataformas (...) está plagado de paradojas: aparenta ser igualitario, pero es jerárquico; es casi totalmente corporativo, pero parece servir al bien público; aparenta ser neutral y agnóstico, pero su arquitectura conlleva un conjunto particular de valores ideológicos; sus efectos parecen locales, mientras que su alcance e impacto son globales; aparenta reemplazar el modelo verticalista de "gobierno centralizado" con un modelo de "empoderamiento del cliente" participativo, pero lo hace mediante una estructura altamente centralizada que permanece opaca para sus usuarios. (Van Dijck et al., 2018, p. 12)

De este modo, las plataformas no solo median la actividad social, sino que intervienen activamente en la configuración de lo visible y lo invisible mediante decisiones algorítmicas.

Los algoritmos ocupan un lugar central en el funcionamiento de las redes sociales, ya que permiten procesar grandes volúmenes de datos para filtrar contenidos y vincular a los usuarios con información, servicios y publicidad de forma personalizada. Como advierte Gillespie (2018), estas no se limitan a alojar contenidos, sino que, mediante sistemas de moderación, clasificación y priorización algorítmica, establecen normas y definen qué resulta visible o aceptable, configurando activamente el espacio público digital. Sin embargo, estos procesos se caracterizan por su opacidad: los algoritmos suelen resguardarse como secretos comerciales, son cada vez más complejos y están en constante ajuste, lo que dificulta su comprensión y plantea interrogantes sobre la legitimidad y la rendición de cuentas de estas formas de gobernanza.

La plataformización puede entenderse, entonces, como un proceso de reconfiguración estructural de la gobernanza basado en el control de los datos. Tal como sostiene Törnberg (2024), este fenómeno implica una forma de acumulación capitalista basada en la utilización

de datos para privatizar funciones regulatorias y manipular mercados. A diferencia de los modelos tradicionales de regulación estatal, las plataformas constituyen una arquitectura digital esencial para la sociedad que les permiten ejercer control directo sobre las interacciones económicas y sociales, desplazando progresivamente a las instituciones públicas.

Este desplazamiento tiene efectos significativos sobre la relación entre el Estado y las plataformas. A medida que estas últimas expanden su capacidad regulatoria, comienzan a disputar funciones tradicionalmente asociadas a la soberanía estatal. En este marco, resulta pertinente introducir el concepto de soberanía digital de un Estado, entendido por Ali Shoker como "el dominio absoluto sobre todos sus activos digitales, incluyendo toda la cadena de valor: datos, infraestructura, operaciones, cadena de suministro y conocimiento" (Shoker, 2022, p. 4).

Según Törnberg (2024), las grandes corporaciones, a través de las plataformas, no se limitan a operar dentro de los sistemas existentes, sino que buscan moldearlos e incluso sustituirlos, aprovechando debilidades institucionales y movilizando recursos económicos y políticos a gran escala. En este contexto, el Estado deja de ser únicamente un regulador para convertirse también en un competidor en la disputa por el control de los mercados y de los marcos normativos. Así, estas compañías tienden a trascender su rol de prestadoras de servicios, aspirando a apropiarse de funciones propias del Estado y a consolidarse como entidades con capacidad de gobierno.

El debilitamiento del Estado frente a las *Big Tech* no responde solo a dinámicas de imposición, sino también a dinámicas de cooptación que facilitan su inserción en las estructuras de poder. A través de estrategias de *lobby* intensivo, el reclutamiento de funcionarios públicos (que terminan defendiendo agendas privadas), la creación de *think tanks* y programas de capacitación para legisladores, estas empresas logran incidir en la

formulación de políticas y regulaciones, favoreciendo intereses corporativos (Malacalza, 2025). Los llamados “términos de servicio” que regulan la relación entre usuarios y plataformas constituyen instrumentos clave de este poder. Aunque se presentan como acuerdos contractuales, en la práctica funcionan como marcos normativos que establecen derechos, obligaciones y valores, muchas veces sin un consentimiento plenamente informado por parte de los usuarios (Van Dijck et al., 2018).

En conjunto, estos elementos evidencian una creciente difuminación de las fronteras entre lo público y lo privado. Este proceso plantea desafíos fundamentales para la soberanía estatal, ya que introduce nuevos actores con capacidad de ejercer poder a escala planetaria, sin estar sujetos a los mismos mecanismos de control democrático que el resto (Van Dijck et al., 2018).

Capítulo 2: Después de la pandemia: dependencia digital, ciberseguridad y nuevas reglas para el ciberespacio

La pandemia de COVID-19 trajo consigo una profundización de las transformaciones que ya se encontraban en marcha en el escenario internacional, especialmente aquellas vinculadas con la digitalización, la expansión de las plataformas digitales y la creciente relevancia estratégica del ciberespacio. A partir de este proceso, se volvió necesario analizar cómo la dependencia digital adquirió mayor intensidad, cómo las grandes empresas tecnológicas consolidaron su centralidad y de qué manera los Estados comenzaron a responder frente a los riesgos asociados al entorno digital.

En este escenario, el presente capítulo aborda, en primer lugar, la influencia de la pandemia en la aceleración de la digitalización y en la consolidación de la conectividad como recurso esencial. Luego, se analiza la centralidad adquirida por la ciberseguridad en la agenda estatal, en tanto dimensión vinculada a la protección de datos, infraestructuras críticas y capacidades soberanas. Posteriormente, se examinan los principales marcos regulatorios adoptados por los actores estatales y regionales frente a los desafíos del ciberespacio. Finalmente, se desarrollan los mecanismos de gobernanza global, incluyendo espacios multilaterales y acuerdos internacionales orientados a ordenar la cooperación en materia digital y cibernética.

2.1. El COVID-19 como catalizador de la dependencia digital a nivel mundial

La pandemia de COVID-19 constituyó un punto de inflexión en el proceso de digitalización global. Si bien la expansión de las tecnologías digitales ya se encontraba en marcha antes de 2020, la crisis sanitaria aceleró de manera abrupta su incorporación en múltiples dimensiones de la vida social, económica, política y cultural. La rápida propagación

internacional del virus SARS-CoV-2 llevó a que, el 30 de enero de 2020, la Organización Mundial de la Salud (OMS) declarara la emergencia de salud pública de importancia internacional y, el 11 de marzo del mismo año, calificara oficialmente al brote como pandemia. A partir de entonces, numerosos Estados implementaron medidas de contención, tales como cuarentenas obligatorias, restricciones a la circulación, cierres de fronteras y suspensión de actividades presenciales. Estas políticas, orientadas a reducir los contagios y evitar el colapso de los sistemas sanitarios, produjeron una disrupción sin precedentes en el funcionamiento cotidiano de las sociedades.

En este contexto, la conectividad digital pasó de ocupar un lugar complementario a convertirse en una infraestructura esencial para sostener actividades básicas. Las restricciones a la movilidad y el distanciamiento social obligaron a trasladar gran parte de la vida cotidiana al entorno digital. Actividades como el trabajo, la educación, el consumo, el entretenimiento y la interacción social comenzaron a depender crecientemente de plataformas digitales, acelerando procesos de digitalización que ya estaban en marcha.

Uno de los ámbitos donde este cambio fue más evidente fue el trabajo. El teletrabajo se convirtió en la norma para millones de personas en todo el mundo, especialmente en sectores vinculados a los servicios, permitiendo la continuidad de diversas actividades económicas en medio de las restricciones sanitarias. Según datos de la Organización Internacional del Trabajo (OIT), durante el punto más alto de la pandemia cerca del 20% de la fuerza laboral mundial trabajaba desde sus hogares, con cifras más elevadas en economías desarrolladas (OIT, 2020). En este proceso, aplicaciones como Zoom, Microsoft Teams y Google Meet adquirieron una centralidad inédita, al transformarse en herramientas indispensables para sostener reuniones laborales, capacitaciones virtuales, conferencias, actividades administrativas y vínculos organizacionales.

Sin embargo, este desplazamiento hacia el teletrabajo no fue homogéneo ni estuvo exento de tensiones. La posibilidad de trabajar desde el hogar dependió del tipo de actividad realizada, del nivel de conectividad disponible, del acceso a dispositivos adecuados y de las capacidades digitales de trabajadores y organizaciones. En consecuencia, la pandemia también puso en evidencia desigualdades preexistentes entre sectores económicos, regiones y grupos sociales. Mientras algunas actividades pudieron adaptarse rápidamente al entorno digital, otras quedaron paralizadas o debieron sostenerse de manera presencial, exponiendo diferencias en términos de vulnerabilidad laboral, acceso tecnológico y capacidad de adaptación.

El sistema educativo experimentó una transformación igualmente abrupta. De acuerdo con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), más de 1.600 millones de estudiantes en más de 190 países se vieron afectados por el cierre de instituciones educativas en 2020 (UNESCO, 2020). Frente a esta situación, la educación a distancia se implementó de manera masiva, muchas veces sin la preparación pedagógica, técnica e institucional necesaria. Las plataformas de videoconferencia, las aulas virtuales y los servicios digitales de almacenamiento y comunicación se volvieron recursos fundamentales para garantizar cierta continuidad educativa. No obstante, esta transición también evidenció profundas brechas en el acceso a una conexión a internet de calidad, a dispositivos tecnológicos y a condiciones adecuadas de estudio, lo que condicionó de manera desigual las posibilidades de adaptación de estudiantes, docentes e instituciones.

Al mismo tiempo, se produjo un notable incremento en el consumo digital y en el uso de plataformas. El comercio electrónico, los servicios de *streaming*, las redes sociales y los sistemas de pago digital registraron un crecimiento acelerado. Empresas tecnológicas como Amazon, Netflix o Meta vieron expandirse significativamente su base de usuarios y sus ingresos.

Esta expansión del uso de plataformas también generó presión sobre la infraestructura digital existente. El aumento del tráfico en internet, la demanda de servicios en la nube, la multiplicación de reuniones virtuales y el crecimiento del *e-commerce* evidenciaron la importancia estratégica de contar con redes robustas, seguras y estables.

El desarrollo de vacunas a fines de 2020 permitió iniciar campañas de vacunación masiva durante 2021, lo que contribuyó a reducir la mortalidad y la gravedad de los casos. Gracias a esto, los Estados flexibilizaron las restricciones y las actividades presenciales fueron retomándose progresivamente. Finalmente, en mayo de 2023, la OMS declaró el fin de la emergencia sanitaria internacional, marcando el cierre formal de la fase más crítica de la crisis. Sin embargo, las transformaciones impulsadas durante este período no desaparecieron con el fin de la emergencia. Muchas prácticas digitales incorporadas durante la pandemia persistieron y se consolidaron como parte del funcionamiento habitual de las sociedades contemporáneas.

Entre los efectos más significativos de la pandemia se encuentra la consolidación de la conectividad digital como un recurso estratégico y, en muchos casos, como un componente indispensable para el ejercicio de derechos básicos. Diversos gobiernos implementaron medidas orientadas a garantizar el acceso a internet, ampliar redes de banda ancha, reducir brechas digitales y promover la inclusión tecnológica. Esto contribuyó a instalar la idea de que la conectividad no puede ser entendida únicamente como un bien de mercado, sino también como una infraestructura de interés público, vinculada al acceso a la educación, al trabajo, a la información, a los servicios estatales y a la participación social.

2.2. La ciberseguridad en el centro de la agenda estatal

La intensificación de la dependencia digital durante la pandemia tuvo como consecuencia directa una mayor exposición de Estados, sociedades, empresas e individuos a los riesgos propios del espacio digital, en tanto incrementó la superficie potencial de ataque disponible para actores maliciosos. En otras palabras, cuanto mayor fue la incorporación de tecnologías digitales en la vida cotidiana, mayor fue también la vulnerabilidad frente a intrusiones, filtraciones de datos, fraudes informáticos, ataques a infraestructuras críticas y operaciones de desinformación.

En este escenario, la pandemia contribuyó a reforzar la percepción del ciberespacio como un ámbito de competencia estratégica. La expansión de la interacción digital incrementó las oportunidades para que actores estatales y no estatales desarrollaran operaciones de espionaje, sabotaje, robo de información, interrupción de servicios y manipulación informativa. Johanson y Chong (2024) sostienen que la mayor dependencia de herramientas digitales posterior a la pandemia incrementó la vulnerabilidad de las personas y de los sistemas frente a ciberataques, al mismo tiempo que ofreció nuevas oportunidades para que Estados en conflicto afectaran las capacidades de otros países sin recurrir necesariamente a una confrontación física directa.

Así, la ciberseguridad comenzó a consolidarse como una prioridad estratégica de la agenda estatal. Ya no se trataba únicamente de proteger sistemas informáticos aislados, sino de preservar la confidencialidad, integridad y disponibilidad de datos sensibles, redes e infraestructuras digitales indispensables para el funcionamiento de las sociedades contemporáneas. En consecuencia, los ciberataques dejaron de ser percibidos exclusivamente como amenazas contra empresas o usuarios particulares y comenzaron a ser interpretados como riesgos capaces de afectar la seguridad nacional, la estabilidad económica, la prestación de servicios esenciales y, en algunos casos, la paz y la seguridad internacional.

> La ciberseguridad consiste en medidas para proteger el funcionamiento de un sistema informático o la integridad de sus datos frente a acciones hostiles. También puede concebirse como un estado de cosas: la ausencia de intrusiones no autorizadas en los sistemas informáticos y su correcto funcionamiento. Una concepción alternativa de la ciberseguridad, a menudo denominada «seguridad de la información», implica la protección gubernamental de los canales de flujo de información en la sociedad. (Kello, 2013, p. 18)

Esta doble dimensión resulta especialmente relevante para el presente análisis, ya que muestra que la ciberseguridad no se limita a la prevención de fallas técnicas, sino que involucra cuestiones de autoridad, control, soberanía y poder sobre la circulación de información en el espacio digital.

En la misma línea, Henen (2025) sostiene que la ciberseguridad se configura como un campo en constante evolución, orientado al desarrollo de estándares, procedimientos y mecanismos de protección que permiten prevenir incidentes, mitigar vulnerabilidades y reducir el impacto de posibles ataques.

La gravedad de los riesgos asociados al ciberespacio llevó a un número creciente de Estados a incorporar medidas de ciberseguridad dentro de sus doctrinas, estrategias y políticas de seguridad. Esta tendencia se inscribe en una transformación digital más amplia, caracterizada por la integración de tecnologías avanzadas en áreas sensibles de la gestión estatal, tales como los sistemas energéticos, sanitarios, financieros, logísticos, administrativos y de telecomunicaciones (Henen, 2025).

2.3. Las nuevas reglas del entorno digital: respuestas estatales y regionales

La consolidación de la ciberseguridad como prioridad estratégica se tradujo, a partir de 2020, en una proliferación de estrategias nacionales, leyes, directivas y marcos

regulatorios orientados a ordenar el funcionamiento del ciberespacio. Estas respuestas estatales no fueron homogéneas, por el contrario, adoptaron formas diversas según las capacidades institucionales de cada país, sus tradiciones jurídicas, sus intereses geopolíticos, su grado de desarrollo tecnológico y el lugar que ocupan dentro de la economía digital global.

En relación con esto, Mukherjee (2025) sostiene que la revolución tecnológica abrió un nuevo ámbito de competencia digital en el que actores estatales y no estatales aprovechan las innovaciones emergentes para alcanzar objetivos económicos y geopolíticos. En respuesta a estos cambios, diversas naciones impulsaron regulaciones destinadas a salvaguardar los datos, proteger los sistemas digitales y establecer condiciones de funcionamiento para las empresas tecnológicas que operan dentro de sus jurisdicciones.

Por ello, los marcos regulatorios adoptados desde 2020 no deben ser interpretados únicamente como respuestas defensivas frente al aumento de ciberamenazas, sino también como instrumentos de reafirmación de soberanía digital. A través de estas normas, los Estados buscan definir quién puede recolectar, almacenar y transferir datos; qué obligaciones tienen las empresas tecnológicas frente a los usuarios y las autoridades públicas; cómo deben protegerse las infraestructuras críticas; qué responsabilidades corresponden a las empresas frente a incidentes de seguridad; y bajo qué condiciones pueden operar tecnologías consideradas sensibles. A continuación, se presentan algunos ejemplos relevantes de marcos regulatorios adoptados en los últimos años por actores centrales del sistema internacional.

2.3.1. EE. UU.

En el caso de EE. UU., la respuesta regulatoria posterior a la pandemia estuvo fuertemente asociada a la seguridad nacional, la protección de infraestructuras críticas, la seguridad de las cadenas de suministro digitales y la cooperación público-privada.

Una primera medida relevante fue la Orden Ejecutiva 14028: *Improving the Nation's Cybersecurity*, emitida por la administración Biden en mayo de 2021. Esta orden planteó la necesidad de mejorar sus capacidades para identificar, disuadir, proteger, detectar y responder frente a acciones cibernéticas maliciosas. Además, destacó que la ciberseguridad no podía depender exclusivamente de la acción estatal, sino que requería una asociación estrecha con el sector privado, dado que muchas de las tecnologías, productos y servicios digitales esenciales son desarrollados y operados por empresas privadas (The White House, 2021).

La Orden introdujo, asimismo, una amplia agenda de modernización de la ciberseguridad federal. Entre sus principales líneas de acción se incluyeron la eliminación de barreras para compartir información sobre amenazas entre proveedores tecnológicos y agencias federales, la modernización de la seguridad informática del gobierno federal, la adopción de arquitecturas de confianza cero, el uso de autenticación multifactorial y cifrado, la mejora de la seguridad de la cadena de suministro de *software* bajo la dirección del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), la creación de un *Cyber Safety Review Board* y el fortalecimiento de las capacidades de detección, investigación y respuesta frente a incidentes cibernéticos (General Services Administration, 2021).

En cumplimiento de ese mandato, el NIST desarrolló diversas guías y herramientas destinadas a aumentar la trazabilidad de los componentes utilizados en productos digitales y mejorar la capacidad de detectar vulnerabilidades antes de que sean explotadas. De este modo, la ciberseguridad dejó de pensarse únicamente como protección reactiva frente a ataques y comenzó a incorporar una lógica preventiva orientada a reducir riesgos desde el diseño, desarrollo, adquisición y mantenimiento del *software* (NIST, 2021).

Posteriormente, en junio de 2021 la administración Biden emitió la Orden Ejecutiva 14034, orientada a evaluar los riesgos de seguridad nacional asociados con aplicaciones digitales vinculadas a países considerados adversarios extranjeros. Esta orden revocó las medidas previas de la administración Trump contra TikTok y WeChat, pero mantuvo la preocupación por el acceso extranjero a datos personales, la posible explotación de información sensible y la influencia de determinadas aplicaciones sobre el entorno digital estadounidense. A diferencia de la Orden Ejecutiva 14028, centrada en la modernización de la ciberseguridad federal, esta nueva medida se enfocó específicamente en los riesgos derivados de plataformas extranjeras y anticipó el conflicto entre EE. UU. y TikTok, que será desarrollado con mayor profundidad en el capítulo 3.

Luego, la Estrategia Nacional de Ciberseguridad de 2023 consolidó esta orientación. Este documento estableció cinco pilares principales: defender infraestructuras críticas; desarticular y desmantelar actores maliciosos; modificar los incentivos de mercado para promover seguridad y resiliencia; invertir en un futuro digital más seguro; y fortalecer alianzas internacionales.

Más allá de estos puntos, el cambio conceptual más relevante de la estrategia fue su llamado a "rebalancear" la responsabilidad de defender el ciberespacio. Esto implicó reconocer que durante años la carga de la ciberseguridad había recaído de manera desproporcionada sobre usuarios individuales, pequeñas organizaciones y actores con menor capacidad técnica, mientras que los grandes proveedores tecnológicos y las empresas con mayores recursos se encontraban en mejores condiciones para reducir riesgos sistémicos (The White House, 2023a). De este modo, la estrategia plantea que la seguridad del ecosistema digital depende mayormente de privados, pero asigna al Estado un papel central en la coordinación, regulación e imposición de obligaciones.

La Estrategia Nacional de Ciberseguridad fue complementada por un Plan de Implementación publicado en julio de 2023, posteriormente actualizado en 2024. Este plan tradujo los objetivos generales de la estrategia en iniciativas concretas, asignadas a agencias responsables y asociadas a plazos de cumplimiento (The White House, 2023b; The White House, 2024).

En la misma línea, la Ley de Notificación de Incidentes Cibernéticos para Infraestructuras Críticas de 2022 dispuso que la Agencia de Ciberseguridad y Seguridad de Infraestructura desarrollara regulaciones para exigir a determinadas entidades que proveen arquitectura digital crítica el reporte de incidentes cibernéticos relevantes y pagos por *ransomware*. Su objetivo principal fue mejorar la visibilidad del Estado sobre el panorama de amenazas, permitir una asistencia más rápida a las víctimas, identificar patrones entre sectores y compartir información con otros defensores de redes para prevenir ataques similares (Agencia de Ciberseguridad y Seguridad de Infraestructuras, 2022).

Finalmente, en junio de 2025, la administración Trump emitió la Orden Ejecutiva 14306: *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity,* orientada a sostener ciertos esfuerzos de fortalecimiento de la ciberseguridad nacional y modificar órdenes ejecutivas previas. Esta medida mantuvo la atención sobre áreas como desarrollo seguro de *software*, criptografía poscuántica y amenazas extranjeras (The White House, 2025).

En síntesis, la respuesta regulatoria de EE. UU. postpandemia estuvo orientada, en gran parte, por la elevada dependencia de sectores estratégicos respecto de infraestructuras digitales operadas muchas veces por actores privados. En consecuencia, el Estado centró su atención en fortalecer su capacidad de coordinación, establecer estándares mínimos de seguridad y ampliar los mecanismos de intercambio de información con el sector privado. En

la tabla 1 se recuperan los principales marcos regulatorios vinculados al espacio digital implementados por EE. UU. en el período postpandemia.

Tabla 1: Síntesis de los marcos regulatorios de EE. UU. relativos a la ciberseguridad (2020-2025)

Marco regulatorio	Objetivo	Año de adopción/aplicación
Orden Ejecutiva 14028: *Improving the Nation's Cybersecurity*	Modernizar la ciberseguridad federal, fortalecer la detección y respuesta ante incidentes y mejorar la seguridad de la cadena de suministro de *software*.	2021
Orden Ejecutiva 14034: *Protecting Americans' Sensitive Data from Foreign Adversaries*	Evaluar los riesgos de seguridad nacional asociados a aplicaciones digitales vinculadas con adversarios extranjeros.	2021
Ley de Notificación de Incidentes Cibernéticos para Infraestructuras Críticas	Exigir el reporte de incidentes cibernéticos relevantes y pagos por *ransomware* en sectores de infraestructura crítica.	2022
Estrategia Nacional de Ciberseguridad	Defender infraestructuras críticas, desarticular actores maliciosos, redistribuir responsabilidades y fortalecer la resiliencia del ecosistema digital.	2023
Orden Ejecutiva 14306: *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity*	Sostener y actualizar esfuerzos clave de ciberseguridad nacional, especialmente en *software* seguro, criptografía poscuántica y amenazas extranjeras.	2025

Fuente: Elaboración propia en base a las fuentes citadas en el presente apartado.

2.3.2. Unión Europea

La Unión Europea (UE), por su parte, desarrolló un modelo regulatorio más integral y normativo frente a los desafíos del ciberespacio. A diferencia del enfoque estadounidense, la estrategia europea combinó ciberseguridad, protección de derechos fundamentales, regulación de plataformas, competencia digital, resiliencia operativa, IA y autonomía estratégica. En este sentido, la UE buscó no solo proteger sus sistemas digitales frente a amenazas cibernéticas, sino también construir un marco común de reglas para ordenar el

mercado digital, limitar el poder de los actores privados y proyectar estándares regulatorios más allá de sus fronteras.

Un primer hito de este proceso fue la presentación de la Estrategia de Ciberseguridad de la UE para la Década Digital, en diciembre de 2020. Esta estrategia tuvo como objetivo reforzar la resiliencia de la región frente a amenazas cibernéticas, garantizar que ciudadanos y empresas pudieran beneficiarse de servicios digitales confiables y seguros, y defender un ciberespacio global, abierto, libre y seguro (Comisión Europea y Alto Representante de la UE, 2020).

Asimismo, en marzo de 2021, el Consejo de la UE vinculó explícitamente la ciberseguridad con el objetivo de alcanzar una mayor autonomía estratégica, preservando al mismo tiempo una economía abierta. De esta manera, la UE no plantea la ciberseguridad únicamente como una defensa frente a amenazas técnicas, sino como una condición para fortalecer su liderazgo digital, reducir dependencias estratégicas y aumentar su capacidad de tomar decisiones autónomas en un entorno tecnológico crecientemente competitivo (Consejo de la UE, 2021).

Dentro de este marco, la Segunda Directiva sobre los Sistemas de Red e Información (Directiva NIS2, por sus siglas en inglés) adoptada en 2022 constituyó una pieza fundamental, en tanto reemplazó y amplió la normativa anterior sobre seguridad de redes y sistemas de información. Su objetivo fue establecer un nivel común elevado de ciberseguridad en toda la Unión, incorporando obligaciones más estrictas para entidades consideradas esenciales e importantes. La directiva buscó armonizar criterios entre los Estados miembros y ampliar el alcance de la regulación hacia sectores críticos (UE, 2022).

La importancia de NIS2 radica en que desplaza la ciberseguridad desde una lógica voluntaria o sectorial hacia una lógica de obligación jurídica. Las entidades alcanzadas deben

adoptar medidas técnicas, operativas y organizativas adecuadas y proporcionales para gestionar los riesgos que afectan la seguridad de redes y sistemas de información. Entre estas medidas se incluyen políticas de análisis de riesgos, gestión de incidentes, continuidad del negocio, copias de seguridad, recuperación ante desastres, seguridad de la cadena de suministro, gestión de vulnerabilidades, ciberhigiene, formación, criptografía, control de accesos y autenticación multifactorial (UE, 2022).

A la par de estas medidas, el bloque europeo avanzó en la regulación de plataformas digitales mediante el Reglamento de Servicios Digitales (DSA, por sus siglas en inglés) y el Reglamento de Mercados Digitales (DMA, por sus siglas en inglés). Por un lado, el DSA comenzó a aplicarse a todas las plataformas en línea de la UE en febrero de 2024, aunque sus obligaciones reforzadas ya regían desde agosto de 2023 para las plataformas y motores de búsqueda de muy gran tamaño. Este instrumento es destacable ya que introduce obligaciones de transparencia, evaluación y mitigación de riesgos sobre actores privados que cumplen funciones de intermediación social y política. Las grandes plataformas ya no son concebidas únicamente como proveedoras de servicios digitales, sino como sistemas de comunicación con capacidad de incidir en derechos, procesos democráticos, circulación de información y seguridad pública (Comisión Europea, 2024).

El DMA, por el otro lado, comenzó a aplicarse en mayo de 2023 y buscó garantizar mercados digitales más justos y disputables. A diferencia del DSA, este reglamento apunta a limitar prácticas anticompetitivas de las empresas digitales que actúan como *gatekeepers*, es decir, que ocupan una posición de intermediación clave entre usuarios empresariales y consumidores. Se observa que estos actores pueden funcionar como “reguladores privados” del acceso a mercados digitales, generando cuellos de botella y condicionando la capacidad de competencia de otras empresas (Comisión Europea, 2023).

En efecto, en septiembre de 2023, la Comisión Europea designó por primera vez a seis *gatekeepers* bajo el DMA: Alphabet, Amazon, Apple, ByteDance, Meta y Microsoft. En conjunto, fueron identificados 22 servicios básicos de plataforma sujetos a obligaciones específicas. Estas empresas debieron adaptar sus prácticas en un plazo de seis meses para cumplir con las obligaciones del reglamento (Comisión Europea, 2023).

A estas normas se sumó el Reglamento de Ciberresiliencia, adoptado por el Consejo de la UE en octubre de 2024, que introdujo requisitos de ciberseguridad para productos con elementos digitales, incluyendo *software* y *hardware* conectados. Su finalidad es asegurar que los productos digitales sean diseñados, desarrollados, producidos y comercializados con estándares de seguridad adecuados durante todo su ciclo de vida (Consejo de la UE, 2024). Esto implica que fabricantes y desarrolladores deben incorporar requisitos de ciberseguridad antes de colocar productos en el mercado, así como mantener actualizaciones y mecanismos de gestión de vulnerabilidades.

Otro componente relevante es el Reglamento de Resiliencia Operativa Digital (DORA, por sus siglas en inglés), aplicable desde enero de 2025. Este instrumento está orientado al sector financiero y busca garantizar que entidades financieras puedan resistir, responder y recuperarse frente a perturbaciones relacionadas con las TIC (Autoridad Europea de Valores y Mercados, 2025).

Finalmente, la UE aprobó el Reglamento de IA, en vigor desde agosto de 2024. Esta norma estableció un marco regulatorio uniforme para el desarrollo y uso de sistemas de IA, basado en un enfoque de riesgos. El reglamento distingue entre usos de riesgo mínimo, riesgo limitado, alto riesgo y prácticas prohibidas, e introduce obligaciones diferenciadas para desarrolladores y usuarios según el nivel de riesgo que los sistemas puedan representar para la salud, la seguridad y los derechos fundamentales (Comisión Europea, 2024).

Esta normativa amplía el alcance de la regulación digital europea hacia tecnologías algorítmicas capaces de incidir en decisiones públicas y privadas. De esta forma, expresa la preocupación de la Unión por evitar que el desarrollo de sistemas de IA quede exclusivamente en manos de grandes empresas tecnológicas sin controles públicos suficientes.

En conjunto, estas iniciativas muestran que la UE construyó un modelo regulatorio denso, transversal y con vocación de proyección global. Los marcos regulatorios adoptados post pandemia no deben entenderse como normas aisladas, sino como partes de una arquitectura regulatoria orientada a fortalecer la capacidad europea de gobernar el espacio digital. En la tabla 2 se recuperan los principales marcos regulatorios vinculados al espacio digital implementados por la UE en el período postpandemia.

Tabla 2: Síntesis de los marcos regulatorios de la UE relativos a la ciberseguridad (2020-2025)

Marco regulatorio	Objetivo	Año de adopción/aplicación
Estrategia de Ciberseguridad de la Unión Europea para la Década Digital	Reforzar la resiliencia cibernética europea y promover un ciberespacio global, abierto, libre y seguro.	2020
Directiva NIS2	Establecer un nivel común elevado de ciberseguridad en la UE mediante obligaciones para entidades esenciales e importantes.	2022
Reglamento de Mercados Digitales	Limitar el poder de los *gatekeepers* y garantizar mercados digitales más justos, abiertos y disputables.	2023
Reglamento de Servicios Digitales	Regular plataformas e intermediarios digitales mediante obligaciones de transparencia, responsabilidad y mitigación de riesgos sistémicos.	2024
Reglamento de Ciberresiliencia	Incorporar requisitos de ciberseguridad para productos digitales durante todo su ciclo de vida.	2024
Reglamento de Inteligencia Artificial	Regular los sistemas de IA según su nivel de riesgo y proteger la seguridad, la salud y los derechos fundamentales.	2024
Reglamento de Resiliencia	Fortalecer la capacidad del sector	2025

Marco regulatorio	Objetivo	Año de adopción/aplicación
Operativa Digital	financiero para resistir, responder y recuperarse de incidentes vinculados a las TIC.	

Fuente: Elaboración propia en base a las fuentes citadas en el presente apartado.

2.3.3. China

El caso de China expresa un modelo regulatorio distinto al estadounidense y al europeo, centrado en la soberanía cibernética, la seguridad nacional, el control estatal de los datos y la subordinación del ecosistema digital a los objetivos políticos, económicos y estratégicos del Estado.

Un primer elemento central de este modelo es la Ley de Seguridad de Datos, adoptada en junio de 2021, la cual estableció un marco general para regular las actividades de procesamiento de datos. Esta nueva política promueve la circulación de datos en tanto favorece la innovación y el crecimiento, pero queda sujeta a mecanismos de clasificación, supervisión y control estatal cuando puede afectar intereses estratégicos. Esta norma también introdujo una lógica de clasificación y jerarquización de los datos en tres categorías principales: datos ordinarios, datos importantes y datos vinculados a sectores sensibles (National People's Congress of China, 2021).

En paralelo, la Ley de Protección de Información Personal, adoptada en agosto de 2021, reguló el tratamiento de datos personales, los derechos de los individuos y las obligaciones de quienes procesan información personal. La norma estableció principios para la recolección, uso, almacenamiento, transferencia y eliminación de información personal, así como obligaciones específicas para los procesadores de datos. También incorporó disposiciones sobre transferencia transfronteriza de información personal y sobre las responsabilidades de plataformas que procesan grandes volúmenes de datos de usuarios (National People's Congress of China, 2021).

Según este modelo, la privacidad aparece protegida, pero dentro de un esquema donde el Estado conserva amplias capacidades de supervisión y donde las empresas tecnológicas deben adecuarse a las prioridades regulatorias definidas por las autoridades. Por ello, la regulación china de datos personales no debe interpretarse únicamente como una política de derechos individuales, sino también como parte de una arquitectura más amplia de control estatal sobre el ecosistema digital.

Otro componente relevante fue el fortalecimiento de la protección de infraestructuras críticas de información a partir de la aprobación del Reglamento sobre la Seguridad y Protección de Infraestructuras Críticas de Información, vigente desde septiembre de 2021. Este reglamento define como infraestructuras críticas a redes e información vinculadas con sectores como telecomunicaciones, servicios de información, energía, transporte, finanzas, servicios públicos, gobierno electrónico y otros ámbitos cuya destrucción, pérdida de funcionamiento o filtración de datos pueda afectar gravemente la seguridad nacional, la economía, la vida social o el interés público (State Council of the People's Republic of China, 2021).

A esta arquitectura se sumaron las Medidas de Revisión de Ciberseguridad, vigentes desde febrero de 2022. Estas medidas ampliaron el alcance de los controles sobre operadores de plataformas digitales, en particular, las firmas tecnológicas que posean información personal de más de un millón de usuarios y busquen cotizar en el extranjero deben someterse a una revisión de ciberseguridad (Cyberspace Administration of China, 2022). Desde la perspectiva china, la salida de empresas digitales a mercados extranjeros puede generar riesgos no solo financieros, sino también informacionales y geopolíticos, en la medida en que datos sensibles puedan quedar expuestos a autoridades, regulaciones o presiones externas.

En la misma línea, en 2022, la Administración del Ciberespacio de China emitió medidas de evaluación de seguridad para la exportación de datos, destinadas a regular las condiciones bajo las cuales ciertos datos personales o datos importantes pueden transferirse al exterior (Library of Congress, 2022). Este régimen fue ajustado en 2024 mediante las Disposiciones para Promover y Regular los Flujos Transfronterizos de Datos. Estas disposiciones buscaron precisar estándares de declaración, delimitar escenarios exceptuados de evaluación y facilitar ciertos flujos transfronterizos, especialmente en actividades comerciales, contractuales, laborales o de emergencia (Cyberspace Administration of China, 2024).

China también tuvo grandes avances en el campo de las tecnologías emergentes. En efecto, las Disposiciones sobre la Administración de Recomendaciones Algorítmicas en los Servicios de Información de Internet, vigentes desde marzo de 2022, establecieron obligaciones para proveedores de servicios de recomendación en internet, incluyendo transparencia, opciones para usuarios, gestión de contenidos, evaluaciones de seguridad y registros ante autoridades cuando los servicios tengan capacidad de influir en la opinión pública o movilización social (Cyberspace Administration of China, 2021).

Posteriormente, en 2023, China adoptó las Medidas Provisionales para la Administración de los Servicios de IA Generativa, haciendo énfasis en la protección de la seguridad nacional, el interés público, los derechos de las personas y la gestión del contenido generado por estas tecnologías (State Council of the People’s Republic of China, 2023).

Por todo esto, el caso chino resulta especialmente relevante para comprender que la disputa por el poder digital no adopta una única forma. En China, la respuesta estatal no se orienta principalmente a equilibrar mercado y derechos, como en la UE, ni a fortalecer la resiliencia público-privada frente a amenazas, como en EE. UU., sino a consolidar la

capacidad del Estado para dirigir, supervisar y condicionar el desarrollo del ecosistema digital. Esta orientación revela una concepción del ciberespacio como territorio estratégico de gobierno, donde datos, plataformas, algoritmos e infraestructuras se integran a una política más amplia de seguridad, desarrollo y soberanía nacional. En la tabla 3 se recuperan los principales marcos regulatorios vinculados al espacio digital implementados por China en el período postpandemia.

Tabla 3: Síntesis de los marcos regulatorios de China relativos a la ciberseguridad (2020-2025)

Marco regulatorio	Objetivo	Año de adopción/aplicación
Ley de Seguridad de Datos	Regular el procesamiento, clasificación y circulación de datos para proteger la seguridad nacional y los intereses estratégicos del Estado.	2021
Ley de Protección de Información Personal	Proteger la información personal y establecer obligaciones para quienes recolectan, procesan, almacenan o transfieren datos personales.	2021
Reglamento sobre la Seguridad y Protección de Infraestructuras Críticas de Información	Proteger redes, sistemas e información crítica cuya afectación pueda comprometer la seguridad nacional, la economía o el interés público.	2021
Medidas de Revisión de Ciberseguridad	Evaluar riesgos de seguridad nacional asociados a operadores críticos, plataformas digitales y transferencia de datos sensibles.	2022
Disposiciones sobre la Administración de Recomendaciones Algorítmicas en los Servicios de Información de Internet	Regular los sistemas de recomendación algorítmica, promoviendo transparencia, control estatal y gestión de contenidos.	2022
Medidas Provisionales para la Administración de los Servicios de Inteligencia Artificial Generativa	Regular los servicios de IA generativa para proteger la seguridad nacional, el interés público y los derechos de las personas.	2023
Disposiciones para Promover y Regular los Flujos Transfronterizos de Datos	Ordenar y facilitar transferencias internacionales de datos, precisando requisitos, evaluaciones y excepciones regulatorias.	2024

Fuente: Elaboración propia en base a las fuentes citadas en el presente apartado.

2.3.4. Brasil

Desde una perspectiva latinoamericana, el caso de Brasil resulta especialmente relevante en tanto muestra cómo la preocupación por la ciberseguridad también se incorporó crecientemente a la agenda del Sur global.

Como antecedente inmediato, en febrero de 2020, Brasil aprobó su primera Estrategia Nacional de Seguridad Cibernética, la cual fue concebida como una orientación del gobierno federal para la sociedad brasileña respecto de las principales acciones nacionales e internacionales en materia de seguridad cibernética (Presidência da República do Brasil, 2020). Su aprobación al inicio del período pandémico resulta relevante, ya que anticipó la necesidad de organizar capacidades estatales en un contexto en el que la digitalización se aceleraría de manera abrupta y aumentaría la exposición de personas, empresas e instituciones públicas a amenazas cibernéticas.

Posteriormente, la Medida Provisional n.º 1.068, firmada por Jair Bolsonaro en 2021, buscó modificar el Marco Civil de Internet para limitar la capacidad de las plataformas digitales de remover contenidos, suspender cuentas o aplicar medidas de moderación de manera unilateral. La norma exigía que las empresas operadoras justificaran sus decisiones bajo criterios más estrictos y fue presentada por el gobierno como una medida orientada a proteger la libertad de expresión de los usuarios. Esta medida será retomada con mayor detalle en el capítulo 3, al analizar la evolución del conflicto entre Brasil y X.

La institucionalización de esta agenda se profundizó en diciembre de 2023 con el Decreto n.º 11.856, en el que el Estado brasileño instituyó la Política Nacional de Ciberseguridad y el Comité Nacional de Ciberseguridad, cuya finalidad consistió en orientar la actividad de seguridad cibernética en el país (Presidência da República do Brasil, 2023). La relevancia de esta política radica en que articula la ciberseguridad con tres dimensiones

centrales para el análisis de la disputa por el poder digital. En primer lugar, la vincula con la soberanía nacional, al considerar que la protección del ciberespacio forma parte de la defensa de los intereses estratégicos del país. En segundo lugar, la relaciona con la protección de derechos fundamentales, especialmente en materia de privacidad, datos personales, libertad de expresión y acceso a la información. En tercer lugar, la conecta con la resiliencia de arquitectura digital crítica y servicios esenciales, lo que implica reconocer que la interrupción de redes, sistemas y servicios digitales puede afectar el funcionamiento cotidiano del Estado, la economía y la sociedad.

Asimismo, el decreto estableció dos soportes fundamentales a dicha política, a saber, la Estrategia Nacional de Ciberseguridad y el Plan Nacional de Ciberseguridad, e instituyó el Comité Nacional de Ciberseguridad como órgano encargado de acompañar la implementación y evolución de esta (Presidência da República do Brasil, 2023).

El caso brasileño también debe leerse en relación con la protección de datos personales. Si bien la Ley General de Protección de Datos Personales fue promulgada en 2018, su relevancia se consolidó durante el período posterior a la pandemia, cuando la expansión de servicios digitales intensificó la recolección, tratamiento y circulación de información personal. Esta ley regula el tratamiento de datos personales realizado por personas naturales o jurídicas, públicas o privadas, y tiene como objetivo proteger los derechos fundamentales de libertad, privacidad y libre desarrollo de la personalidad (Autoridade Nacional de Proteção de Dados, 2024).

La evolución de esta política continuó en 2025, cuando Brasil instituyó una nueva Estrategia Nacional de Ciberseguridad. Esta última fue presentada como la segunda versión de la estrategia brasileña y se estructuró en cuatro ejes temáticos: protección y concientización del ciudadano y de la sociedad; seguridad y resiliencia de servicios esenciales

e infraestructuras críticas; cooperación e integración entre órganos y entidades públicas y privadas; y soberanía nacional y gobernanza (Presidência da República do Brasil, 2025). La nueva estrategia también refuerza una preocupación central para Brasil, esto es, la necesidad de fortalecer la autonomía tecnológica y reducir dependencias externas en materia de ciberseguridad. En este sentido, el Gabinete de Seguridad Institucional destaca que la estrategia de 2025 busca promover la soberanía e independencia del país mediante el desarrollo tecnológico nacional, la estructuración de mecanismos de regulación, fiscalización, coordinación y control, la mejora de la protección de servicios esenciales e infraestructuras críticas, y la creación de un mecanismo nacional unificado de notificación de incidentes cibernéticos (Gabinete de Segurança Institucional, 2025).

En conjunto, el caso brasileño permite observar una modalidad de respuesta estatal distinta a la de los casos anteriores: Brasil no cuenta con el mismo poder tecnológico de EE. UU., ni con la capacidad de proyección normativa global que la UE, ni con el grado de control estatal característico del modelo chino. Sin embargo, su experiencia muestra cómo la ciberseguridad se volvió una preocupación estratégica también para países latinoamericanos que dependen de infraestructuras digitales globales, plataformas extranjeras y cadenas tecnológicas transnacionales. En la tabla 4 se recuperan los principales marcos regulatorios vinculados al espacio digital implementados por Brasil en el período postpandemia.

Tabla 4: Síntesis de los marcos regulatorios de Brasil relativos a la ciberseguridad (2020-2025)

Marco regulatorio	Objetivo	Año de adopción/aplicación
Ley General de Protección de Datos Personales	Proteger los derechos fundamentales de libertad, privacidad y libre desarrollo frente al tratamiento de datos personales.	2018/2020
Estrategia Nacional de Seguridad Cibernética	Orientar las acciones nacionales e internacionales de Brasil en materia de seguridad cibernética.	2020
Medida Provisional n.º 1.068	Limitar la moderación unilateral de contenidos por parte de las	2021

Marco regulatorio	Objetivo	Año de adopción/aplicación
	plataformas digitales, exigiendo mayores justificaciones para la remoción de publicaciones o suspensión de cuentas bajo el argumento de proteger la libertad de expresión.	
Decreto n.º 11.856	Orientar y coordinar la seguridad cibernética en Brasil, fortaleciendo la soberanía nacional, la protección de derechos, la resiliencia de infraestructuras críticas y la cooperación entre actores públicos y privados.	2023
Estrategia Nacional de Ciberseguridad	Fortalecer la protección ciudadana, la resiliencia de infraestructuras críticas, la cooperación público-privada y la soberanía digital.	2025

Fuente: Elaboración propia en base a las fuentes citadas en el presente apartado.

2.4. Gobernar un espacio sin fronteras: cooperación, fragmentación y límites de la gobernanza global

La expansión del poder digital y la multiplicación de amenazas cibernéticas pusieron en evidencia la necesidad de pensar la gobernanza del ciberespacio como un problema central de las Relaciones Internacionales contemporáneas. Esta cuestión se inscribe en la lógica anárquica del sistema internacional, entendida como la ausencia de una autoridad superior a los Estados capaz de regular de manera jerárquica y universal sus comportamientos (Waltz, 1979). No obstante, en el ciberespacio dicha ausencia de autoridad central adquiere una complejidad particular, debido a su carácter transnacional, descentralizado y técnicamente complejo, así como a la participación de actores no estatales con creciente capacidad de incidencia.

A diferencia de otros ámbitos regulados de forma más directa por los Estados, el entorno digital difícilmente puede ser delimitado mediante fronteras territoriales. Sus infraestructuras, flujos de datos y amenazas atraviesan múltiples jurisdicciones, lo que limita la eficacia de respuestas exclusivamente nacionales. En este sentido, Chang y Grabosky

(2026) advierten que, incluso cuando las leyes logran actualizarse frente a los avances tecnológicos, su eficacia continúa condicionada por arquitecturas digitales transfronterizas y por la necesidad de cooperación entre Estados.

Por ello, la gobernanza del ciberespacio no depende únicamente de normas estatales, sino de la interacción entre regulaciones nacionales, estándares técnicos, decisiones corporativas, acuerdos privados, instituciones internacionales, comunidades expertas y mecanismos de cooperación público-privada. En este marco, el carácter plural de la gobernanza del ciberespacio suele vincularse con el modelo *multistakeholder* o multiactor. Raymond y DeNardis definen el *multistakeholderism* como la participación de "dos o más clases de actores comprometidos en una empresa común de gobernanza sobre cuestiones que consideran de naturaleza pública" (Raymond y DeNardis, 2015, p. 573). Desde esta perspectiva, Estados, empresas, sociedad civil, comunidades técnicas y organismos internacionales pueden intervenir, con distintos grados de poder e influencia, en la definición de reglas y estándares digitales.

Sin embargo, este modelo no debe ser idealizado. Los autores advierten que la participación de múltiples actores no garantiza necesariamente una distribución equilibrada de la autoridad ni una representación igualitaria de intereses (Raymond y DeNardis, 2015). En la práctica, las asimetrías económicas, tecnológicas y políticas hacen que ciertos actores tengan mayor capacidad para incidir en la orientación de la gobernanza global. De este modo, la pluralidad de actores no elimina las relaciones de poder, sino que las reconfigura dentro de un entorno más descentralizado y fragmentado.

En este marco, Nye propone comprender la gobernanza del ciberespacio como un "complejo de regímenes". El autor sostiene que "si bien no existe un régimen único para la gobernanza del ciberespacio, existe un conjunto de normas e instituciones débilmente

acopladas" (Nye, 2014, p. 7). Esta perspectiva permite evitar la idea de que existe un único régimen internacional del ciberespacio y, en cambio, muestra que su gobernanza se organiza de manera fragmentada, a través de arreglos institucionales parciales, superpuestos y no siempre coherentes entre sí.

En relación con lo anterior, uno de los espacios más relevantes en el plano multilateral ha sido el Grupo de Trabajo de Composición Abierta sobre la Seguridad y el Uso de las Tecnologías de la Información y las Comunicaciones (2021-2025) de Naciones Unidas. Este grupo fue creado por la Asamblea General mediante la Resolución 75/240, adoptada el 31 de diciembre de 2020, con el propósito de continuar el tratamiento intergubernamental de las amenazas existentes y potenciales vinculadas al uso de las TIC. Su mandato incluye el desarrollo de reglas, normas y principios de comportamiento responsable de los Estados; el estudio de iniciativas estatales orientadas a garantizar la seguridad en el uso de las TIC; la aplicación del derecho internacional al ciberespacio; la adopción de medidas de cooperación; el fortalecimiento de medidas de fomento de la confianza; y la creación de capacidades, especialmente para reducir asimetrías entre Estados con distintos niveles de desarrollo tecnológico (Naciones Unidas, 2025).

No obstante, los debates en torno a su constitución reflejaron las divergencias persistentes entre modelos de gobernanza: mientras algunos Estados defienden una Internet abierta, interoperable, segura y basada en la cooperación multiactor, otros enfatizan la soberanía estatal, la seguridad nacional y el control sobre los flujos informativos. Estas diferencias no son meramente técnicas, sino políticas: expresan distintas concepciones sobre el alcance legítimo de la autoridad estatal en el entorno digital, el papel de las empresas tecnológicas, la protección de derechos en línea y la relación entre seguridad, libertad y control de la información.

Otro hito relevante fue la adopción del Pacto Digital Global, incorporado como anexo del Pacto para el Futuro, aprobado en la Cumbre del Futuro de Naciones Unidas el 22 de septiembre de 2024. Este instrumento constituye un marco político de cooperación digital que busca orientar la gobernanza de las tecnologías digitales y de la IA desde una perspectiva global. Su importancia radica en que reconoce que la transformación digital no puede ser abordada únicamente desde agendas nacionales o sectoriales, sino que requiere coordinación internacional en materia de conectividad, inclusión digital, derechos humanos en línea, seguridad digital, gobernanza de datos, responsabilidad de las empresas operadoras y desarrollo de capacidades. En ese sentido, el Pacto Digital Global expresa la incorporación definitiva de la cuestión digital dentro de las discusiones sobre reforma y actualización del multilateralismo contemporáneo (Naciones Unidas, 2024).

El Pacto Digital Global también permite observar que la gobernanza del ciberespacio excede el campo estricto de la ciberseguridad. Si bien la protección frente a amenazas digitales continúa siendo central, la agenda multilateral se amplía hacia problemas como la brecha digital, la inclusión tecnológica, la protección de datos, la gobernanza de la IA, la responsabilidad de las empresas operadoras y la necesidad de garantizar que las tecnologías digitales contribuyan al desarrollo sostenible.

En materia de ciberdelito y cooperación judicial, también se produjeron avances significativos. Un instrumento clave es el Segundo Protocolo Adicional al Convenio de Budapest sobre Ciberdelincuencia, abierto a la firma el 12 de mayo de 2022. Este protocolo fue diseñado para responder a uno de los principales problemas de la persecución penal del cibercrimen: la dificultad de obtener evidencia electrónica cuando esta se encuentra almacenada en jurisdicciones extranjeras, múltiples, cambiantes o incluso desconocidas. Mientras el cibercrimen se expande y la evidencia digital se vuelve cada vez más transnacional, las facultades tradicionales de investigación continúan estando limitadas por

fronteras territoriales. En este sentido, el Protocolo busca enfrentar esa dificultad mediante herramientas de cooperación reforzada y divulgación de evidencia electrónica (Consejo de Europa, 2022). Este tipo de instrumentos muestra cómo la gobernanza global del ciberespacio requiere articular capacidades estatales con la colaboración de intermediarios privados.

A nivel universal, el avance más importante fue la Convención de Naciones Unidas contra la Ciberdelincuencia, adoptada por la Asamblea General el 24 de diciembre de 2024 mediante la Resolución 79/243. La Convención constituye el primer tratado global integral en esta materia y busca proporcionar a los Estados un conjunto de herramientas para prevenir y combatir la ciberdelincuencia, así como fortalecer la cooperación internacional para el intercambio de evidencia electrónica en delitos graves (Naciones Unidas, 2024).

La Convención fue abierta a la firma el 25 de octubre de 2025 en Hanoi, Vietnam, y permanecerá abierta a la firma en la sede de Naciones Unidas en Nueva York hasta el 31 de diciembre de 2026. De acuerdo con su artículo 65, entrará en vigor noventa días después del depósito del cuadragésimo instrumento de ratificación, aceptación, aprobación o adhesión. Su eficacia, entonces, dependerá de la ratificación, implementación y cooperación efectiva de los Estados parte. Desde el punto de vista sustantivo, la Convención procura armonizar ciertos aspectos de la criminalización, establecer medidas procesales, fortalecer la cooperación internacional, promover asistencia técnica y facilitar el intercambio de información (Naciones Unidas, 2024).

En conjunto, estos espacios multilaterales y acuerdos internacionales muestran que la gobernanza global del ciberespacio se encuentra en construcción. Si bien existe una arquitectura institucional global orientada a abordar los desafíos del entorno digital —integrada por organismos multilaterales, foros de diálogo, acuerdos internacionales, iniciativas técnicas y mecanismos de cooperación—, esta continúa caracterizándose por la

fragmentación normativa y por el predominio de instrumentos de *soft law*, tales como principios, recomendaciones, estándares voluntarios y compromisos políticos no vinculantes. Esta situación refleja las dificultades para construir consensos fuertes en un campo atravesado por intereses divergentes entre grandes potencias, diferencias sobre el alcance de la soberanía estatal, tensiones entre seguridad y derechos, y disputas en torno al papel de las empresas tecnológicas en el tablero político internacional.

Capítulo 3: La soberanía digital puesta a prueba: los casos de TikTok en EE. UU. y X en Brasil

Los capítulos anteriores permitieron observar cómo la digitalización transformó las formas tradicionales de poder, desplazando parte de la autoridad hacia actores privados capaces de controlar datos, infraestructuras, algoritmos y espacios centrales de comunicación pública. A su vez, se mostró que la pandemia aceleró la dependencia digital y reforzó la preocupación de los Estados por la ciberseguridad, la regulación de plataformas y la protección de capacidades soberanas. En ese marco, la soberanía digital aparece como una dimensión cada vez más relevante de la política internacional contemporánea, en tanto expresa la disputa por definir quién controla, regula y gobierna los procesos que estructuran la vida social en el ciberespacio.

Este capítulo analiza dos casos recientes que permiten observar esas tensiones en la práctica: el conflicto entre EE. UU. y TikTok, y el enfrentamiento entre Brasil y X. El primero muestra cómo una aplicación de entretenimiento puede ser reinterpretada como un recurso estratégico en el marco de la rivalidad geopolítica entre EE. UU. y China. El segundo permite analizar la capacidad de un Estado para exigir el cumplimiento de decisiones judiciales a una compañía transnacional que interviene directamente en el debate público. En conjunto, ambos casos muestran que la soberanía digital no se limita al control técnico de datos o redes, sino que involucra también seguridad nacional, libertad de expresión, gobernanza democrática y poder privado transnacional.

3.1. EE. UU. vs. TikTok: la disputa por una plataforma estratégica

3.1.1. Del crecimiento de TikTok a la presión por la desinversión

El conflicto entre EE. UU. y TikTok no debe comprenderse únicamente como una controversia sobre una aplicación de entretenimiento o sobre la protección de datos personales. Su desarrollo expresa una disputa más amplia por el control de las infraestructuras digitales, algoritmos de recomendación, datos masivos y canales de circulación de información. Las preocupaciones de EE. UU. no surgieron en el vacío, sino en un contexto de creciente rivalidad estratégica con China, donde la competencia tecnológica, el control de datos y la influencia sobre infraestructuras digitales comenzaron a ser interpretados como dimensiones centrales de la seguridad nacional. En este sentido, TikTok se transformó en un caso paradigmático porque combinó tres dimensiones sensibles para Washington: la propiedad extranjera de una aplicación utilizada por millones de ciudadanos estadounidenses, la posibilidad de acceso a datos personales por parte de un Estado rival, y el temor a que el algoritmo de recomendación pudiera incidir sobre el entorno informativo interno.

TikTok surgió como la versión internacional de Douyin, aplicación de videos cortos lanzada por ByteDance en la República Popular China (RPC o China) en 2016. Dos años después, ByteDance adquirió musical.ly, una aplicación de origen chino que operaba principalmente en EE. UU., y la relanzó bajo la marca TikTok. A partir de esa operación, migró a sus usuarios hacia la nueva plataforma y aceleró su expansión en el mercado estadounidense. Desde entonces, TikTok se convirtió en una de las redes sociales más populares en los EE. UU., apoyándose en un formato de videos breves y un sofisticado algoritmo de recomendación de contenidos (Sutherland et al., 2025). Gracias a esto, la plataforma no solo permite crear y compartir videos, sino que selecciona contenidos para

cada usuario a partir de interacciones, metadatos y configuraciones de cuenta y dispositivo, lo que convierte al algoritmo en una pieza central de su atractivo y de su valor económico.

Este crecimiento adquirió relevancia geopolítica en tanto que TikTok pasó a ser una de las primeras plataformas no estadounidenses capaces de desafiar de manera significativa a las grandes empresas de Silicon Valley, en un mercado global históricamente dominado por plataformas estadounidenses (Facebook, Instagram, YouTube, X, entre otras) (Gray, 2021).

A medida que TikTok aumentó su presencia en el país norteamericano, principalmente durante los años de la pandemia, también crecieron inquietudes políticas y regulatorias sobre su estructura societaria. La plataforma es operada por TikTok Ltd., subsidiaria de ByteDance Ltd., empresa incorporada en las Islas Caimán, pero con operaciones centrales y liderazgo ubicados en China (Sutherland et al., 2025). Esta arquitectura empresarial resultó especialmente problemática para las autoridades estadounidenses porque separaba formalmente la titularidad jurídica de la plataforma de su inserción operativa en el ecosistema chino. Es decir, aunque TikTok se presentaba como una empresa global con sedes en Los Ángeles y Singapur, su casa matriz mantenía una relación estructural con la RPC. De esta manera, ByteDance se encuentra bajo un marco legal que puede exigirle “asistencia” al gobierno chino, incluso mediante la entrega de datos de usuarios (Insisa, 2025). Desde esta perspectiva, el riesgo no consistía únicamente en que TikTok recolectara datos, sino en que esos datos pudieran quedar indirectamente expuestos a una potencia rival. Por eso, para los legisladores y funcionarios estadounidenses, la cuestión central era si ByteDance podía garantizar que la información de los usuarios estadounidenses permaneciera separada de Beijing.

TikTok negó reiteradamente esas acusaciones y afirmó que nunca ha compartido, ni recibido una petición para compartir datos de usuarios estadounidenses con el gobierno chino

(Sutherland et al., 2025). Juned et al. (2023) subraya que no existía evidencia concreta de que TikTok hubiera entregado datos de usuarios estadounidenses al gobierno chino. Sin embargo, para Washington, la discusión se vinculaba menos con la prueba de una transferencia efectiva de datos y más con la posibilidad de que dicha transferencia pudiera ocurrir.

El primer gran momento institucional del conflicto se produjo en 2019, cuando el Comité de Inversión Extranjera en EE. UU. (CFIUS, por sus siglas en inglés)[1] inició una revisión retroactiva de la adquisición de musical.ly por parte de ByteDance. La operación no había sido sometida originalmente al análisis de CFIUS, a pesar de que implicaba la adquisición de una aplicación con presencia relevante en el mercado estadounidense y con capacidad de recolectar datos personales de usuarios estadounidenses (Sutherland et al., 2025). En paralelo, comenzaron a aparecer restricciones sectoriales: a fines de 2019 y comienzos de 2020, distintas ramas de las Fuerzas Armadas estadounidenses prohibieron el uso de TikTok en dispositivos oficiales por motivos de seguridad (The Editors of ProCon, 2026).

La disputa escaló durante la administración de Donald Trump quien, en agosto de 2020, emitió la Orden Ejecutiva 13942, invocando la Ley de Poderes Económicos de Emergencia Internacional (IEEPA, por sus siglas en inglés)[2] para prohibir ciertas transacciones vinculadas con TikTok y avanzar hacia una restricción de la aplicación en el país. La justificación de la medida combinó dos argumentos: la protección de datos personales y la manipulación de la información (Horowitz y Check, 2022).

---

[1] CFIUS es un comité interagencial presidido por el Departamento del Tesoro que evalúa si determinadas inversiones extranjeras pueden afectar la seguridad nacional estadounidense.

[2] IEEPA es una herramienta legal que otorga al presidente amplias facultades para restringir transacciones económicas luego de declarar una emergencia nacional.

De esta manera, la estrategia de Trump combinó dos caminos: por un lado, el uso de IEEPA para restringir transacciones; por el otro, la vía de CFIUS para presionar una desinversión.

Sin embargo, el intento de prohibición encontró límites judiciales. TikTok y ByteDance recurrieron a los tribunales, y la Corte del Distrito de Columbia suspendió las restricciones impulsadas por la administración Trump. El problema jurídico principal era si IEEPA podía utilizarse para restringir una plataforma cuyo funcionamiento involucraba comunicaciones personales y materiales informativos (Horowitz y Check, 2022). Esas excepciones legales limitaron la posibilidad de aplicar IEEPA al caso y mostraron que una norma diseñada antes de la economía digital no ofrecía una respuesta clara frente a los riesgos asociados con flujos transfronterizos de datos.

Con el cambio de administración, el enfoque se modificó parcialmente. En junio de 2021, el presidente Joe Biden revocó la orden ejecutiva de Trump y la reemplazó por la Orden Ejecutiva 14034. Como se mencionó en el capítulo 2, esta medida, a diferencia de la anterior, no se concentró exclusivamente en TikTok, sino que buscó evaluar de manera más general los riesgos de seguridad nacional vinculados con aplicaciones controladas por entidades sujetas a países considerados “adversarios extranjeros” (Sutherland et al., 2025). Así, Biden abandonó el formato de prohibición inmediata, pero mantuvo la preocupación por el acceso extranjero a datos estadounidenses.

En ese marco surgió el denominado Proyecto Texas, presentado por TikTok en enero de 2023 como una estrategia de mitigación para responder a las preocupaciones de seguridad nacional planteadas por el gobierno estadounidense. Su nombre aludía a Oracle, empresa tecnológica con sede en Texas, que ocuparía un rol central en el almacenamiento y supervisión de datos. El objetivo principal del proyecto era la localización de los datos

generados por usuarios estadounidenses y el monitoreo de los flujos transfronterizos de información por una nueva subsidiaria ubicada en EE. UU: TikTok U.S. Data Security (Sutherland et al., 2025).

TikTok afirmó que, desde julio de 2022, todos los nuevos datos de usuarios estadounidenses se almacenaban automáticamente en la infraestructura de Oracle en EE. UU., aunque algunos expertos y legisladores sostuvieron que la localización de datos no resolvía por completo el problema del acceso de empleados de ByteDance a información de usuarios estadounidenses (Sutherland et al., 2025). Por ello, Proyecto Texas funcionó como una solución parcial, aunque no logró cerrar definitivamente la disputa política y regulatoria.

Durante 2022 y 2023, el conflicto se desplazó progresivamente hacia el Congreso y otras agencias estatales. En 2022, el Congreso aprobó una disposición dentro de la Ley de Asignaciones Consolidadas que ordenaba a la Oficina de Gestión y Presupuesto (OMB, por sus siglas en inglés) establecer estándares y directrices para remover TikTok de dispositivos y sistemas informáticos del gobierno federal, publicadas finalmente en febrero de 2023 (Sutherland et al., 2025). Ese mismo año, las preocupaciones se intensificaron tras reportes sobre investigaciones del FBI y el Departamento de Justicia respecto del presunto acceso indebido de empleados de TikTok a datos de periodistas estadounidenses (The Editors of ProCon, 2026). A partir de entonces, el debate dejó de girar exclusivamente en torno al almacenamiento de datos y pasó a incluir con más fuerza la posibilidad de vigilancia, influencia política y manipulación informativa.

El punto de inflexión legislativo llegó en abril de 2024, cuando el Congreso aprobó la Ley de Protección de los Estadounidenses frente a Aplicaciones Controladas por Adversarios Extranjeros (PAFACAA, por sus siglas en inglés). La misma definió expresamente a TikTok y a las aplicaciones operadas por ByteDance como “aplicaciones controladas por un

adversario extranjero", y prohibió que tiendas de aplicaciones y servicios de alojamiento en internet permitieran su distribución, mantenimiento o actualización en EE. UU. salvo que sus propietarios ejecutaran una "desinversión calificada" dentro del plazo previsto (Sutherland et al., 2025). En términos prácticos, la norma no obligaba directamente a ByteDance a vender TikTok bajo amenaza de una sanción inmediata, pero sí colocaba a la plataforma en una posición difícil: desprenderse de su control chino o perder el soporte necesario para operar en el mercado estadounidense (Grimmelmann, 2025).

TikTok y ByteDance respondieron judicialmente. En mayo de 2024 presentaron una demanda ante la Corte de Apelaciones del Distrito de Columbia, argumentando que la ley violaba la Primera Enmienda[3], así como otras garantías constitucionales. También usuarios y organizaciones que publicaban contenidos en TikTok presentaron impugnaciones, alegando que la restricción afectaba su libertad de expresión y su capacidad de comunicarse mediante la plataforma. En diciembre de 2024, la Corte de Apelaciones rechazó los planteos constitucionales y sostuvo la validez de la norma, lo que llevó a los demandantes a acudir rápidamente ante la Corte Suprema (Grimmelmann, 2025).

El 17 de enero de 2025, la Corte Suprema confirmó la decisión de la instancia anterior y concluyó que, en su aplicación al caso, las disposiciones impugnadas de PAFACAA no violaban los derechos de la Primera Enmienda de TikTok, ByteDance ni sus usuarios (Sutherland et al., 2025). La decisión fue relevante en tanto permitió que el argumento de seguridad nacional prevaleciera frente a una objeción basada en libertad de expresión.

Con la entrada en vigor de la ley el 19 de enero de 2025, TikTok y otras aplicaciones relacionadas dejaron de estar disponibles temporalmente para usuarios estadounidenses. Sin

[3] La Primera Enmienda de la Constitución de los EE. UU. prohíbe al Congreso crear leyes que establezcan una religión oficial o interfieran con su práctica, y protege la libertad de expresión, la libertad de prensa, el derecho a la reunión pacífica y el derecho a solicitar al gobierno la reparación de agravios.

embargo, la interrupción fue breve. 24 horas después, ya iniciado su nuevo mandato, Donald Trump firmó la Orden Ejecutiva 14166, instruyendo al fiscal general a no ejecutar la ley durante 75 días, con el argumento de permitir que su administración definiera una salida ordenada que protegiera la seguridad nacional sin provocar el cierre abrupto de una aplicación de entretenimiento utilizada por millones de estadounidenses (Sutherland et al., 2025). Esta decisión mantuvo a TikTok operativa mientras continuaban las negociaciones sobre una posible estructura de propiedad aceptable para Washington.

El cambio de postura de Trump frente a TikTok no implicó necesariamente el abandono de las preocupaciones de seguridad nacional, sino una reformulación de la estrategia para abordarlas. Mientras que en su primera administración predominó una lógica de prohibición y presión directa sobre ByteDance, en su segundo mandato Trump adoptó una posición más pragmática, orientada a evitar el cierre de una plataforma que había adquirido valor político interno durante la campaña presidencial de 2024. En efecto, la red social se había convertido en un canal relevante para llegar a votantes jóvenes y para disputar la comunicación electoral. De este modo, el objetivo dejó de ser simplemente excluir a TikTok del mercado estadounidense y pasó a ser reconfigurar sus condiciones de operación en el país.

La aplicación de la ley fue postergada en varias oportunidades hasta que, en enero de 2026, se anunció el cierre de un acuerdo para separar la aplicación estadounidense de TikTok de su negocio global[4]. Según el esquema informado, una nueva entidad, TikTok USDS Joint Venture LLC, sería responsable de proteger los datos, las aplicaciones y los algoritmos correspondientes al mercado estadounidense mediante medidas de privacidad y

[4] Si bien la delimitación temporal de este trabajo comprende el período 2020-2025, se incorpora de manera excepcional este acontecimiento ocurrido en enero de 2026 debido a su relevancia para comprender la evolución y el desarrollo posterior del conflicto entre EE. UU. y TikTok. Su inclusión no modifica el recorte temporal establecido, sino que responde únicamente a fines explicativos y analíticos.

ciberseguridad. La nueva empresa operaría con una junta directiva de siete miembros de mayoría estadounidense; Oracle, Silver Lake y MGX participarían como inversores principales, cada uno con una participación del 15 por ciento, mientras que ByteDance conservaría el 19,9 por ciento del negocio. Oracle, además, quedaría a cargo de asegurar los datos de los usuarios estadounidenses y supervisar el reentrenamiento del algoritmo de recomendación, que pasaría a entrenarse únicamente con datos de usuarios de EE. UU. (Tewari y Jamali, 2026).

3.1.2. Lo que revela el caso TikTok

La reconstrucción cronológica del caso permite observar que el conflicto entre EE. UU. y TikTok no se redujo a una controversia puntual sobre privacidad de datos ni a una discusión aislada sobre una red social extranjera. A medida que el caso avanzó, TikTok dejó de ser tratada como una simple aplicación de entretenimiento para ser considerada una infraestructura digital con implicancias estratégicas. Esta transformación se explica por la combinación de cuatro elementos: su escala masiva de usuarios, su capacidad de recolectar y procesar datos, la centralidad de su algoritmo de recomendación y su vínculo societario con ByteDance, empresa sometida al marco jurídico y político chino. En ese cruce, una red social asociada al ocio, a la creatividad y al consumo cultural que tomó fuerza entre los jóvenes durante los tiempos del COVID-19, se convirtió en un problema de seguridad nacional.

El punto central no fue únicamente que TikTok recolectara datos personales —práctica común para las aplicaciones digitales—, sino quién podía acceder a ellos, bajo qué condiciones y con qué fines. Como se desarrolló en el capítulo 1, las plataformas digitales ocupan un lugar protagónico en el proceso de datificación contemporáneo: organizan interacciones, concentran información y extraen valor de la actividad cotidiana de los

usuarios. En el caso de TikTok, esa lógica adquirió una dimensión especialmente sensible porque la plataforma operaba sobre una base masiva de usuarios estadounidenses, pero bajo una estructura de propiedad que Washington consideraba vulnerable a la presión de Beijing.

La dimensión geopolítica resulta indispensable para comprender por qué el caso adquirió tanta relevancia. La disputa geopolítica entre EE. UU. y China no se limita al comercio o al poder militar, sino que incluye una competencia más amplia por moldear el futuro tecnológico global. Para Washington, resolver el caso no implicaba solo regular una aplicación extranjera, sino evitar que una infraestructura digital de enorme alcance quedara vinculada a un competidor estratégico.

En este marco, TikTok condensó dos temores principales. Por un lado, el temor a que China pudiera acceder, directa o indirectamente, a datos de ciudadanos estadounidenses a través de una empresa privada. Por otro, el temor a que una plataforma sometida a influencia china pudiera intervenir sobre los flujos de información dentro del propio espacio público estadounidense. Esta doble preocupación explica por qué las soluciones parciales, como Project Texas, no lograron cerrar el conflicto. La localización de datos en servidores estadounidenses podía responder al problema del almacenamiento, pero no resolvía plenamente la cuestión del control corporativo, del acceso operativo ni de la administración del algoritmo. La aprobación de PAFACAA mostró que el diagnóstico estatal había cambiado: ya no bastaba con mitigar riesgos técnicos, sino que era necesario modificar la estructura de propiedad y control de la plataforma.

La respuesta estadounidense puede interpretarse, entonces, como un acto de defensa de soberanía digital. El gobierno de EE. UU. buscó recuperar su autoridad en el ciberespacio frente a una plataforma global que operaba dentro de su territorio, pero cuya empresa matriz estaba vinculada a una potencia rival. Esta reacción se vincula con lo desarrollado en el

capítulo 2, donde se señaló que, tras la pandemia, la ciberseguridad pasó a ocupar un lugar central en la agenda estatal, no solo como protección frente a ataques informáticos, sino también como resguardo de datos, infraestructuras críticas y capacidades soberanas.

Al mismo tiempo, el conflicto dejó planteada una tensión normativa difícil de resolver. TikTok y sus usuarios presentaron la ley como una vulneración de la libertad de expresión, mientras que el gobierno estadounidense la justificó por razones de seguridad nacional. Esta tensión muestra que la regulación de plataformas no es un asunto meramente técnico o económico: involucra derechos fundamentales, intereses estatales y el poder de actores privados que administran espacios clave de comunicación pública.

De esta manera, la pregunta de fondo ya no es solo quién puede operar una plataforma, sino quién controla los datos que produce, quién define los criterios algorítmicos de visibilidad y bajo qué autoridad jurídica se gobiernan esos procesos.

3.2. Brasil vs. X: el límite entre libertad de expresión y autoridad estatal

3.2.1. De la desinformación electoral al bloqueo de la plataforma

El conflicto entre Brasil y X debe situarse en una tensión más amplia entre la capacidad regulatoria de los Estados nacionales y el creciente poder de las *Big Tech*. Este enfrentamiento se vincula principalmente con el cumplimiento de decisiones judiciales, la desinformación política, la representación legal local, la libertad de expresión y la autoridad del Estado para hacer cumplir sus normas dentro del territorio nacional.

El caso brasileño no comenzó de manera repentina en 2024. Sus antecedentes se remontan al lugar que ocuparon las redes sociales en la política brasileña durante la pandemia de COVID-19, la disputa electoral de 2022 y los ataques a las instituciones democráticas del

8 de enero de 2023. Estos acontecimientos demostraron que las plataformas no funcionaron únicamente como canales de comunicación entre usuarios, sino también como espacios de disputa política.

En 2020, la circulación de información falsa o engañosa sobre el COVID-19 colocó a las plataformas digitales en el centro del debate público. El entonces presidente brasileño, Jair Bolsonaro, cuestionó públicamente la gravedad del virus, promovió tratamientos no aprobados, como la hidroxicloroquina, y desalentó el uso de mascarillas y la vacunación. En ese contexto, Twitter[5] intervino sobre algunas publicaciones, etiquetando o limitando contenidos que, según sus propias reglas, podían resultar dañinos para la salud pública. Esta intervención abrió un primer debate sobre la capacidad de un actor privado para moderar el discurso de un jefe de Estado y, al mismo tiempo, sobre si esa moderación protegía el acceso a información veraz o constituía una restricción indebida a la libertad de expresión. En consecuencia, en 2021, el presidente firmó la Medida Provisional N.º 1.068, orientada a limitar la capacidad de las plataformas digitales para eliminar contenidos de manera unilateral (Schtivelband Guindi, 2025).

Durante la campaña presidencial de 2022, la disputa por la información digital se volvió todavía más intensa. Las redes sociales se convirtieron en espacios centrales para la circulación de noticias falsas, teorías conspirativas y discursos violentos. El triunfo de Lula da Silva en 2022 no cerró esa disputa, sino que la profundizó. El 8 de enero de 2023, miles de simpatizantes de Bolsonaro atacaron las sedes de los tres poderes del Estado en Brasilia. Este episodio hizo que la controversia escalara en tensiones sociales, judiciales y mediáticas, y superara el conflicto inicial entre la red social y las autoridades electorales (Ortega, 2024).

[5] Twitter cambió oficialmente su nombre y logotipo a X el 23 de julio de 2023, bajo la dirección de Elon Musk, quien adquirió la plataforma el 27 de octubre de 2022.

En este punto adquirió centralidad el término “milicias digitales”, utilizado para describir redes organizadas de usuarios, cuentas y *bots* vinculadas a la difusión de desinformación, ataques a instituciones y promoción de narrativas antidemocráticas (Schtivelband Guindi, 2025). En la misma línea, Rodrigues Brancher (2024) explica que las investigaciones judiciales se relacionaban con la posible comisión de delitos de obstrucción de investigaciones de organización criminal e incitación al delito, en el marco de pesquisas sobre milicias digitales y ataques al Congreso Nacional, al Supremo Tribunal Federal y al Palacio del Planalto.

A partir de esos antecedentes, el juez Alexandre de Moraes, integrante del Supremo Tribunal Federal (STF) y también autoridad relevante en el Tribunal Superior Electoral (TSE), asumió un papel clave en la respuesta judicial frente a la desinformación. Moraes ya había asumido la responsabilidad de supervisar las investigaciones sobre desinformación desde 2020 y, en el marco del STF y el TSE, ordenó a X eliminar perfiles y publicaciones que, según su criterio, atentaban contra la legitimidad de las instituciones del país (Ortega, 2024). La cuestión central pasó a ser, entonces, si una empresa transnacional podía negarse a cumplir órdenes judiciales nacionales alegando defensa de la libertad de expresión.

En abril de 2024, el conflicto entró en una nueva etapa. Se difundieron los llamados “Twitter Files Brazil”. Estos documentos internos mostraron roces previos entre la dicha aplicación y el sistema judicial brasileño, y funcionaron como punto de partida para que Elon Musk iniciara una ofensiva pública contra Moraes. Musk acusó al juez de censura y abuso de poder, personalizando el conflicto. El empresario llegó a calificar a Moraes como un “dictador malvado disfrazado de juez” (Ortega, 2024). Esa retórica transformó la controversia jurídica en una disputa pública y política entre el titular de una plataforma global y un juez de la Corte Suprema brasileña. En los meses siguientes, la tensión se profundizó por el

incumplimiento de órdenes judiciales: la empresa estadounidense se negó a suspender determinadas cuentas que, para las autoridades brasileñas, estaban vinculadas con desinformación, discursos de odio y ataques contra el Estado de derecho.

La confrontación escaló cuando X Corp. retiró su oficina de representación en Brasil, luego de que Moraes amenazara con arrestos por el incumplimiento de sus órdenes (Nicas y Conger, 2024). Esta decisión tuvo consecuencias jurídicas directas, ya que el derecho brasileño exige que las empresas extranjeras designen un representante legal en Brasil para poder operar legalmente. El objetivo de esa exigencia es asegurar que la sociedad extranjera pudiera ser fiscalizada y controlada por el poder público, evitando que opere en condiciones privilegiadas frente a otras empresas (Rodrigues Brancher, 2024). Desde esta perspectiva, la falta de representante legal impedía a la firma actuar dentro del orden jurídico brasileño y abría la posibilidad de sanciones severas, incluida la suspensión de actividades.

Sin embargo, esta exigencia también generó cuestionamientos. Para Rodrigues Brancher (2024), la medida puede producir inseguridad jurídica para empresas extranjeras que no tienen una presencia física en Brasil, pero que ofrecen servicios en el país. Según el autor, no existe una previsión normativa clara que obligue a toda empresa extranjera que opera plataformas digitales a nombrar un representante legal en Brasil si no está formalmente constituida en territorio nacional. Esta observación no niega la relevancia del conflicto ni la necesidad de garantizar el cumplimiento de órdenes judiciales, pero introduce una discusión sobre los límites jurídicos de la respuesta estatal.

La situación llegó a su punto crítico el 28 de agosto de 2024, cuando X recibió una orden judicial para designar un representante legal en Brasil en un plazo de 24 horas. La empresa no cumplió con la intimación y, el 30 de agosto, Moraes ordenó bloquear el acceso a la plataforma en todo el país (Machado Neto, 2025). La orden de bloqueo tuvo una fuerte

fundamentación política e institucional. En su decisión, Moraes afirmó que Musk permitía la propagación masiva de desinformación, discursos de odio e incitación a actos antidemocráticos (Nicas y Conger, 2024).

La medida vino acompañada de sanciones económicas y tecnológicas. En primer lugar, Moraes ordenó el congelamiento de las finanzas de Starlink, empresa de internet satelital de SpaceX, para intentar cobrar alrededor de tres millones de dólares en multas impuestas a X (Nicas y Conger, 2024). Esta decisión se apoyó en el reconocimiento de la existencia de un "grupo económico de hecho" entre X Brasil, Starlink Brazil Holding y Starlink Brazil Servicios de Internet, todas vinculadas a SpaceX y controladas por Elon Musk (Rodrigues Brancher, 2024). En segundo lugar, Moraes ordenó notificar a empresas como Apple y Google para que eliminaran la aplicación X de sus tiendas digitales e implementaran obstáculos tecnológicos para impedir su uso.

No obstante, el aspecto más controversial de la decisión no se vinculó necesariamente con el bloqueo general de la aplicación, sino con la decisión de imponer multas de hasta nueve mil dólares diarios a usuarios que intentaran evadir el bloqueo mediante "subterfugios tecnológicos" como redes privadas virtuales (VPN, por sus siglas en inglés) (Schtivelband Guindi, 2025). En este sentido, Schtivelband Guindi (2025) considera que esa disposición resultaba desproporcionada en tanto trasladaba el foco del incumplimiento desde la empresa hacia los usuarios, quienes podían recibir una sanción sin haber participado previamente en el proceso.

El bloqueo produjo consecuencias inmediatas en el ecosistema digital brasileño. Acurio Del Pino (2024) afirma que la suspensión de X tuvo un impacto multifacético en la libertad de expresión, generó debate sobre los límites de ese derecho, provocó protestas y afectó la comunicación y el diálogo público. Este punto es importante porque muestra la

tensión inherente al caso: la medida buscaba hacer cumplir decisiones judiciales y proteger el orden democrático, al tiempo que restringía temporalmente el acceso a una plataforma central para la expresión pública.

El debate se organizó, entonces, alrededor de dos posiciones. Para Musk y sus seguidores, la suspensión de X era un acto de censura incompatible con la libertad de expresión. Para Moraes y los defensores de la medida, en cambio, la compañía no debía considerarse inmune al orden jurídico nacional. Ortega (2024) sintetiza esa postura al recordar que Moraes sostuvo que las redes sociales no son "un territorio sin ley" y que deben operar dentro de las normativas locales.

Durante septiembre de 2024, comenzaron negociaciones para resolver el conflicto. Según Schtivelband Guindi (2025), el gobierno brasileño mantuvo una postura firme, exigiendo tres condiciones: la designación de un representante legal en el país, el pago de multas y el bloqueo de una lista de cuentas ilícitas. X, que inicialmente había resistido las órdenes judiciales, empezó a retroceder. En efecto, hacia fines de septiembre, X Corp. nombró a Raquel de Oliveira Conceição como representante legal en Brasil, lo que constituyó un movimiento clave para recomponer la situación jurídica de la plataforma (Machado Neto, 2025).

La regularización se completó con el pago de multas y el cumplimiento de órdenes de bloqueo de cuentas. A partir de ello, el gobierno brasileño autorizó la reactivación de la plataforma, aunque advirtió que X seguiría bajo vigilancia y que nuevos incumplimientos podían generar sanciones adicionales.

3.2.2. Lo que revela el caso X

El caso X permite observar una dimensión distinta de la soberanía digital. A diferencia del conflicto entre EE. UU. y TikTok, aquí el eje no estuvo puesto en la propiedad extranjera de una plataforma asociada a una potencia rival, sino en la capacidad del Estado para hacer cumplir sus decisiones frente a una empresa tecnológica transnacional. El problema central no fue quién controlaba los datos o el algoritmo, sino quién tenía autoridad para fijar las reglas de funcionamiento de una plataforma que intervenía directamente en el debate público brasileño.

X no funcionaba únicamente como una red social privada, sino como un espacio relevante para la comunicación política, la circulación de información y la disputa pública. En este marco, el caso permite observar cómo la acción política contenciosa se transformó en el entorno digital: las TIC facilitan la difusión de información a gran escala y en tiempo real, a la vez que permiten la articulación y coordinación de actos masivos en espacios tanto físicos como digitales (Ortega, 2024).

Este punto conecta con lo trabajado en el capítulo 1 respecto del poder de las *Big Tech*. X no actúa como un intermediario neutral: establece reglas de uso, modera contenidos, decide qué cuentas permanecen activas y organiza, mediante sus propios criterios técnicos y corporativos, parte de la visibilidad del debate público. Schtivelband Guindi (2025) sostiene que estas corporaciones han transgredido jurisdicciones nacionales y desplazado el debate sobre la libertad de expresión hacia la pregunta por cómo garantizar ese derecho en los nuevos soportes digitales. En el caso brasileño, esta tensión se volvió explícita: una empresa privada invocó la libertad de expresión para resistir decisiones judiciales, mientras el Estado sostuvo que ninguna plataforma podía funcionar como un espacio ajeno al orden jurídico nacional.

Desde una perspectiva de soberanía digital, el bloqueo de X puede interpretarse como un intento del Estado brasileño de afirmar su autoridad sobre una compañía transnacional. Desde este enfoque, Machado Neto (2025) ubica el caso dentro de un debate global sobre los enfrentamientos entre empresas tecnológicas y gobiernos, y sobre los intentos estatales de controlar flujos de datos, combatir *fake news* y enfrentar procesos de desinformación capaces de afectar elecciones e instituciones nacionales. En este sentido, la controversia no se limitó a una disputa entre un juez y un empresario, sino que expresó una tensión más amplia entre poder privado transnacional, regulación estatal y gobernanza democrática del espacio digital.

La exigencia de un representante legal en Brasil fue, en este contexto, mucho más que una cuestión administrativa. Sin una representación local, la capacidad estatal para notificar, responsabilizar y sancionar a la empresa quedaba debilitada. La suspensión de X funcionó, entonces, como una medida extrema para forzar el cumplimiento de decisiones judiciales y reafirmar la obligación de responder ante las normas locales.

Sin embargo, el caso no admite una lectura lineal. Acurio Del Pino (2024) señala que el bloqueo de la aplicación tuvo impacto sobre la libertad de expresión y reabrió el debate sobre los límites de la regulación estatal. Esta tensión se volvió especialmente visible en la discusión sobre las multas a usuarios que intentaran acceder mediante VPN: a diferencia de las sanciones dirigidas a la empresa, esa medida trasladaba parte del costo del conflicto hacia los usuarios, aun cuando estos no habían sido parte del proceso judicial. Por ello, Schtivelband Guindi (2025) considera que ese aspecto resultaba problemático desde el punto de vista de la proporcionalidad.

El conflicto también dialoga con el capítulo 2, donde se analizó cómo la pandemia aceleró la dependencia digital y llevó a los Estados a fortalecer sus marcos regulatorios. Brasil aparece aquí como un caso relevante del Sur global: no actúa como potencia

tecnológica dominante, pero intenta preservar márgenes de autoridad frente a empresas extranjeras que administran espacios centrales de comunicación pública. En ausencia de reglas globales vinculantes, la respuesta brasileña fue nacional y judicial: exigir representación local, cumplimiento de órdenes, pago de multas y remoción de cuentas investigadas.

En síntesis, el caso Brasil-X revela uno de los principales desafíos de la gobernanza digital contemporánea: equilibrar autoridad estatal, poder privado transnacional, libertad de expresión y protección del orden democrático. Su relevancia no radica únicamente en el bloqueo de una plataforma, sino en la pregunta más amplia que deja planteada: bajo qué condiciones puede un Estado exigir responsabilidad a una empresa global sin afectar de manera desproporcionada los derechos fundamentales que busca proteger.

3.3. Cierre comparativo: dos casos, una misma disputa por la autoridad digital

La comparación entre los casos de EE. UU. frente a TikTok y Brasil frente a X permite observar dos formas distintas de una misma tensión: el intento de los Estados por recuperar capacidad de control frente al poder creciente del sector tecnológico internacional. En el primer caso, la preocupación estuvo vinculada principalmente con la seguridad nacional, la rivalidad geopolítica con China, el control de datos personales, la propiedad extranjera y la posible influencia algorítmica sobre el entorno informativo estadounidense. En el segundo, el eje estuvo puesto en el cumplimiento de decisiones judiciales, la representación legal local, la desinformación política y los límites entre libertad de expresión y autoridad estatal.

A pesar de esas diferencias, ambos casos muestran que las plataformas digitales ya no pueden ser comprendidas únicamente como proveedoras de servicios tecnológicos. TikTok y X funcionan como espacios de comunicación, circulación de información, producción de datos, organización de visibilidad y disputa política. Por eso, cuando sus decisiones o estructuras de control afectan intereses considerados estratégicos, los Estados tienden a intervenir para reafirmar su autoridad.

Las respuestas estatales adoptaron formas diferentes. EE. UU. recurrió a una combinación de revisión de inversiones extranjeras, órdenes ejecutivas, legislación federal, judicialización y negociación empresarial para reconfigurar la propiedad y el control de TikTok. Brasil, en cambio, actuó principalmente a través del Poder Judicial, exigiendo el cumplimiento de órdenes, el pago de multas, la designación de un representante legal y, finalmente, bloqueando temporalmente la plataforma.

Ahora bien, ambos casos muestran los riesgos de esta intervención: la defensa de la seguridad nacional o del orden democrático puede entrar en tensión con derechos fundamentales como la libertad de expresión, el acceso a la información y la participación pública. Por ello, la disputa no consiste simplemente en si los Estados deben regular o no a las plataformas, sino en cómo hacerlo sin reproducir formas desproporcionadas de control.

En definitiva, TikTok y X muestran que la soberanía digital se ha convertido en un terreno clave de disputa entre actores estatales y actores privados transnacionales. Aunque cada caso respondió a contextos, fundamentos y herramientas distintas, ambos revelan una misma tendencia: los Estados buscan reafirmar su autoridad frente a las grandes corporaciones tecnológicas que disputan su protagonismo en el sistema internacional.

Conclusión

Durante mucho tiempo, la noción de poder en las Relaciones Internacionales fue pensada a partir de imágenes relativamente estables: el territorio, las fronteras, los recursos estratégicos, la diplomacia y la autoridad jurídica del Estado. Sin embargo, el siglo XXI incorporó una nueva dimensión a esa disputa. Hoy, una parte cada vez más decisiva de la política internacional se despliega en un espacio menos visible, pero igualmente conflictivo: el espacio digital. Allí circulan datos, se organizan vínculos sociales, se construyen narrativas, se disputan mercados, se proyectan influencias y se desafían autoridades. Las fronteras no desaparecieron, pero se volvieron más difíciles de ubicar.

Esta tesina partió de una preocupación central, esto es, comprender de qué manera se transformó la disputa por el poder digital entre los Estados y las grandes empresas tecnológicas a partir de la pandemia de COVID-19, y qué estrategias desplegaron los Estados para reafirmar su soberanía frente a ese escenario. El recorrido realizado permite sostener que esa disputa se volvió más intensa, más visible y más política: los Estados ya no confrontan únicamente con otros Estados por recursos estratégicos, sino también con empresas capaces de controlar plataformas, datos sensibles, algoritmos y sistemas digitales que organizan una parte significativa de la vida pública. Las plataformas digitales ya no pueden ser comprendidas como simples herramientas de comunicación; por el contrario, se han convertido en infraestructuras sociales, económicas y políticas sobre las que descansan prácticas cotidianas, debates públicos, flujos de información y nuevas formas de dependencia.

A lo largo del trabajo se sostuvo que la pandemia de COVID-19 intensificó la disputa global por el poder digital. La crisis sanitaria no creó desde cero la dependencia tecnológica, pero la aceleró, la hizo visible y la volvió políticamente urgente. Durante ese período, la conectividad dejó de ser un complemento de la vida social para convertirse en una condición

de posibilidad del trabajo, la educación, el comercio, la comunicación, el acceso a la información y la continuidad de múltiples funciones estatales. Aquello que antes podía percibirse como una comodidad tecnológica pasó a presentarse como una necesidad estructural. Al mismo tiempo, esa dependencia expuso nuevas vulnerabilidades: los Estados advirtieron que una parte creciente de su capacidad de gobierno estaba mediada por infraestructuras, servicios y reglas que no siempre controlaban.

Esta transformación permitió confirmar la hipótesis que guio la investigación: la creciente influencia de las grandes empresas tecnológicas sobre la seguridad, la soberanía y la vida política de los Estados impulsó respuestas regulatorias, judiciales y discursivas orientadas a reafirmar la autoridad estatal en el espacio digital. En este contexto, la soberanía digital emerge como una de las grandes preguntas políticas de nuestro tiempo. No se trata de una simple extensión de la soberanía clásica al mundo tecnológico, ni de la posibilidad de cerrar el espacio digital detrás de fronteras nacionales. Se trata, más bien, de una disputa por la autoridad: quién decide sobre los datos, quién regula las plataformas, quién controla los algoritmos, quién responde por los daños, quién protege los derechos y quién establece los límites entre libertad, seguridad y control. La soberanía digital no aparece como una posesión estable, sino como una capacidad en permanente construcción.

Los casos de TikTok en EE. UU. y X en Brasil muestran dos expresiones concretas de esa disputa. En el primero, una plataforma de entretenimiento fue reinterpretada como una posible amenaza estratégica en el marco de la rivalidad entre EE. UU. y China. El conflicto reveló que los datos, los algoritmos y la propiedad de una plataforma pueden ser entendidos como asuntos de seguridad nacional. En el segundo, una red social global desafió el cumplimiento de decisiones judiciales dentro de un Estado democrático, poniendo en tensión la libertad de expresión, la moderación de contenidos, la desinformación y la autoridad

jurisdiccional. Aunque ambos casos respondieron a contextos distintos, comparten una misma lógica: los Estados buscan reafirmar su capacidad de decisión frente a actores digitales que producen efectos políticos dentro de sus territorios.

Sin embargo, esta reafirmación estatal no está exenta de dilemas. Regular el espacio digital resulta necesario, pero también riesgoso. La ausencia de reglas puede dejar decisiones fundamentales en manos de actores privados sin suficiente control democrático. Pero una intervención estatal desproporcionada puede derivar en censura, vigilancia o restricciones indebidas de derechos. Por eso, el problema central no consiste simplemente en elegir entre Estado o mercado, entre regulación o libertad, entre seguridad o expresión. El verdadero desafío reside en construir formas de gobernanza capaces de responsabilizar a los actores digitales sin clausurar el carácter abierto, plural y democrático del espacio digital.

Desde esta perspectiva, la disputa por la soberanía digital revela una tensión más profunda de las Relaciones Internacionales contemporáneas: el poder ya no se concentra exclusivamente en los Estados, pero tampoco se ha desplazado por completo fuera de ellos. Más bien, se distribuye, se fragmenta y se negocia entre actores estatales, empresas tecnológicas, organismos internacionales, comunidades técnicas e individuos. Dicho de otro modo, las empresas digitales no reemplazan al Estado, pero sí lo desafían. Lo obligan a redefinir sus herramientas, sus márgenes de acción y su capacidad para ejercer autoridad en un entorno que desborda las categorías tradicionales de la política internacional.

La gobernanza global del ciberespacio continúa siendo insuficiente para ordenar estas tensiones. Existen foros, acuerdos, principios y mecanismos de cooperación, pero todavía predominan la fragmentación normativa, las respuestas nacionales y las diferencias entre modelos políticos. Esta falta de consensos refleja que el espacio digital no es un ámbito neutral ni meramente técnico, sino un campo atravesado por intereses estratégicos, valores en

disputa y asimetrías de poder. Gobernar internet implica, en última instancia, discutir qué tipo de orden internacional se está construyendo.

El espacio digital no es un territorio sin ley, pero tampoco puede gobernarse únicamente con herramientas del pasado. Sus fronteras son móviles, sus actores son múltiples y sus efectos atraviesan simultáneamente lo local, lo nacional y lo global. La soberanía digital aparece, entonces, no como una respuesta definitiva, sino como una pregunta abierta: cómo gobernar un mundo cada vez más conectado sin renunciar a la seguridad, a la libertad, a la democracia ni a la responsabilidad pública. Este interrogante, lejos de cerrarse con los casos analizados, será decisivo para comprender cómo se ejercerá, disputará y limitará el poder en el escenario internacional de los próximos años.

Referencias bibliográficas

Acurio Del Pino, S. (2024). Bloqueo de X en Brasil: Atentado a la libertad de expresión o actuación soberana. https://www.academia.edu/123752795/Caso_X_en_Brasil

Agencia de Ciberseguridad y Seguridad de Infraestructura. (2022). Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA): Fact sheet. https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia?os=wtmb5utkcxk5refappamp_kit%3D1

Autoridad Europea de Valores y Mercados. (2025). Digital Operational Resilience Act (DORA). https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

Autoridade Nacional de Proteção de Dados. (2024). Privacidade e Proteção de Dados Pessoais. https://www.gov.br/mec/pt-br/acesso-a-informacao/perguntas-frequentes/privacidade-e-protecao-de-dados-pessoais

Bremmer, I. (2021). The technopolar moment. Eurasia Group.

Chang, L., y Grabosky, P. (2026). The governance of cyberspace. En Regulatory Theory. Australian National University Press.

Comisión Europea y Alto Representante de la Unión Europea. (2020). The EU's Cybersecurity Strategy for the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

Comisión Europea. (2023). Digital Markets Act: Commission designates six gatekeepers. https://digital-strategy.ec.europa.eu/en/news/digital-markets-act-commission-designates-six-gatekeepers

Comisión Europea. (2023). DMA: Rules for digital gatekeepers to ensure open markets start to apply. https://digital-markets-act.ec.europa.eu/dma-rules-digital-gatekeepers-ensure-open-markets-start-apply-2023-05-02_en

Comisión Europea. (2024). AI Act enters into force. https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en

Comisión Europea. (2024). Digital Services Act starts applying to all online platforms in the EU. https://digital-strategy.ec.europa.eu/en/news/digital-services-act-starts-applying-all-online-platforms-eu

Comisión Europea. (2024). NIS2: Commission implementing regulation on critical entities and networks. https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks

Consejo de Europa. (2022). Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence. CETS No. 224.

Consejo de la Unión Europea. (2021). Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy. https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

Consejo de la Unión Europea. (2024). Cyber resilience act: Council adopts new law on security requirements for digital products.

https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/

Cyberspace Administration of China. (2021). Provisions on the Administration of Algorithmic Recommendation in Internet Information Services. https://regulations.ai/regulations/china-2021-12-algorithmic-recommendation

Cyberspace Administration of China. (2022). Cybersecurity Review Measures (Revised). Traducción de DigiChina, Stanford University. https://digichina.stanford.edu/work/translation-cybersecurity-review-measures-revised-effective-feb-15-2022/

Cyberspace Administration of China. (2024). Provisions on Promoting and Regulating Cross-Border Data Flows. https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm

DeNardis, L. (2014). The Global War for Internet Governance. Yale University Press.

Gabinete de Segurança Institucional. (2025). E-Ciber: Estratégia Nacional de Cibersegurança. https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao-e-cibernetica/estrategia-nacional-de-ciberseguranca-eciber

General Services Administration. (2021). Improving the nation's cybersecurity: Executive Order 14028. https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/executive-order-14028

Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.

Gray, J. E. (2021). The geopolitics of "platforms": The TikTok challenge. Internet Policy Review, 10(2), 1–26. https://doi.org/10.14763/2021.2.1557

Grimmelmann, J. (2025). The TikTok ban and its consequences. Communications of the ACM, 68(5), 18–20. https://doi.org/10.1145/3722147

Henen, B. (2025). Cybersecurity in the Digital Era: Between Digital Transformation and Protection Challenges. Law and World.

Horowitz, B., y Check, T. (2022). TikTok v. Trump and the uncertain future of national security-based restrictions on data trade. Journal of National Security Law & Policy, 13(1), 61–111.

Insisa, A. (2025). The US TikTok ban, the RedNote moment and China. IAI Commentaries.

Johanson, M., y Chong, K. J. (2024). Cybersecurity as the New Frontier for States' Hard Power. Department of International Relations, Universitas Pelita Harapan, Tangerang.

Juned, M., Maryam, S., Salam, S., y Utami, R. A. A. (2023). TikTok's conflict of interest with the US government: Between big data security and economics (2017–2023). European Journal of Communication and Media Studies, 2(4), 1–8. https://doi.org/10.24018/ejmedia.2023.2.4.23

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security.

Keohane, R. O. (1984). After hegemony: Cooperation and discord in the world political economy. Princeton University Press.

Library of Congress. (2022). China: Measures of Security Assessment for Cross-Border Data Transfer Take Effect. Global Legal Monitor. https://www.loc.gov/item/global-legal-monitor/2022-12-12/china-measures-of-security-assessment-for-cross-border-data-transfer-take-effect/

Machado Neto, E. (2025). Tech giants vs. national sovereignty: Brazil's legal battle with Elon Musk's X. DCU Law and Tech.

Makovetka, O., Dubov, G., Didych, T., Malyshev, B., y Varych, O. (2024). Global challenges to state sovereignty in the 21st century. Salud, Ciencia y Tecnología - Serie de Conferencias.

Malacalza, B. (2021). América Latina y la Disrupción Digital: Transformaciones en la Cooperación Internacional para el Desarrollo. Consejo Nacional de Investigaciones Científicas y Técnicas. Universidad Nacional de Quilmes, Argentina.

Malacalza, B. (2025). A propósito de las cruzadas tecnológicas en América Latina: ¿Hacia una nueva agenda contra-distópica? Análisis Carolina. Cooperación Española.

Mayer-Schönberger, V., y Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

Morgenthau, H. J. (1948). Politics among nations: The struggle for power and peace. Alfred A. Knopf.

Mukherjee, B. B. (2025). Regulating Digital Fintech: How States Navigate Power and Geopolitics. UNISCI Journal, 68. Galgotias University.

Naciones Unidas. (2024). Pact for the Future, Global Digital Compact and Declaration on Future Generations. Cumbre del Futuro. Documentos Finales.

Naciones Unidas. (2024). United Nations Convention against Cybercrime: Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes.

Naciones Unidas. (2025). Final report of the open-ended Working Group on security of and in the use of information and communications technologies 2021–2025.

National Institute of Standards and Technology. (2021). Software security in supply chains. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains

National People's Congress of China. (2021). Data Security Law of the People's Republic of China. https://en.spp.gov.cn/2021-06/10/c_948426_2.htm

National People's Congress of China. (2021). Personal Information Protection Law of the People's Republic of China. https://personalinformationprotectionlaw.com/

Nicas, J., y Conger, K. (2024). Brazil blocks X after Musk ignores court orders. The New York Times.

Noël, J.-C. (2019). What is digital power? French Institute of International Relations.

Nye, J. S. (2010). Cyber power. Harvard Kennedy School.

Nye, J. S. (2011). The future of power. Public Affairs.

Nye, J. S. (2014). The regime complex for managing global cyber activities. Global Commission on Internet Governance Paper Series, 1. Centre for International Governance Innovation and Chatham House.

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2020). COVID-19 learning disruption and recovery: Snapshot of UNESCO's work in education in 2020. https://www.unesco.org/en/articles/COVID-19-learning-disruption-recovery-snapshot-unescos-work-education-2020

Organización Internacional del Trabajo. (2020). Working from home: Estimating the worldwide potential. https://www.ilo.org/resource/brief/working-home-estimating-worldwide-potential

Ortega, A. (2024). Brasil y X: El dilema entre la regulación digital y la libertad de expresión. Centro de Estudios Estratégicos de Relaciones Internacionales.

Presidência da República do Brasil. (2020). Decreto N.º 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222impressao.htm

Presidência da República do Brasil. (2023). Decreto N.º 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11856.htm

Presidência da República do Brasil. (2025). Decreto N.º 12.573, de 4 de agosto de 2025. Institui a Estratégia Nacional de Cibersegurança. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12573.htm

Raymond, M., y DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. International Theory. Cambridge University Press.

Rodrigues Brancher, P. M. (2024). El bloqueo de la plataforma X por el Supremo Tribunal Federal y la exigencia para empresas extranjeras de indicar representante legal en Brasil. Revista Iberoamericana de Derecho Informático, 15(2), 117–124.

Schtivelband Guindi, J. (2025). Del test tripartito a los términos y condiciones: Tensiones entre Brasil y X (2020–2024) en torno a la regulación y moderación del debate público. Argumentos. Revista de Crítica Social, 32, 817–847.

Shoker, A. (2022). Digital sovereignty strategies for every nation. Applied Cybersecurity & Internet Governance, 1(1), 1–17. https://doi.org/10.5604/01.3001.0016.0943Srnicek, N. (2017). Platform capitalism. Polity Press.

State Council of the People's Republic of China. (2021). Regulation to strengthen protection over critical information infrastructure. https://english.www.gov.cn/policies/latestreleases/202108/17/content_WS611b8062c6d0df57f98de907.html

State Council of the People's Republic of China. (2023). China moves to support generative AI, regulate applications. https://english.www.gov.cn/news/202307/13/content_WS64aff5b3c6d0868f4e8ddc01.html

Strange, S. (1988). States and markets. Pinter Publishers.

Strange, S. (1996). The retreat of the state: The diffusion of power in the world economy. Cambridge University Press.

Sutherland, M. D., Benson, P. J., y Cho, C. Y. (2025). TikTok: Frequently asked questions and issues for Congress (R48023). Congressional Research Service.

Tewari, S., y Jamali, L. (2026). TikTok closes deal to split US app from global business. BBC.

The Editors of ProCon. (2026). TikTok: Should TikTok be banned? Encyclopaedia Britannica.

The White House. (2021). Executive Order 14028 - Improving the nation's cybersecurity. https://www.presidency.ucsb.edu/documents/executive-order-14028-improving-the-nations-cybersecurity

The White House. (2023a). National Cybersecurity Strategy.

The White House. (2023b). National cybersecurity strategy implementation plan.

The White House. (2024). National cybersecurity strategy implementation plan, version 2.

The White House. (2025). Sustaining select efforts to strengthen the nation's cybersecurity and amending Executive Order 13694 and Executive Order 14144. https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/

Törnberg, P. (2024). Platforms as States: The rise of governance through data power.

Unión Europea. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. EUR-Lex. https://eur-lex.europa.eu/eli/dir/2022/2555/en

Van Dijck, J., Poell, T., y de Waal, M. (2018). The platform society: Public values in a connective world. Oxford University Press.

Waltz, K. N. (1979). Theory of international politics. McGraw-Hill.

Wendt, A. (1999). Social theory of international politics. Cambridge University Press.

Anexo I: Lista de abreviaciones y siglas

Abreviación/sigla	Significado
5G	Quinta generación de tecnologías de redes móviles
API	Interfaz de programación de aplicaciones (*Application Programming Interface*)
CFIUS	Comité de Inversión Extranjera en Estados Unidos (*Committee on Foreign Investment in the United States*)
COVID-19	Enfermedad por coronavirus de 2019 (*Coronavirus Disease 2019*)
DMA	Reglamento de Mercados Digitales (*Digital Markets Act*)
DORA	Reglamento de Resiliencia Operativa Digital (*Digital Operational Resilience Act*)
DSA	Reglamento de Servicios Digitales (*Digital Services Act*)
EE. UU.	Estados Unidos
FBI	Buró Federal de Investigaciones (*Federal Bureau of Investigation*)
IA	Inteligencia artificial
IEEPA	Ley de Poderes Económicos de Emergencia Internacional (*International Emergency Economic Powers Act*)
IoT	Internet de las cosas (*Internet of Things*)
LLC	Sociedad de responsabilidad limitada (*Limited Liability Company*)
NIS2	Segunda Directiva sobre la Seguridad de Redes y Sistemas de Información *(Network and Information Security Directive 2)*
NIST	Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*)
OIT	Organización Internacional del Trabajo
OMB	Oficina de Gestión y Presupuesto (*Office of Management and Budget*)
OMS	Organización Mundial de la Salud
PAFACAA	Ley de Protección de los Estadounidenses frente a Aplicaciones Controladas por Adversarios Extranjeros (*Protecting Americans from Foreign Adversary Controlled Applications Act*)
RPC	República Popular China
SARS-CoV-2	Coronavirus 2 del síndrome respiratorio agudo severo
STF	Supremo Tribunal Federal
TIC	Tecnologías de la Información y la Comunicación
TSE	Tribunal Superior Electoral
UE	Unión Europea
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
USDS	Seguridad de Datos de Usuarios Estadounidenses (*U.S. Data Security*)
VPN	Red privada virtual (*Virtual Private Network*)

Anexo II: Principales tecnologías digitales asociadas a la Cuarta Revolución Industrial

Función	Tecnología	Definición conceptual	Naturaleza tecnológica	Aplicación en el ámbito público y social	Origen y evolución temporal
Tecnologías habilitantes de la infraestructura digital	Tecnologías de la Información y Comunicación	Conjunto de tecnologías digitales que permiten la producción, almacenamiento, procesamiento y transmisión de información a través de sistemas electrónicos, incluyendo redes de telecomunicaciones, computadoras y plataformas digitales.	Hardware y software	Gobierno electrónico (*e-government*), digitalización de servicios públicos, educación virtual, sistemas de salud digital (historias clínicas electrónicas), inclusión digital y gestión de datos administrativos.	Conceptualización en la década de 1970; expansión global a partir de los años 1990 con la masificación de internet.
	Computación de la nube (*Cloud computing*)	Modelo de provisión de servicios informáticos a través de internet que permite acceder a recursos como almacenamiento, procesamiento y software bajo demanda, sin necesidad de infraestructura local.	Hardware y software	Digitalización gubernamental, almacenamiento de datos públicos, interoperabilidad entre organismos, educación virtual y servicios digitales escalables.	Conceptualización en la década de 1960; desarrollo moderno y adopción masiva en la década de 2000 con empresas como Amazon y Google.
	Redes 5G	Quinta generación de tecnologías de redes móviles que permite una conectividad ultrarrápida, baja latencia y alta capacidad de transmisión de datos, habilitando la comunicación masiva entre dispositivos.	Hardware y software	Ciudades inteligentes, vehículos autónomos, telemedicina, automatización industrial, gestión de infraestructuras críticas y expansión del Internet de las cosas.	Desarrollo conceptual en la década de 2010; primeras implementaciones comerciales a partir de 2019.

Función	Tecnología	Definición conceptual	Naturaleza tecnológica	Aplicación en el ámbito público y social	Origen y evolución temporal
Tecnologías de procesamiento y gestión de datos	Inteligencia artificial	Campo de la informática orientado al desarrollo de sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento, la toma de decisiones y el reconocimiento de patrones.	Principalmente software (con soporte en hardware especializado)	Automatización de servicios públicos, análisis predictivo para políticas públicas, vigilancia y seguridad, sistemas judiciales asistidos, *chatbots* gubernamentales y diagnóstico médico.	Término acuñado en 1956 en la conferencia de Dartmouth.
	Análisis de macrodatos (*Big Data analytics*)	Conjunto de tecnologías y técnicas destinadas al procesamiento y análisis de grandes volúmenes de datos, estructurados y no estructurados, para extraer información útil y apoyar la toma de decisiones.	Hardware y software	Políticas públicas basadas en evidencia, análisis epidemiológico, seguridad pública, gestión fiscal, planificación urbana y monitoreo social.	Desarrollo conceptual en la década de 1990; expansión y popularización en los años 2000.
	Cadena de bloques (*Blockchain*)	Tecnología de registro distribuido que permite almacenar información de manera descentralizada, segura e inmutable mediante criptografía, sin necesidad de intermediarios.	Software	Gobierno digital, identidad digital, trazabilidad en cadenas de suministro, votación electrónica, registros públicos y contratos inteligentes.	2008, con la publicación del *whitepaper* de Satoshi Nakamoto.
Tecnologías de aplicación e interacción	Internet de las cosas	Sistema de interconexión de objetos físicos dotados de sensores, software y conectividad que les permite recopilar e	Hardware y software	Ciudades inteligentes (gestión de tránsito, alumbrado público), monitoreo ambiental, infraestructura urbana	Término acuñado en 1999 por Kevin Ashton; desarrollo de dispositivos desde principios de la década de 1990.

Función	Tecnología	Definición conceptual	Naturaleza tecnológica	Aplicación en el ámbito público y social	Origen y evolución temporal
		intercambiar datos en tiempo real a través de internet.		inteligente, gestión de residuos, sistemas de seguridad pública y salud remota.	
	Plataformas digitales	Infraestructuras digitales que facilitan la interacción entre múltiples actores (usuarios, empresas, gobiernos) mediante la recolección, procesamiento y monetización de datos.	Software	Comunicación política, difusión de información, economía digital, prestación de servicios, formación de opinión pública y gobernanza de contenidos.	Desarrollo en la década de 2000 con la expansión de internet; consolidación global en la década de 2010.
	Robótica	Disciplina tecnológica que diseña, construye y opera robots capaces de ejecutar tareas de manera autónoma o semiautónoma mediante sensores, actuadores y sistemas de control.	Hardware y software	Automatización industrial, robótica médica, seguridad y defensa, logística, asistencia en desastres y servicios urbanos.	Término introducido por Karel Čapek en 1920; desarrollo tecnológico moderno desde los años 1960–1970.
	Realidad virtual	Tecnología que permite la inmersión del usuario en entornos digitales tridimensionales generados por computadora, mediante dispositivos que simulan la presencia física en dichos entornos.	Hardware y software	Capacitación en fuerzas de seguridad y salud, simulaciones militares, educación inmersiva, planificación urbana y terapias psicológicas.	Concepto inicial en los años 1960 (dispositivos como el sensorama); consolidación como tecnología digital en la década de 1980.
	Realidad aumentada	Tecnología que superpone	Hardware y software	Capacitación técnica,	Surge en paralelo con el

Función	Tecnología	Definición conceptual	Naturaleza tecnológica	Aplicación en el ámbito público y social	Origen y evolución temporal
		elementos digitales (imágenes, datos, objetos tridimensionales) sobre el entorno físico en tiempo real, enriqueciendo la percepción del mundo real.		mantenimiento de infraestructura, educación interactiva, aplicaciones en turismo, planificación urbana y asistencia en emergencias.	concepto de realidad virtual, pero el término fue acuñado en la década de 1990 por Boeing.

Fuente: Elaboración propia en base a Malacalza (2025)