

# Soberanía Digital

Revista Latinoamericana de Economía y Sociedad Digital

Issue Número Especial 1, Julio 2022

---

**Autores:** [Julia Pohle](#) , [Thorsten Thiel](#) 

**DOI:** [10.53857/OLMH2516](https://doi.org/10.53857/OLMH2516)

**Publicado:** 29 julio, 2022

**Cita sugerida:** Pohle, J., & Thiel, T. (2022). Soberanía digital. Revista Latinoamericana de Economía Y Sociedad Digital. <https://doi.org/10.53857/olmh2516>

**Licencia:** Creative Commons Atribución-NoComercial 4.0 Internacional ([CC BY-NC 4.0](https://creativecommons.org/licenses/by-nc/4.0/))

**Tipo:** [Ensayo](#), [Traducción](#)

**Palabras clave:** [Autoridad Estatal](#), [Economía Digital](#), [Gobernanza de Internet](#), [Soberanía Digital](#)

---

## Nota sobre la traducción

Este artículo fue originalmente publicado en la sección [Concepts of the Digital Society](#) de la revista Internet Policy Review, editada por Christian Katzenbach y Thomas Christian Bächle. Es publicado en la Revista Latinoamericana de Economía y Sociedad Digital según los lineamientos de acceso abierto del artículo original, con licencia Creative Commons Attribution 3.0 Germany.

**Título Original:** Digital Sovereignty

**Fecha de publicación original:** 17 de Diciembre de 2020

**Link al artículo original:** <https://policyreview.info/concepts/digital-sovereignty>

**DOI original:** <https://doi.org/10.14763/2020.4.1532>

Traducido del idioma inglés por [The Pillow Books](#) para la Revista Latinoamericana de Economía y Sociedad Digital en Mayo 2022.

## Resumen

En la última década, la soberanía digital se ha convertido en un elemento central en los discursos políticos sobre temas digitales. Aunque su popularidad ha aumentado, tanto en los

países centralizados/autoritarios como en los democráticos, el concepto es aún muy controvertido. Tras investigar los desafíos a la soberanía que en apariencia plantea la transformación digital, este ensayo explora cómo la soberanía ha reaparecido como una categoría clave en relación con lo digital. Luego de sistematizar los diversos argumentos de carácter normativo sobre la soberanía digital, expone cómo, en la actualidad, el concepto se entiende más como una práctica discursiva en la política y en la normativa que como un concepto jurídico u organizativo.

## Abstract

Over the last decade, digital sovereignty has become a central element in policy discourses on digital issues. Although it has become popular in both centralised/authoritarian and democratic countries alike, the concept remains highly contested. After investigating the challenges to sovereignty apparently posed by the digital transformation, this essay retraces how sovereignty has re-emerged as a key category with regard to the digital. By systematising the various normative claims to digital sovereignty, it then goes on to show how, today, the concept is understood more as a discursive practice in politics and policy than as a legal or organisational concept.

## INTRODUCCIÓN

En julio de 2020, en su programa oficial para la presidencia del Consejo Europeo, el gobierno alemán anunció su intención de “establecer la soberanía digital como *leitmotiv* de la política digital europea” (Presidencia alemana del consejo de la UE, 2020, p.8). Este es solo uno de los muchos episodios recientes [si bien uno muy destacado] en el que el término soberanía digital ha sido utilizado por los gobiernos para transmitir la idea de que los Estados deben reafirmar su autoridad sobre la internet y proteger a su ciudadanía y a sus empresas de los múltiples desafíos que ésta supone para la autodeterminación en la esfera digital.

A primera vista, la transformación digital y la infraestructura técnica global de la internet parecen representar un desafío a la soberanía. Los principios de territorialidad y jerarquía estatal parecen oponerse a las constelaciones difusas, flexibles y en constante cambio de las redes digitales globales. Además, las aplicaciones digitales y las prácticas en materia de comunicación han generado un impulso que parece desafiar la gobernanza y el control legales. Por lo tanto, el crecimiento de las redes digitales en la década de 1990 hizo que la desaparición del Estado fuera un escenario plausible en lo inmediato. Esto se plasmó de forma célebre en la audaz *Declaración de independencia del ciberespacio*, de John Perry Barlow (1996). Sin embargo, aunque esta referencia sigue muy presente en el discurso público, hoy en día se interpreta más como una amenaza que como una promesa. Para contrarrestar los riesgos que podría suponer a su autoridad, los Estados han permitido la

aplicación de leyes nacionales y la realización de intervenciones gubernamentales en la esfera digital. A lo largo de los años, han creado y reformado instrumentos técnicos y jurídicos para abordar cuestiones de gobernanza digital (Goldsmith y Wu, 2006). Además, han logrado convencer a la ciudadanía de que la soberanía y la autoridad estatal son necesarias para proteger “bienes vitales”, que van desde la seguridad y la prosperidad, hasta las normas culturales y el control de los medios de comunicación. Como resultado, en la actualidad, la ciudadanía de muchos países espera que su gobierno proteja su privacidad en línea o combata la desinformación digital y la ciberdelincuencia. Sin embargo, en los últimos años, los múltiples llamados a la soberanía digital, tanto en los países centralizados/autoritarios como en las democracias liberales, no solo reafirman la autoridad y la intervención del Estado en la esfera digital. El concepto de soberanía digital se ha convertido en un poderoso término en el discurso político que busca reinstaurar el Estado-nación, incluidas la economía y la ciudadanía de la nación, como una categoría relevante en la gobernanza global de las infraestructuras digitales y el desarrollo de las tecnologías digitales. Es previsible que el concepto de soberanía digital adquiera aún más vigencia política en los próximos años, dado el amplio despliegue de tecnologías digitales altamente invasivas que van desde la inteligencia artificial hasta el “internet de las cosas”.

Hasta ahora, el concepto de soberanía digital se ha utilizado de forma generalizada en el discurso político, pero rara vez se ha analizado en la investigación académica, salvo un número reducido pero creciente de excepciones (Couture y Toupin, 2019; Mueller, 2010, 2019; Pohle, 2020c; Pohle y Thiel, 2019; Thiel, 2014, 2019; Glasze y Dammann, en prensa; Peuker, 2020). Para comprender de dónde viene el concepto y hacia dónde se dirige, partimos de dos pasos. En primer lugar, reconstruimos las controversias clave que definen la relación entre la soberanía y las redes digitales. A continuación, analizamos cómo resurgieron el concepto de soberanía y la categoría de Estado y se elevó la soberanía digital hasta convertirse en una forma valorada de soberanía por derecho propio. En segundo lugar, sistematizamos las distintas reivindicaciones de la soberanía digital, con lo que se ponen de manifiesto las tensiones y contradicciones internas del concepto. Al rastrear la dinámica de la politización, buscamos demostrar que la soberanía es una práctica discursiva en la política y en la normativa, más que un concepto jurídico y organizativo, que es como se ha concebido de forma tradicional.

## **LA RELACIÓN ENTRE LA SOBERANÍA Y LO DIGITAL: UNA RECONSTRUCCIÓN**

El concepto de soberanía, entendido como el poder del que goza un órgano de gobierno para gobernar sobre sí mismo, libre de cualquier interferencia de fuentes u organismos externos, deriva de la palabra latina *superanus*, que significa “sobre” o “superior”. Mientras que la teoría tradicional de la soberanía, propuesta en el siglo XVI por el filósofo político francés Jean Bodin, se refería a la autoridad del gobernante para tomar decisiones

definitivas, Jean-Jacques Rousseau reformuló el concepto para que se centrara en la soberanía popular y no en la soberanía monárquica; con el tiempo, se asoció cada vez más con la democracia, el Estado de derecho y la territorialidad. En la actualidad, se entiende por soberanía la independencia de un Estado frente a otros estados (soberanía externa), así como su poder supremo de mando sobre todos los poderes dentro del territorio del Estado (soberanía interna). Entendida como soberanía democrática, abarca la soberanía popular y el derecho de la ciudadanía a ejercer la autodeterminación mediante el ejercicio de sus derechos inalienables. En todas las acepciones es crucial la especificación geográfica, es decir, la restricción de la soberanía a un territorio concreto, considerado un requisito funcional para que la autoridad se ejerza de forma efectiva (Grimm, 2015).<sup>[1]</sup>

Desde la época de Bodin, la soberanía ha sido un concepto central para comprender la política. Pero en la década de 1990, esta importancia pareció menguar, lo que llevó a hablar de un mundo postsoberano en el que los Estados ya no serían la fuente más importante y, a la postre, superior, de poder y donde la democracia estaría asociada de forma más cercana al pluralismo y la participación que a la capacidad de un pueblo (*demos*) de autogobernarse (MacCormick, 1999). Esta prevista pérdida de importancia del Estado tuvo una influencia importante en las primeras etapas del desarrollo y la gobernanza de la internet. La idea de la soberanía del Estado se vio particularmente desafiada por dos corrientes discursivas diferentes, aunque relacionadas, que configuraron de forma significativa los discursos públicos y académicos: *el excepcionalismo cibernético* y *la gobernanza multiactor de la internet*. Sin embargo, en años recientes, los actores políticos han logrado justificar y reafirmar la soberanía en la esfera digital frente a estas dos perspectivas.

## **DOS DESAFÍOS: EL EXCEPCIONALISMO CIBERNÉTICO Y LA GOBERNANZA DE LA INTERNET**

El primer desafío, *el excepcionalismo cibernético*, sugiere que, desde el punto de vista cualitativo, el ámbito digital es distinto al analógico y que, por lo tanto, los espacios digitales deben abordarse con un criterio diferente al de todas las innovaciones tecnológicas previas. Aunque esta perspectiva gozó de una gran popularidad durante el auge de la internet comercial en la década de 1990, aún está presente en el discurso público y académico. El razonamiento detrás del excepcionalismo cibernético se basa en la suposición de que la creciente importancia de la comunicación en red asistida por computadora implica la desaparición de la soberanía estatal (Katz, 1997). Aunque el desarrollo de la internet no se produjo fuera de espacios legales concretos y no habría sido posible sin los incentivos proporcionados por los mercados, los regímenes reguladores o las infraestructuras públicas de investigación (Mazzucato, 2011), el excepcionalismo cibernético —que suele adoptar la forma de *libertarismo cibernético* (Keller, 2019)— fue la ideología que dominó en aquella primera época y gozó de un fuerte respaldo cultural y económico en Silicon Valley (Barbrook y Cameron, 1996; Turner, 2006).

Como actores que desconfían en gran medida de las instituciones políticas establecidas, los libertarios cibernéticos sostienen que las formas de política mediadas por la tecnología digital darán pie a la organización descentralizada de las sociedades. Esto debería facilitar una respuesta mejor adaptada a las complejas exigencias que supone el gobierno de las sociedades modernas que la ofrecida por las formas tradicionales de organización política. Desde esta perspectiva, se espera que la soberanía externa, el derecho y la territorialidad resulten menos importantes en el contexto de las redes transnacionales. Los argumentos para ello son múltiples. En primer lugar, la complejidad de las responsabilidades imbricadas y el alcance global de las redes no pueden abordarse de forma adecuada dentro de las jurisdicciones nacionales; en segundo lugar, los procedimientos legislativos son demasiado lentos para seguir el ritmo de la innovación de las tecnologías digitales y los modelos de negocio asociados; y en tercer lugar, las tecnologías digitales permiten a las personas eludir responsabilidades, ya que en el mundo digital la atribución se convierte en un constructo inestable (Post, 2007). Por lo tanto, en contraste con un mundo limitado por territorios y naciones soberanas, el mundo invocado por el libertarismo cibernético requiere de la existencia de *soberanía cibernética*, con el [ciberespacio](#) como un nuevo y autónomo reino virtual, independiente de la interferencia del gobierno (Barlow, 1996).<sup>[2]</sup>

Hoy en día, aún resuenan las posturas del excepcionalismo y del libertarismo cibernéticos; por ejemplo, en los debates sobre las criptomonedas (Pistor, 2020). Pero el argumento principal, a saber, que el auge de las redes digitales como tal conducirá a la desaparición de las concepciones territoriales de la soberanía, ha perdido su atractivo. Las infraestructuras y la gestión de la comunicación digital no han cesado de transformarse, lo que facilita la observación y la orientación de los flujos digitales. Esta tendencia se ha visto reforzada por la comercialización de la internet, ya que ha propiciado el surgimiento de jardines amurallados y de nuevos agentes interesados en una arquitectura más fina, menos anónima y horizontal, que permite intervenir en múltiples puntos (DeNardis, 2012; Deibert y Crete-Nishihata, 2012).

Al menos desde el año 2000, surgió un segundo desafío, relacionado con la soberanía en su sentido original, pero menos conflictivo: la *gobernanza multiactor de la internet*. En este caso, la atención no se centra en las deficiencias de los Estados al momento de regular asuntos relacionados con el ámbito digital, sino en los diferentes papeles, ajenos a la soberanía, que deben desempeñar en el marco de un ideal normativo que considera que la administración de la internet es tarea de quienes se ven afectados de forma directa por ella. Con sus orígenes en la comunidad técnica, caracterizada por la pericia y la toma de decisiones basada en el mérito, surgieron diversos procesos descentralizados, diseñados para servir al desarrollo y la aplicación de normas, reglas y procedimientos compartidos para mantener y desarrollar la internet (Klein, 2002; Chenou, 2014). En esta visión, la autogobernanza tendría lugar en una estructura de gobernanza multiactor basada en los principios de apertura, inclusión, colaboración ascendente y toma de decisiones consensuada. Según se argumentó, esta forma de coordinación podría contrarrestar la necesidad de una autoridad central de toma de decisiones (Hofmann, 2016; Raymond y

DeNardis, 2015).

Aunque la gobernanza multiactor de la internet se ha consolidado como un campo relativamente autónomo en el ámbito político mundial, está marcada por conflictos de diversa índole. En general, el origen de sus conflictos externos es que el modelo de gobernanza multiactor aún rechaza de manera categórica a las instituciones internacionales establecidas, que son controladas por los gobiernos, y pretende sustituirlas por el principio del transnacionalismo. En cambio, representantes de algunos Estados han insistido en atribuir a las instituciones multilaterales la facultad de tomar decisiones vinculantes en materia de gobernanza de la internet y, por tanto, someterlas en mayor medida al control estatal (Musiani y Pohle, 2014; Glen, 2014). Los conflictos internos en este ámbito se deben a problemas de coordinación cada vez más evidentes causados por los múltiples procesos de gobernanza, a menudo paralelos, así como a un cambio temático que se aparta de las cuestiones de carácter principalmente tecnológico para acercarse a asuntos más abiertamente de índole política o social (Malcolm, 2008). Además, la idea de la gobernanza multiactor de la internet suele asociarse con el pensamiento neoliberal (Chenou, 2014). Así, las esperanzas de un cambio duradero o expansivo en la forma de hacer política a nivel transnacional no se han cumplido. En vista de que las naciones, tanto autoritarias como democráticas, intentan cada vez más regionalizar el desarrollo de las redes digitales, cabe dudar que los esfuerzos por reformar la gobernanza multiactor de la internet logren la aceptación necesaria para preservar el modelo y sus principios (Voelsen, 2019b). Por lo tanto, la gobernanza multiactor de la internet no puede considerarse el futuro de la gobernanza como tal, ni una alternativa dicotómica a la toma de decisiones por parte de los Estados soberanos, sino, más bien, un modelo de gobernanza paralelo adaptado para procesos de coordinación no vinculantes.

## **RESURGIMIENTO DE LA SOBERNÍA COMO PRINCIPIO DEL DISEÑO DE POLÍTICAS DIGITALES**

En muchos aspectos, el imaginario público que considera que la comunicación digital es en cierto modo hostil a la soberanía del Estado, así como los desafíos prácticos que suponen ejercer el poder soberano en el ámbito digital, se han mantenido (Mueller, 2010). No obstante, los argumentos a favor de descartar la soberanía estatal se han debilitado de forma significativa; en cambio, diversos actores han comenzado a proclamar la necesidad de establecer la soberanía en el ámbito digital. Las justificaciones de estos llamados son diversas.

En primer lugar, suele argumentarse que el verdadero desafío a la soberanía del Estado ya no reside en las cualidades organizativas amorfas de las redes descentralizadas, sino en el enorme poder de los actores corporativos que prosperan en nuestro entorno comercializado de la internet y ostentan el poder material e inmaterial de poseer estructuras sociales vitales. El enfoque comercial de la internet se ha centrado en la publicidad y la explotación

de los efectos de red (Christl, 2017). El papel de las empresas intermediarias y de las plataformas digitales en la difusión de contenidos es tan dominante que los protocolos abiertos de la internet, en los que se basa la comunicación digital, pierden todo sentido (Pasquale, 2016; Srnicek, 2017; Hindman, 2018). Hoy en día, no se trata tan solo de los enormes recursos que dichas empresas intermediarias manejan, sino también de la forma en que ejercen el control, lo que las convierte en uno de los mayores desafíos para el concepto de soberanía democrática (Staab, 2019; Zuboff, 2019). Las empresas que ofrecen servicios de internet son las que dotan de infraestructura a nuestras sociedades y, por lo tanto, interfieren en los asuntos del Estado en aspectos muy delicados. Los ejemplos abundan: ya sea que hablemos de la creación y regulación de los mercados o de la provisión y estructuración de la comunicación pública, la economía digital actual difiere en gran medida de anteriores configuraciones sociales; a tal punto que muchos de los poderosos actores corporativos podrían describirse como cuasisoberanos. La aparición de estos centros de poder corporativos, que parecen no tener que rendir cuentas a través de los mecanismos políticos tradicionales, ha suscitado [sobre todo en Europa] una nueva reflexión, más estructural y a menudo más amplia, sobre las exigencias y los ámbitos de la autogobernanza democrática (van Dijck, 2002).

Una segunda justificación para ampliar e impulsar la soberanía digital se hace más evidente cuando observamos la respuesta, un tanto paradójica, de los gobiernos ante las revelaciones de Edward Snowden en 2013 sobre las prácticas de vigilancia global masiva de los servicios de inteligencia de Estados Unidos y sus aliados (Tréguer, 2017, 2018; Steiger *et al.*, 2017). Snowden reveló el ejercicio del poder hegemónico, en gran medida ilimitado, y las enormes posibilidades de recopilación, análisis y control de datos por parte de las agencias de inteligencia y las empresas tecnológicas de Estados Unidos y otros países de occidente. Resulta sorprendente que su decisión de comportarse como entidades soberanas, pero no territoriales, no condujera a una crítica de la aglomeración de poder (Hintz & Dencik, 2016). En cambio, desencadenó la exigencia de una esfera digital desvinculada que permitiera ejercer un control nacional exclusivo sobre las comunicaciones, los datos y la regulación. Desde las revelaciones de Snowden, la exigencia de una soberanía digital nacional (o regional) es invocada por actores que destacan los riesgos de la vigilancia y la manipulación extranjeras, con ejemplos que incluyen desde la desinformación (Tambiana, 2020) hasta la infraestructura de telecomunicaciones (Voelsen, 2019a) y la política industrial (Hobbs *et al.*, 2020).

Si hacemos un resumen de las observaciones realizadas hasta ahora, podemos ver cómo la soberanía (del Estado), que siempre se consideró la base de la política moderna, se ha convertido en un concepto polémico. Sin embargo, poco a poco ha ido encontrando la manera de adaptarse a la era digital. En la actualidad, abundan las justificaciones para insistir en la soberanía. En las relaciones internacionales, en particular, se observa el resurgimiento de la soberanía como reivindicación geopolítica, lo que ha puesto en marcha una carrera por establecer y ampliar el alcance de la soberanía. No obstante, la soberanía digital debe explicarse y ajustarse de forma activa para que pueda adaptarse a nuestras

sociedades interconectadas, con su amplia gama de comunicaciones, sus fuertes lazos transnacionales y su concepción pluralista de la democracia.

## **DISCURSO(S) POLÍTICO(S) EN MATERIA DE SOBERANÍA DIGITAL**

En la actualidad, el concepto de soberanía digital se utiliza en diversos ámbitos políticos y económicos, desde los países más centralizados y autoritarios hasta las democracias liberales. Ha adquirido una gran variedad de connotaciones, variantes y cualidades cambiantes. Su significado específico varía en función de los diferentes entornos nacionales y los acuerdos entre actores, pero también según el tipo de autodeterminación que dichos actores destacan (Pohle, 2020c; Lambach, 2019; Wittpahl, 2017). Al centrarnos en este último factor, podemos sistematizar las demandas de soberanía digital al establecer una distinción entre si abordan la capacidad de autodeterminación digital de los Estados, las empresas o las personas. Lo que comparten las diferentes capas discursivas resultantes de esta variedad de demandas es su carácter prescriptivo y normativo; más que referirse a instrumentos existentes o a prácticas concretas, suelen formular aspiraciones o recomendaciones para tomar medidas.<sup>[3]</sup>

## **LA AUTONOMÍA DEL ESTADO Y LA SEGURIDAD DE LAS INFRAESTRUCTURAS NACIONALES**

En la categoría más destacada de las demandas en relación con la soberanía digital, se hace hincapié en la idea de que una nación o una región debe adoptar acciones y decisiones autónomas en relación con sus infraestructuras digitales y el despliegue de tecnología. La mayoría de estas demandas se refiere a la restricción geográfica de la soberanía a un territorio específico y a los esfuerzos de los Estados por garantizar la seguridad de las infraestructuras digitales y su autoridad, en materia de comunicación digital, en relación con sus territorios y su ciudadanía.

Podemos identificar dos vertientes de esta línea de pensamiento. Por un lado, las potencias ajenas al mundo liberal han experimentado el auge de la comunicación en red como una amenaza para los sistemas políticos existentes. China fue el primer país en responder a esto al difundir y desarrollar su idea de soberanía digital, enmarcada en gran medida como *soberanía cibernética* o *soberanía de internet* (Creemers, 2016, 2020; Jiang, 2010; Zeng *et al.*, 2017). Las ideas subyacentes fueron adaptadas más adelante por otros países de corte autoritario y semiautoritario, entre los que destaca Rusia (Budnitsky y Jia, 2018; Stadnik, 2019; Nocetti, 2015). Por otro lado, antes, los Estados occidentales ya también habían abordado la necesidad de control e independencia en materia digital. En este caso, la justificación para crear arquitecturas de control fue motivada sobre todo por temas de seguridad. A medida que surgían las redes globales, los Estados eran cada vez más



conscientes de sus vulnerabilidades, que se expresaban en cuestiones relacionadas con el control de infraestructuras. La seguridad informática se tradujo entonces en seguridad nacional y se expandió cada vez a más áreas (Nissenbaum, 2005; Hansen y Nissenbaum, 2009). En este proceso, el papel y las capacidades de los Estados democráticos y del control de las infraestructuras han cobrado cada vez mayor importancia (Cavelty y Egloff, 2019), aunque con frecuencia estas prácticas han entrado en conflicto con los ideales liberales y democráticos de la sociedad y con las antiguas concepciones de la tecnología como inclusiva y pluralista (Möllers, 2020). Desde las revelaciones de Snowden en 2013, el enfoque en la autonomía y la seguridad del Estado se ha convertido en un elemento central de los discursos sobre la soberanía digital.

Los principales ejemplos de prácticas e ideas promovidas por los gobiernos, que se derivan de esta vertiente discursiva, son las numerosas propuestas recientes relativas a la localización de datos. Dichas propuestas buscan restringir el almacenamiento, el movimiento y/o el procesamiento de datos a áreas y jurisdicciones específicas y suelen justificarse por la necesidad de limitar el acceso que las agencias comerciales y de inteligencia extranjeras pueden tener a ciertos tipos de datos como, por ejemplo, los datos industriales o personales. Con frecuencia se asume, aunque rara vez se afirma con claridad, que detrás de muchas de estas propuestas existen otras motivaciones, como un mayor acceso a los datos de la ciudadanía por parte de agentes de inteligencia y de los organismos encargados de hacer cumplir la ley, así como el deseo de generar ingresos para actores como las empresas proveedoras de servicios de internet a nivel local (Chander y Le, 2015; Hill, 2014). Hasta ahora, en muchos países, incluidos Brasil y la India [dos importantes economías emergentes] las propuestas de localización de datos solo se han realizado de manera fragmentada o se limitan a contextos específicos (Panday y Malcom, 2018; Selby, 2017). Un caso emblemático de una iniciativa de localización de datos propuesta en Europa es la idea del *Schengen Routing*, es decir, la propuesta de evitar el enrutamiento de los flujos de datos dentro de Europa, a través de puntos de intercambio y rutas fuera de dicho continente (Glasze y Dammann, en prensa, p. 11). La idea, propuesta por Deutsche Telekom, el mayor proveedor de internet de Alemania y la mayor organización de telecomunicaciones de la Unión Europea, fue objeto de un acalorado debate, tanto en la esfera pública como en la política; sin embargo, al final no logró obtener suficiente apoyo político (Kleinhaus, 2013).

Las demandas y medidas propuestas que ponen énfasis en la autonomía y la autodeterminación de los Estados y la seguridad de infraestructuras digitales esenciales, presentes tanto en los países autoritarios como en los democráticos, han sido objeto de severas críticas. Tanto los actores políticos como quienes son meros testigos, como el personal académico y técnico experto, temen que los esfuerzos que se centran en la seguridad de las TI y en la regulación de temas vinculados con la internet a nivel nacional interfieran con la naturaleza abierta de acceso universal de la internet (Maurer *et al.*, 2014) y, en última instancia, conduzcan a una *reterritorialización* de la internet global y, en consecuencia, provoquen su *fragmentación* en segmentos nacionales de internet (Drake *et al.*, 2016, Mueller, 2017). Esto, a su vez, podría tener consecuencias negativas importantes

en términos económicos y políticos para los países involucrados, debido a su aislamiento digital y geográfico (Hill, 2014).

## **AUTONOMÍA ECONÓMICA Y COMPETENCIA**

Hay una segunda categoría de demandas relativas a la soberanía digital que, si bien guarda una estrecha relación, difiere de la que se centra en la autonomía del Estado. Esta categoría destaca los desafíos, importantes y con frecuencia opuestos, en relación con el entorno digital, y se centra en la autonomía de la economía nacional respecto a la tecnología extranjera y a las empresas proveedoras de servicios. Al igual que las aseveraciones de la categoría previa, las demandas centradas en la autodeterminación económica han sido incentivadas, sobre todo, por la percepción del dominio del mercado por parte de las empresas tecnológicas de Estados Unidos y, cada vez más, también de China (Steiger *et al.*, 2017, p. 11). Asimismo, las medidas e instrumentos específicos que los gobiernos implementan para compensar estos desequilibrios en la economía digital se superponen, en parte, con las medidas que buscan reforzar la seguridad de los sistemas tecnológicos y la autonomía nacional (Baums, 2016). Sin embargo, a diferencia de la primera categoría, estas medidas suelen formar parte de una estrategia nacional de política económica e industrial más amplia, cuyo objetivo es la transformación digital de sectores enteros de la economía. Como tales, afectan tanto a las industrias y sectores tradicionales (telecomunicaciones, medios de comunicación, logística) como a los nuevos sectores económicos relacionados con las tecnologías de la información, y tienen como objetivo principal promover el poder innovador de la economía nacional y fomentar la competencia local (Bria, 2015). Además, un número creciente de instrumentos se centran en el comercio digital y tratan de regular el comercio y los flujos de datos suministrados a través de las redes digitales (Burri, 2017; Ferracane, 2017).

Un magnífico ejemplo de una iniciativa que pretende reforzar la autonomía económica es Gaia-X, el servicio de nube europeo, anunciado de manera conjunta por Francia y Alemania en 2019, que aún no se ha puesto en marcha (BMW, 2020). El proyecto prevé conectar a proveedores de servicios de nube pequeños y medianos en Europa a través de un estándar compartido que les permita ofrecer una alternativa europea abierta, segura y confiable a los principales proveedores de este tipo de servicios a nivel mundial, a menudo con sede en Estados Unidos (por ejemplo, Amazon, Google, Microsoft). Ello sin dejar de cumplir con los valores y las normas de protección de datos europeos. La iniciativa ha recibido gran promoción por parte de los actores políticos como un paso importante hacia la *soberanía de datos* europea (BMBF, 2019a; Summa, 2020); otro concepto muy relacionado. Pero también ha sido criticada por ser considerado un proyecto demasiado ambicioso y puramente estatal, que no supone una verdadera innovación y que tendrá que competir por la aceptación en el mercado con proveedores más consolidados (Lumma, 2019; Mahn, 2020).

Al igual que en la categoría anterior, tanto en los países autoritarios como en los

democráticos, la meta de lograr una mayor independencia de las tecnologías extranjeras y promover el poder innovador de la industria nacional es un elemento central de los discursos sobre la soberanía digital. En los países democráticos, algunas medidas se justifican, además, por el objetivo de proteger a los consumidores a través de la oferta de servicios tecnológicos respetuosos de los derechos de las personas usuarias y las leyes y normas nacionales, como las regulaciones de protección de datos (Hill, 2014; Mauer *et al.*, 2014, p. 8). En muchas economías emergentes, como la India, las medidas propuestas también suelen ir claramente dirigidas a lo que tanto actores políticos como académicos han descrito como imperialismo digital o colonialismo digital. Ambos términos se refieren a la posición excesivamente dominante de las corporaciones tecnológicas occidentales en el Sur Global, que conduce a nuevas formas de hegemonía y explotación (Pinto, 2018; Kwet, 2019; PTI, 2019). No es de extrañar que tales demandas e iniciativas hayan sido recibidas con escepticismo y repudio por algunos países occidentales, donde los actores políticos y empresariales se han apresurado a etiquetar tales ideas y prácticas como *proteccionismo digital*, en el sentido de la “construcción de barreras o impedimentos al comercio digital” (Aaronson, 2016, p. 8; véase también Aaronson y Leblond, 2018). Sin embargo, mientras en Estados Unidos, donde la noción de soberanía digital suele tener una connotación negativa (Couture y toupin, 2019, p.2313), una gran variedad de políticas son consideradas proteccionistas en potencia [incluidas la censura, la filtración, la localización y las medidas y regulaciones relativas a la propiedad intelectual para prevenir la desinformación y proteger la privacidad], en otras regiones y países, como Europa y Canadá, se han propuesto definiciones más restringidas que dan cuenta de restricciones comerciales específicas, debido a inquietudes sobre la privacidad y las excepciones culturales (Aaronson, 2016, p.10).

## **AUTONOMÍA DE LA PERSONA USUARIA Y AUTODETERMINACIÓN INDIVIDUAL**

En los últimos años ha surgido una tercera categoría de demandas relativas a la soberanía digital. Está presente sobre todo en los discursos de los países democráticos y se destaca en el debate político sobre la soberanía digital en Alemania (Pohle, 2020a, p. 7ff.; Glasze y Dammann, en prensa, p. 13). Estas demandas, que hacen hincapié en la importancia de la autodeterminación individual, se centran en la autonomía de la ciudadanía en su papel de empleada, consumidora y usuaria de tecnologías y servicios digitales. Un aspecto interesante de esta categoría es que se aleja de una concepción de la soberanía centrada en el Estado. En lugar de considerar a la soberanía como requisito previo para ejercer autoridad en un territorio concreto, los actores la ven como la capacidad de las personas de actuar y decidir de manera consciente, deliberada e independiente. Al fortalecer estas capacidades, las personas deben quedar protegidas como consumidoras y ver reforzados sus derechos como ciudadanía democrática (Gesellschaft für Informatik, 2020; VZBV, 2014). Las demandas de las personas legisladoras y los actores de la sociedad civil, en esta categoría,

también se refieren a la soberanía de la persona usuaria y a la soberanía del consumidor digital, con lo que sustituyen el control de las personas usuarias y de la ciudadanía, que podrían estar sujetas a medidas de soberanía digital en los regímenes autoritarios, con el objetivo de fortalecer la capacidad de autodeterminación de las personas usuarias de internet en el ámbito nacional (Pohle, 2020c, p. 8ff.; SVRV, 2017).

Los medios propuestos para lograr este tipo de soberanía en la esfera digital incluyen incentivos económicos para el desarrollo de tecnologías locales y fáciles de usar, pero también la introducción de funciones técnicas que permitan un cifrado eficaz, la protección de datos y una mayor transparencia de los modelos comerciales. Además, gran parte de las medidas dirigidas a la autodeterminación individual buscan mejorar la alfabetización mediática y digital de las personas usuarias y, con ello, reforzar las competencias y la confianza de las personas usuarias y consumidoras en la esfera digital. En Alemania, por ejemplo, un fondo de innovación, de reciente creación por parte del Ministerio Federal de Educación e Investigación (el fondo “Interacción Humano-Tecnología para la Soberanía Digital”), se basa en la idea de que la alfabetización digital va más allá de tener conocimientos tecnológicos o ser competente en el uso de las herramientas digitales. Más bien, se entiende como el compromiso crítico o consciente de las personas usuarias con la tecnología y con sus propios datos (*Datenbewusstsein*, véase BMBF, 2019b).

Un aspecto interesante de esta categoría discursiva de la soberanía digital son las referencias a la soberanía tecnológica o digital de las personas usuarias por parte de activistas tecnológicos y movimientos sociales. Su perspectiva contradice una comprensión de la soberanía centrada en el Estado y, en cambio, hace hincapié en la necesidad de que las personas usuarias comprendan mejor los poderes comerciales y estatales en la esfera digital y se apropien de sus tecnologías, datos y contenidos (Couture y Toupin, 2019, p. 2315ff). Esto podría lograrse, ya sea al priorizar el software y los servicios abiertos y libres o mediante la protección de las personas usuarias contra la explotación de sus datos personales por parte de las empresas tecnológicas, a través de la protección de datos y las prácticas de encriptación (Haché, 2014, 2018; Cercy y Nitot, 2016). Aunque algunos aspectos de esta perspectiva y algunas de las medidas propuestas pueden alinearse con las demandas de autodeterminación individual que encontramos en las democracias, las creencias subyacentes son, sin embargo, diferentes. Además, es preciso evaluar con sumo cuidado las referencias y las medidas sugeridas por las personas responsables de elaborar políticas para aumentar la soberanía de las personas usuarias. En muchos casos, la ciudadanía se ve reducida a consumidora de servicios digitales, en lugar de ser valorada en su calidad de ciudadanía democrática. Sin embargo, el enfoque en la autonomía y la seguridad de las personas consumidoras podría confundir las medidas que sirven, en primer lugar, a fines económicos y de seguridad, lo que llevaría a una situación en la que los derechos fundamentales de las personas usuarias [como la privacidad o la libertad de expresión] se restringen, en lugar de hacerse valer.

## LA SOBERANÍA EN UN MUNDO INTERCONECTADO

En este ensayo se ha argumentado que quienes defienden el concepto de soberanía digital, tan popular en el discurso político y público en la actualidad, no solo han tenido que modificar algunas de sus primeras creencias sobre la gobernabilidad en un mundo interconectado, sino que la propia idea de soberanía ha cambiado a medida que ha ido cobrando relevancia. El tema ya no es la *soberanía cibernética* como un desafío no territorial a la soberanía propia del ámbito virtual de la internet. Hoy en día, la *soberanía digital* se ha convertido en un concepto mucho más amplio, que aborda no solo cuestiones de comunicación y conexión a través de la internet, sino también la transformación digital de las sociedades, que es mucho más amplia. La soberanía digital, sobre todo en Europa, se utiliza a menudo como una forma de referirse a una esfera digital ordenada, basada en valores, regulada y, por lo tanto, razonable y segura. Se asume que resuelve los multifacéticos problemas de los derechos y las libertades individuales, la seguridad colectiva e infraestructural, la exigibilidad política y legal y la competencia económica justa (Bendiek y Neyer, 2020).

Por lo general, la soberanía se ha concebido como una ley aplicable respaldada por disposiciones estructurales claras, como el monopolio estatal de la violencia. En este contexto, el Estado se concibe como un actor más o menos coherente, capaz, independiente y, por tanto, autónomo. Aunque la soberanía siempre ha sido imperfecta [su descripción como una “hipocresía organizada”, por Stephen Krasner, es célebre (Krasner, 1999)], los medios del poder soberano en el orden westfaliano han sido más bien sencillos. Pero, debido a la digitalización, la globalización y la plataformización, la situación se ha complicado. La soberanía digital de un Estado no puede reducirse a su capacidad para establecer, comunicar y hacer cumplir las leyes. Más que basarse en la representación simbólica y la capacidad organizativa del Estado, la soberanía digital tiene un carácter profundamente invasivo. En muchos casos, la idea de reforzar la soberanía digital significa no solo gestionar de forma activa las dependencias, sino también crear infraestructuras de control y (posible) manipulación. Por lo tanto, creemos que es necesario reflexionar y debatir mucho más sobre la forma de exigir a los poderes soberanos una rendición de cuentas democrática con respecto al ámbito digital. No basta con proponer la posibilidad de controlar el poder de las grandes empresas digitales al someterlas a la soberanía democrática, como han sugerido muchos gobiernos democráticos en todo el mundo. Del mismo modo, no debemos limitarnos a equiparar la soberanía (digital) con la capacidad de defender los valores liberales y democráticos, como suelen hacer los actores políticos en Europa. La soberanía digital no es un fin en sí mismo. Por el contrario, para lograr una verdadera democratización de la soberanía digital, debemos reflexionar aún más sobre el marco procedimental que permite que el poder soberano rinda cuentas y se abra a la reflexión y el control públicos.

## REFERENCIAS

- Aaronson, S. A. (2016). *The digital trade imbalance and its implications for internet governance* (Paper No. 25; Global Commission on Internet Governance). Centre for International Governance Innovation.
- Aaronson, S. A. y Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, 21(2), 245–272.  
<https://doi.org/10.1093/jiel/jgy019>
- Barbrook, R. y Cameron, A. (1996). The Californian ideology. *Science as Culture*, 6(1), 44–72. <https://doi.org/10.1080/09505439609526455>
- Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. <https://www.eff.org/cyberspace-independence>
- Baums, A. (2016). Digitale Standortpolitik in der Post-Snowden-Welt. In M. Friedrichsen y P.-J. Bisa (eds.), *Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft* (pp. 223–235). Springer VS. [https://doi.org/10.1007/978-3-658-07349-7\\_20](https://doi.org/10.1007/978-3-658-07349-7_20)
- Bendiek, A. y Neyer, J. (2020). Europas digitale Souveränität. Bedingungen und Herausforderungen internationaler politischer Handlungsfähigkeit. En M. Oswald y I. Borucki (eds.), *Demokratietheorie im Zeitalter der Frühdigitalisierung* (pp. 103–125). Springer VS.
- B.M.B.F. (2019a). “GAIA-X”: *Ein neuer Datenraum für Europa*. Ministerio Federal de Educación e Investigación.  
<https://www.bmbf.de/de/gaia-x-ein-neuer-datenraum-fuer-europa-9996.html>
- B.M.B.F. (2019b). *Mensch-Technik-Interaktion für digitale Souveränität—Mensch-Technik-Interaktion*. Ministerio Federal de Educación e Investigación.  
<https://www.technik-zum-menschen-bringen.de/foerderung/bekanntmachungen/digisou>
- BMWi. (2020). *GAIA-X: A Federated Data Infrastructure for Europe*. Ministerio Federal de Economía y Energía. <https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html>
- Bria, F. (2015). *Public policies for digital sovereignty*. Conferencia del Consorcio de la Plataforma del Cooperativismo, Nueva York.  
[https://www.academia.edu/19102224/Public\\_policies\\_for\\_digital\\_sovereignty](https://www.academia.edu/19102224/Public_policies_for_digital_sovereignty)
- Budnitsky, S. y Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, 21(5), 594–613.  
<https://doi.org/10.1177/1367549417751151>
- Burri, M. (2017). The Regulation of Data Flows through Trade Agreements. *Georgetown Journal of International Law*, 48(1), 408–448.

Cavelty, M. D. y Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review*, 15(1), 37-57.

<https://www.ingentaconnect.com/content/stair/stair/2019/00000015/00000001/art00004>

Cercy, N. y Nitot, T. (2016). *Numérique: Reprendre le contrôle*. Framasoft.

Chander, A. y Le, U. P. (2015). Data Nationalism. *Emory Law Journal*, 64(6), 677-739.

Chenou, J.-M. (2014). From cyber-libertarianism to neoliberalism: Internet exceptionalism, multi-stakeholderism, and the institutionalisation of internet governance in the 1990s. *Globalizations*, 11(2), 205-223. <https://doi.org/10.1080/14747731.2014.887387>

Christl, W. (2017). *Corporate Surveillance In Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* [Report]. Cracked Labs. <http://crackedlabs.org/en/corporate-surveillance>

Couture, S. y Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*, 21(2), 2305-2322. <https://doi.org/10.1177/1461444819865984>

Creemers, R. (2016). *The Chinese cyber-sovereignty agenda* (M. Leonard, Ed.). Consejo Europeo de Relaciones Exteriores.

Creemers, R. (2020). China's Conception of Cyber Sovereignty. En D. Broeders y B. Berg (eds.), *Governing Cyberspace: Behavior, Power and Diplomacy* (pp. 107-145). Rowman & Littlefield.

Deibert, R. J. y Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance*, 18(3), 339-361. <https://doi.org/10.1163/19426720-01803006>

DeNardis, L. (2012). Hidden Levers of Internet Control. *Information, Communication & Society*, 15(5), 720-738. <https://doi.org/10.1080/1369118X.2012.659199>

Drake, W. J., Cerf, V. G. y Kleinwächter, W. (2016). *Internet Fragmentation: An Overview* (Future of the Internet Initiative) [informe oficial]. Foro Económico Mundial. <https://www.weforum.org/reports/internet-fragmentation-an-overview>.

Ferracane, M. (2017). *Restrictions on Cross-Border Data Flows: A Taxonomy* (documento de trabajo núm. 1/2017). European Centre for International Political Economy. <https://doi.org/10.2139/ssrn.3089956>

Gesellschaft für Informatik. (2020). *Schlüsselaspekte Digitaler Souveränität* [documento de trabajo]. Gesellschaft für Informatik. [https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier\\_Digitale\\_Souveraenitaet.pdf](https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier_Digitale_Souveraenitaet.pdf)

Glasze, G. y Dammann, F. (en prensa). Von der „globalen Informationsgesellschaft“ zum „Schengenraum für Daten“ – Raumkonzepte in der Regierung der „digitalen

- Transformation“ in Deutschland. En T. Döbler, C. Pentzold, y C. Katzenbach (eds.), *Räume digitaler Kommunikation (forthcoming)*. Halem.
- Glen, C. M. (2014). Internet Governance: Territorializing Cyberspace? *Politics & Policy*, 5(42), 635–657. <https://doi.org/10.1111/polp.12093>
- Goldsmith, J. y Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. Oxford University Press.
- Grimm, D. (2015). *Sovereignty: The Origin and Future of a Political and Legal Concept*. Columbia University Press.
- Haché, A. (2014). *La Souveraineté technologique (Tomo 1)*. Dossier ritimo. <https://www.ritimo.org/La-Souverainete-technologique>.
- Haché, A. (2018). *La Souveraineté technologique (Tomo 2)*. Dossier ritimo. <https://www.ritimo.org/La-Souverainete-Technologique-Volume2>.
- Hansen, L. y Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175. <https://doi.org/10.1111/j.1468-2478.2009.00572.x>
- Hill, J. F. (2014). The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. *Policymakers and Industry Leaders*. *Lawfare Research Paper Series*, 2(3), 1–41.
- Hindman, M. (2018). *The Internet trap: How the digital economy builds monopolies and undermines democracy*. Princeton University Press. <https://doi.org/10.23943/princeton/9780691159263.001.0001>
- Hintz, A. y Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review*, 5(3). <https://doi.org/10.14763/2016.3.424>
- Hobbs, C. (Ed.). (2020). *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*. Consejo Europeo de Relaciones Exteriores. [https://ecfr.eu/publication/europe\\_digital\\_sovereignty\\_rulemaker\\_superpower\\_age\\_us\\_china\\_rivalry/](https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/).
- Hofmann, J. (2016). Multi-stakeholderism in Internet governance: Putting a fiction into practice. *Journal of Cyber Policy*, 1(1), 29–49. <https://doi.org/10.1080/23738871.2016.1158303>
- Jiang, M. (2010). Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review of International Affairs*, 30(3), 71–89. <https://doi.org/10.1353/sais.2010.0006>
- Johnson, D. R. y Post, D. G. (1996). Law and Borders—The Rise of Law in Cyberspace. *Stanford Law Review*, 48(5), 1367–1402. <https://doi.org/10.2307/1229390>



- Katz, J. (1997). Birth of a Digital Nation. In *Wired*.  
<https://www.wired.com/1997/04/netizen-3/>.
- Keller, C. I. (2019). *Exception and Harmonization: Three Theoretical Debates on Internet Regulation* (2020(2); HIIG Discussion Paper Series). Instituto Alexander von Humboldt para la Internet y la Sociedad. <https://doi.org/10.2139/ssrn.3572763>
- Klein, H. (2002). ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy. *The Information Society*, 18(3), 193–207.  
<https://doi.org/10.1080/01972240290074959>
- Kleinhans, J.-P. (13 de noviembre de 2013). Schengen-Routing, DE-CIX und die Bedenken der Balkanisierung des Internets. *Netzpolitik*.  
<https://netzpolitik.org/2013/schengen-routing-de-cix-und-die-bedenken-der-balkanisierung-d-es-internets/>.
- Krasner, S. D. (1999). *Sovereignty: Organized Hypocrisy*. Princeton.  
<https://doi.org/10.2307/j.ctt7s9d5>
- Kukutai, T. y Taylor, J. (2016). *Indigenous data sovereignty: Toward an agenda*. Anu Press.
- Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3–26. <https://doi.org/10.1177/0306396818823172>
- Lambach, D. (2019). The Territorialization of Cyberspace. *International Studies Review*, 22(3), 482–506. <https://doi.org/10.1093/isr/viz022>
- Lumma, N. (2019). Die „europäische Cloud“ ist eine Kopfgeburt, die nicht überleben wird. *Gründerszene Magazin*.  
<https://www.gruenderszene.de/technologie/gaia-x-europaeische-cloud-wird-scheitern>
- MacCormick, N. (1999). *Questioning Sovereignty: Law, State, and Nation in the European Commonwealth*. Oxford University Press.
- Mahn, J. (2020). Die digitale europäische Idee. Gaia-X: Wie Europa in der Cloud unabhängig werden soll. *Magazin für Computertechnik*, 14.  
<https://www.heise.de/select/ct/2020/14/2015610312088025860>
- Malcolm, J. (2008). *Multi-stakeholder governance and the Internet Governance Forum*. Terminus Press.
- Maurer, T., Morgus, R., Skierka, I. y Hohmann, M. (2014). *Technological Sovereignty: Missing the Point?* [Paper]. New America; Instituto de Política Pública Global.  
[http://www.digitaldebates.org/fileadmin/media/cyber/Maurer-et-al\\_2014\\_Tech-Sovereignty-Europe.pdf](http://www.digitaldebates.org/fileadmin/media/cyber/Maurer-et-al_2014_Tech-Sovereignty-Europe.pdf)
- Mazzucato, M. (2011). *The entrepreneurial state*. Demos.

[http://oro.open.ac.uk/30159/1/Entrepreneurial\\_State\\_-\\_web.pdf](http://oro.open.ac.uk/30159/1/Entrepreneurial_State_-_web.pdf)

Möllers, N. (2020). Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values*, 46(1), 112-138. <https://doi.org/10.1177/0162243920904436>

Mueller, M. (2017). *Will the internet fragment?: Sovereignty, globalization and cyberspace*. Polity.

Mueller, M. (2020). Against Sovereignty in Cyberspace. *International Studies Review*, 22(4), 779-801. <https://doi.org/10.1093/isr/viz044>

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press. <https://doi.org/10.7551/mitpress/9780262014595.001.0001>

Musiani, F. y Pohle, J. (2014). NETmundial: Only a Landmark Event If “Digital Cold War” Rhetoric Abandoned. *Internet Policy Review*, 3(1). <https://doi.org/10.14763/2014.1.251>

Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology*, 7(2), 61-73. <https://doi.org/10.1007/s10676-005-4582-3>

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, 91(1), 111-130. <https://doi.org/10.1111/1468-2346.12189>

Panday, J. y Malcolm, J. (2018). The Political Economy of Data Localization. *Partecipazione e conflitto*, 11(2), 511-527. <https://doi.org/10.1285/i20356609v11i2p511>

Pasquale, F. (2016). Two narratives of platform capitalism. *Yale Law & Policy Review*, 35(1), 309-321. <https://ylpr.yale.edu/two-narratives-platform-capitalism>

Peuker, E. (2020). *Verfassungswandel durch Digitalisierung*. Mohr Siebeck.

Pinto, R. Á. (2018). Digital Sovereignty or Digital Colonialism? New tensions of privacy, security and national policies. *Sur*, 15(27), 15-27. <https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/>

Pistor, K. (2020). Statehood in the digital age. *Constellations*, 27(1), 3-18. <https://doi.org/10.1111/1467-8675.12475>

Pohle, J. (2020a). Digitale Souveränität. En T. Klenk, F. Nullmeier y G. Wewer (eds.), *Handbuch Digitalisierung in Staat und Verwaltung* (pp. 1-13). Springer. [https://doi.org/10.1007/978-3-658-23669-4\\_21-1](https://doi.org/10.1007/978-3-658-23669-4_21-1)

Pohle, J. (2020b). *Digital sovereignty - a new key concept of digital policy in Germany and Europe* [informe de investigación]. Fundación Konrad Adenauer. <https://www.kas.de/en/single-title/-/content/digital-sovereignty>

Pohle, J. y Thiel, T. (2019). Digitale Vernetzung und Souveränität: Genealogie eines

Spannungsverhältnisses. En I. Borucki y W. J. Schünemann (eds.), *Internet und Staat: Perspektiven auf eine komplizierte Beziehung* (pp. 57–80). Nomos.

Post, D. G. (2007). Governing Cyberspace: Law. *Santa Clara High Technology Law Journal*, 24(4), 883–913. <https://digitalcommons.law.scu.edu/chtlj/vol24/iss4/5/>

P.T.I. (2019, January 20). India's data must be controlled by Indians: Mukesh Ambani. *mint*. <https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyI/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html>

Raymond, M. y DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory*, 7(3), 572–616. <https://doi.org/10.1017/S1752971915000081>

Selby, J. (2017). Data localization laws: Trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology*, 25(3), 213–232. <https://doi.org/10.1093/ijlit/eax010>

Srnicek, N. (2017). The challenges of platform capitalism. Understanding the logic of a new business model. *Juncture*, 23(4), 254–257. <https://doi.org/10.1111/newe.12023>

Staab, P. (2019). *Digitaler Kapitalismus: Markt und Herrschaft in der Ökonomie der Unknappheit*. Suhrkamp.

Stadnik, I. (2019). *Internet Governance in Russia-Sovereign Basics for Independent Runet*. 47ª Conferencia de Investigación sobre Comunicación, Información y Política de Internet (TPRC47). <https://doi.org/10.2139/ssrn.3421984>

Steiger, S., Schünemann, W. J. y Dimmroth, K. (2017). Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany. *Media and Communication*, 5(1), 7–16. <https://doi.org/10.17645/mac.v5i1.814>

Summa, H. A. (2020, March). How GAIA-X is Paving the Way to European Data Sovereignty. *Dotmagazine*. <https://www.dotmagazine.online/issues/cloud-and-orientation/build-your-own-internet-gaia-x>

SVRV (Consejo Consultivo en materia de Consumo). (2017). *Digitale Souveränität*. Sachverständigenrat für Verbraucherfragen.

Tambiana, M. (2020). *Digital sovereignty for Europe* (EPRS Ideas Papers, pp. 1–12) [Informe]. Servicio de Investigación del Parlamento Europeo (EPRS). [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

The German Presidency of the EU Council. (2020). *Together for Europe's recovery: Programme for Germany's Presidency of the Council of the European Union (1 de julio al 31 de diciembre de 2020)*. Consejo de la Unión Europea.

- Thiel, T. (2014). Internet und Souveränität. En C. Volk & F. Kuntz (eds.), *Der Begriff der Souveränität in der transnationalen Konstellation* (pp. 215-239). Nomos.
- Thiel, T. (2019). Souveränität: Dynamisierung und Kontestation in der digitalen Konstellation. En J. Hofmann, N. Kersting, C. Ritzi y W. J. Schünemann (eds.), *Politik in der digitalen Gesellschaft: Zentrale Problemfelder und Forschungsperspektiven* (pp. 47-61). Transcripción.
- Tréguer, F. (2017). Intelligence reform and the Snowden paradox: The case of France. *Media and Communication*, 5(1), 17-28. <https://doi.org/10.17645/mac.v5i1.821>
- Tréguer, F. (2018). *US Technology Companies and State Surveillance in the Post-Snowden Context: Between Cooperation and Resistance*. (Informe de investigación núm. 5; entregables de UTIC). SciencesPo. <https://halshs.archives-ouvertes.fr/halshs-01865140>
- Turner, F. (2006). *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. University of Chicago Press.
- Van Dijck, J. (2020). Governing digital societies: Private platforms, public values. *Computer Law & Security Review*, 36. <https://doi.org/10.1016/j.clsr.2019.105377>
- Voelsen, D. (2019a). *5G, Huawei und die Sicherheit unserer Kommunikationsnetze – Handlungsoptionen für die deutsche Politik* (informe núm. 5; SWP-Aktuell). Fundación Ciencia y Política. Instituto Alemán de Asuntos Internacionales y de Seguridad. <https://doi.org/10.18449/2019A05>
- Voelsen, D. (2019b). *Cracks in the internet's foundation: The future of the internet's infrastructure and global internet governance* (Informe de investigación núm. 14). Stiftung Wissenschaft und Politik. Instituto Alemán de Asuntos Internacionales y de Seguridad. <https://doi.org/10.18449/2019RP14>
- VZBV (Federación de Organizaciones de Consumidores de Alemania). (2014). *Digitalisierung: Neue Herausforderungen für Politik und Verbraucher* [Comunicado de prensa]. <https://www.vzbv.de/pressemitteilung/digitalisierung-neue-herausforderungen-fuer-politik-und-verbraucher>
- Wittpahl, V. (ed.). (2017). *Digitale Souveränität: Bürger, Unternehmen, Staat*. Springer Vieweg. <https://doi.org/10.1007/978-3-662-55796-9>
- Zeng, J., Stevens, T. y Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". *Politics & Policy*, 45(3), 432-464. <https://doi.org/10.1111/polp.12202>
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

## Acerca de los Autores

**Dra. Julia Pohle:** es investigadora senior en el grupo de investigación “Políticas de digitalización” en el Berlin Social Science Center (WZB). Su investigación y publicaciones se centran en las políticas de Internet global y nacional, la gobernanza de Internet y la historia de la política de comunicación global. La Dra. Pohle tiene un doctorado en Estudios de la Comunicación de la Vrije Universiteit Brussel y una maestría en Estudios Culturales, Filosofía e Informática de la Humboldt-Universität zu Berlin. Es ex-alumna del Programa Global Governance Futures y anteriormente trabajó en la sede de la UNESCO en París y en SMIT, el Centro de Estudios en Medios, Innovación y Tecnología, en Bruselas. Entre otros roles académicos, Julia actualmente se desempeña como copresidenta de la Sección de Política y Tecnología de la Comunicación (CPT) de la Asociación Internacional para la Investigación de Medios y Comunicación (IAMCR), en el Consejo Editorial de Medios y Comunicación, y en el Comité Directivo del Foro de Gobernanza de Internet de Alemania (IGF-D). Julia se unió al equipo editorial de Internet Policy Review en 2020.

**Dr. Thorsten Thiel:** es investigador senior en ciencias políticas y director del “Grupo de Investigación 12: Democracia y Digitalización” en el Instituto Weizenbaum. Antes de unirse al Instituto Weizenbaum, fue coordinador de la Red de Investigación Leibniz “Crisis de un mundo globalizado” (2013-2017) y becario postdoctoral en el Grupo de Excelencia de Frankfurt “La formación de órdenes normativos” (2010-2013). En el semestre de invierno 2015/2016, representó la Cátedra de Teoría Política e Historia de las Ideas en la Universidad de Trier. Thorsten Thiel se doctoró como miembro del grupo de formación en investigación “Constitución más allá del Estado” (2006-2010), escribiendo una tesis sobre el discurso de la democracia en la Unión Europea.

## Notas

---

- <sup>†1</sup> En las últimas décadas ha habido muchos intentos por extender el concepto de soberanía a otras entidades políticas distintas de los Estados, como las instituciones supranacionales y subnacionales o los pueblos indígenas (por ejemplo, Kukutai y Taylor, 2016). Estos usos derivados del término suelen equiparar a la soberanía con la autonomía y, por tanto, restan importancia a los aspectos de control y legitimación. Aunque creemos que estas comprensiones más amplias son importantes y pueden explicar, en parte, la popularidad del concepto de soberanía digital, nos ceñimos a una comprensión política más tradicional del término.

Una variante del excepcionalismo cibernético, menos aguda pero aún profundamente escéptica con respecto al Estado, es la independencia en red, una corriente discursiva que se encuentra con frecuencia en el discurso jurídico y que se alinea con el discurso sobre la globalización y la gobernanza mundial. Sostiene que la soberanía del Estado está en declive debido a la fragmentación disfuncional de un orden estático ligado a territorios geográficos (Johnson y Post, 1996).

La sistematización propuesta es el resultado de un análisis cualitativo de una selección de documentos relativos a las políticas que aplican la palabra soberanía digital y términos similares (como soberanía tecnológica, resiliencia digital, autonomía digital, etc.), que no pretende ser exhaustivo. Utilizamos ejemplos seleccionados de textos de política y medidas propuestas para ilustrar los diferentes niveles de las demandas de soberanía digital.