

Explorando la Soberanía Digital y su Impacto en Internet



Diciembre de 2022

Resumen ejecutivo

A principios de este año, una amplia alianza de ciudadanos en Brasil publicó una Carta de soberanía digital¹. En ella, lamentaban la extracción y manipulación desenfrenada de datos locales por parte de las grandes empresas tecnológicas e instaban al gobierno a apoyar tecnologías interoperables y abiertas, y centros de datos para uso común.

Al otro lado del mundo, en otro país vasto y con una enorme población, el gobierno de la India dio instrucciones a todos los proveedores de servicios para que retengan información sobre sus usuarios durante cinco años y para sincronizar los relojes de sus sistemas con una sola fuente de tiempo: los propios servidores del gobierno. Estas son disposiciones en las nuevas instrucciones de ciberseguridad del Equipo de respuesta a emergencias informáticas de la India (CERT-In)², un intento de aumentar los informes de incidentes de seguridad y proteger la infraestructura digital del país.

Ambos pronunciamientos proyectan una visión de soberanía en el ciberespacio, pero la forma en que quieren llegar a esa visión, y los actores que la impulsan, no podrían ser más diferentes.

Internet Society comenzó este estudio con el propósito de desarrollar una postura acerca de la soberanía digital. Lejos de un ideal monolítico, lo que encontramos fue una noción amplia y poco definida que diferentes grupos interpretan y aplican de manera diversa en todo el mundo. Estos grupos incluyen a gobiernos que desean controlar cómo se ejecutan las operaciones y los recursos de Internet; empresas locales que denuncian el dominio de las plataformas tecnológicas extranjeras; comunidades indígenas que quieren salvaguardar el conocimiento y los recursos locales; e individuos que quieren afirmar su autonomía sobre sus interacciones con dispositivos, plataformas y cómo administran sus datos.

1 "Programa de Emergencia para una soberanía digital", <https://cartasoberaniadigital.lablivre.wiki.br/carta/>

2 CERT-In. Equipo de Respuesta a Emergencias Informáticas de la India (CERT-In) del Ministerio de Electrónica y Tecnología de la Información (MeitY) del Gobierno de la India, 2022. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf



Este informe busca comprender los diferentes enfoques que existen, reconociendo que cada uno tendrá un impacto diferente en Internet, y proponer un marco para analizar estos efectos. Con este fin, no busca solidificar ni respaldar ninguna definición o posición única sobre la soberanía digital.

Este estudio reduce su alcance para examinar las políticas impulsadas por gobiernos que se han apropiado de la soberanía digital explícitamente. Los agrupa según sus objetivos declarados y evalúa su impacto en la capa técnica de Internet. Nuestro objetivo es brindar una guía matizada para determinar si las políticas de soberanía digital pueden llevarnos desde una Internet que beneficia a todos, hacia una serie de redes fragmentadas y cerradas donde se pierden las oportunidades que surgen de la conexión global.³

En primer lugar, presenta un resumen de las tendencias de las políticas en Asia-Pacífico, África y Europa, incluida Rusia, luego agrupa las políticas y medidas en función de (a) sus objetivos y (b) los actores empoderados para lograr sus metas. Esta categorización destacó dos enfoques diferentes de la soberanía digital:

1. Las políticas que reivindican **la seguridad nacional a través de un mayor control estatal** pretenden hacer cumplir las leyes en el ámbito digital para reforzar la seguridad nacional. Este enfoque se basa en actores estatales autorizados para centralizar el control de las operaciones de las redes, concentrar el poder en el Estado y limitar la autoridad de los operadores. Este tipo de soberanía digital presenta riesgos significativos para los valores y características centrales de Internet y podría conducir a su fragmentación directa.
2. Las políticas que buscan **la autodeterminación económica impulsada por actores económicos** quieren fortalecer a los actores en la economía nacional y en menor medida, garantizar la resiliencia de la cadena de suministro. Estas medidas no interfieren intencionalmente con las operaciones de las redes de Internet. En cambio, intentan impulsar las economías digitales locales a través de un campo de juego nivelado y la reducción de las barreras de entrada al hacer que los datos y otros recursos sean más accesibles. Algunas de las políticas podrían ser proteccionistas y pueden interferir con las operaciones de las redes. En general, buscan aumentar las

3 Si bien apreciamos el discurso académico sobre la soberanía como un concepto político, este informe se enfoca en las consecuencias de la implementación práctica de esta noción en Internet, específicamente, cómo las políticas digitales impulsadas por el estado están impactando la base técnica y la evolución de Internet.

oportunidades creadas por una red global y, sociedades y economías conectadas y pueden mejorar las condiciones para que los actores locales saquen provecho de Internet.

Este informe demuestra que las políticas de soberanía digital pueden afectar negativamente el funcionamiento de Internet y, lo que es más importante, nuestra capacidad para hacer uso de Internet. Para minimizar el riesgo de interrumpir las operaciones de este recurso global del que dependen cada vez más nuestras economías y sociedades, recomendamos encarecidamente a los formuladores de políticas que realicen una Evaluación del impacto en Internet como parte de sus procesos de desarrollo de políticas, especialmente en lo que respecta a las medidas que buscan abordar los desafíos en el entorno digital.

Nuestro análisis inicial se centra en tres regiones, pero reconoce que la soberanía digital, ya sea que se declare implícita o explícitamente, está ganando terreno en las agendas políticas de todo el mundo. Los estudios posteriores sobre este asunto pueden beneficiarse del uso de este marco y el kit de herramientas del Modo Internet de interconectarse, para evaluar el efecto que las políticas de soberanía digital pueden tener en la Internet global, independientemente de dónde aparezcan.

Índice

Resumen ejecutivo.....	1
I. Introducción: ¿Qué es la soberanía digital?	5
1.1 El Concepto de soberanía que conocemos	5
1.2 Objetivo de este informe.....	7
II. Tendencias regionales en la soberanía digital	7
2.1 Asia-Pacífico.....	8
2.2 África.....	10
2.3 Europa, incluida Rusia.....	11
III. Objetivos y resultados: Enfoques de la soberanía digital.....	12
3.1 Cuatro objetivos principales de política.....	12
3.2 Actores empoderados para lograr los objetivos de la política.....	13
IV. Enfoques comunes de la soberanía digital y su impacto en Internet	13
4.1 Enfoque 1: Seguridad nacional impulsada por un aumento del control estatal	14
4.2 Enfoque 2: Autodeterminación económica impulsada por actores económicos.....	18
4.3 Otros enfoque de la soberanía digital	20
V. Conclusión.....	21
Apéndice I — Tendencias regionales de la soberanía digital	23
A. Asia-Pacífico.....	23
B. África.....	26
C. Europa, incluida Rusia.....	27
Apéndice II: El Modo Internet de interconectarse	33
Apéndice III: Metodología de investigación para los tipos de soberanía digital	36
Anexo IV: Cuadros de Políticas y propuestas analizadas.....	39

I. Introducción: ¿Qué es la soberanía digital?

La noción de “soberanía digital” se asocia históricamente con los intentos de los gobiernos no democráticos de vigilar las operaciones y los recursos de Internet dentro de sus fronteras.⁴ En los debates sobre políticas internacionales, el concepto se ha utilizado para desafiar los enfoques de gobernanza de Internet existentes que se basan en procesos descentralizados y de múltiples partes interesadas⁵.

Hoy en día, la “soberanía digital” se usa más ampliamente en contextos variables en todo el mundo y con diferentes fines.

Puede incluir intervenciones políticas para darle a individuos y grupos más control sobre la información, pero también medidas que dan a los ministerios de justicia e interior control directo sobre el tráfico diario de Internet. Muchas de estas políticas cubren diferentes facetas del dominio digital; este estudio se enfoca solo en aquellas que pueden afectar el funcionamiento de Internet.

Las intervenciones políticas que caen bajo el paraguas de la soberanía digital pueden afectar a Internet, pero el término en sí mismo nos dice poco sobre cuál es el impacto. Debido a esta ambigüedad, Internet Society no adopta una postura sobre la soberanía digital como concepto; el objetivo de este informe es evaluar cómo las diversas políticas que la establecen pueden interactuar con Internet.

1.1 El concepto de soberanía que conocemos

Las visiones de la soberanía digital varían significativamente debido a las diferentes interpretaciones del concepto mismo de soberanía. La soberanía invoca ideas de autoridad y control, tanto a nivel individual como estatal, y estas ideas están fuertemente influenciadas por la historia, la cultura y el contexto. Un aspecto de la soberanía es la capacidad del estado para ejercer el poder y control sobre los recursos y las personas en un territorio

4 Adam Segal, “El régimen alternativo de gobernanza cibernética de China”, Consejo de Relaciones Exteriores, 13 de marzo de 2020 https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf

5 Julien Nocetti, “Contest and conquest: Russia and global internet governance.” *International Affairs* 91.1 (2015): 111-130. Milton L. Mueller, ‘China and Global Internet Governance: A Tiger by the Tail’, en Ronald Deibert y otros (eds), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (Cambridge, MA, 2011; ed. en línea, Beca de prensa del MIT en línea, 22 de agosto de 2013)

determinado. En los debates sobre la soberanía digital, esto se extiende a la capacidad de los estados para garantizar que sus leyes se obedezcan en el ámbito digital y para limitar la influencia de los actores externos, incluido el dominio del mercado por parte de empresas extranjeras y su influencia en los asuntos nacionales.

La soberanía también puede entenderse en relación con otros Estados, como un asunto de independencia de las presiones o influencias externas, y en el contexto nacional como una afirmación de la legitimidad política y el Estado de derecho. El reconocimiento de la soberanía de un estado por parte de otros estados conforma la base del derecho internacional y de los tratados y acuerdos que se relacionan con él. En el contexto de la soberanía digital, esta perspectiva centrada en el exterior puede traducirse en preocupaciones sobre la autodeterminación y la legitimidad de la participación de actores no estatales en los procesos de gobernanza.

Finalmente, la soberanía también se invoca para expresar la capacidad de los individuos y comunidades culturalmente distintas, para actuar con un grado razonable de autonomía y tomar decisiones de manera independiente. Esta visión implica que la legitimidad para gobernar proviene del consentimiento de los gobernados y, en consecuencia, del derecho de autodeterminación del individuo o del grupo. Como resultado, algunas cuestiones de la soberanía digital se centran en los derechos de los ciudadanos a la privacidad y la libertad de expresión en el espacio digital, particularmente en relación con el control de sus datos. (En este informe no se cubren la "Identidad auto-soberana" o las formas descentralizadas, no dependientes de la plataforma para que las personas hagan valer su identificación personal en la web).

Para agregar a estas interpretaciones, la soberanía digital a menudo se usa de manera superpuesta e intercambiable con expresiones similares: "soberanía tecnológica", "soberanía de la información", "soberanía cibernética", "soberanía de Internet" y "soberanía de datos".

El término se popularizó por primera vez en declaraciones del gobierno de la República Popular China hace casi veinte años.⁶ Más recientemente, ha sido utilizado por personas del Sur Global para articular una respuesta a la creciente consolidación y poder corporativo en Internet; en

6 Ministerio de Relaciones Exteriores de la República Popular China, "Observaciones de Su Excelencia Xi Jinping, presidente de la República Popular China en la ceremonia de apertura de la Segunda Conferencia Mundial de Internet", 16 de diciembre de 2015, https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

6 China.org.cn, "Full Text: International Strategy of Cooperation on Cyberspace", 7 de marzo de 2017, http://www.china.org.cn/chinese/2017-03/07/content_40424606_2.htm.

este contexto, la soberanía digital es una forma de contrarrestar el “colonialismo digital”⁷ del Norte Global.

1.2 Objetivo de este informe

Este informe no tiene como objetivo proporcionar una descripción definitiva de la soberanía digital, ni investigar los matices de su uso en el discurso político, sino aceptar que estas variaciones existen y analizar cómo las diferentes interpretaciones de la soberanía digital pueden tener impactos muy diferentes en la base técnica Internet.

Primero, resume las tendencias recientes en Asia-Pacífico, África y Europa (incluida Rusia), las regiones donde la soberanía digital se ha manifestado más explícitamente en las políticas públicas y la retórica gubernamental. Luego describe nuestra metodología para analizar medidas políticas relevantes y los principales tipos de políticas que observamos. Evaluamos estos tipos utilizando el **kit de herramientas de Evaluación del impacto en Internet**⁸ de Internet Society y los conocimientos de las tendencias regionales, para determinar los diferentes impactos de las diferentes políticas de soberanía digital en el **Modo Internet de interconectarse**⁹ y las características clave que permiten la existencia de una Internet abierta, conectada globalmente, segura y confiable.

II. Tendencias regionales en la soberanía digital

Este informe muestra políticas gubernamentales en tres regiones que han defendido abiertamente la soberanía digital.¹⁰

No existe una narrativa única que describa las políticas de soberanía digital dentro de las regiones o a nivel mundial.

7 Julia Pohle y Thorstein Thiel. “Digital sovereignty”. Revisión de la política de Internet, 5 de diciembre de 2020, <https://doi.org/10.14763/2020.4.15321>

8 The Internet Society, “Internet Impact Assessment Toolkit”, <https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/>

9 Internet Society, “The Internet Way of Networking: Championing a Thriving Internet for Everyone”, <https://www.internetsociety.org/action-plan/2022/internet-way-of-networking/>

10 Si bien el discurso público sobre la soberanía digital está formado por múltiples partes interesadas, incluidas la academia y la sociedad civil, este informe se centra en las políticas que los propios gobiernos han introducido con la intención explícita y la proclama de promover su soberanía sobre una multitud de aspectos relacionados con Internet

Esto refleja las diferentes interpretaciones y usos del término, y los muchos objetivos y, a veces, contradictorios de las políticas introducidas para promover la soberanía digital.

Para nuestro análisis, seleccionamos leyes nacionales, propuestas de políticas, documentos de estrategia y otra evidencia relacionada con políticas públicas que mencionaran¹¹ explícitamente la soberanía digital, o una variación de ella, en el texto de la política, o que se introdujeran o publicitaran de una manera que resaltara el término. Si bien encontramos muchas políticas en todo el mundo que pueden estar persiguiendo la soberanía digital, este informe excluye las políticas que no lo establecieron claramente como un objetivo. Esto mitiga el riesgo de atribuir falsamente soberanía digital a una política que puede tener otros motivos.

Los pronunciamientos y las disposiciones legales del gobierno se tomaron al pie de la letra, es decir, los analizamos en función de sus objetivos declarados. En el Apéndice I se incluye información más detallada acerca de políticas y propuestas en cada región.

2.1 Asia-Pacífico

Los principales impulsores de las medidas de soberanía digital en los países que cubrimos (Australia, China, India y Vietnam) son proteger la seguridad nacional, los ciudadanos y la estabilidad social; y el proteccionismo económico para impulsar la industria nacional. Otras motivaciones incluyen salvaguardar las normas y valores sociales y culturales (tal como los define el Estado) y ayudar a las personas a controlar sus datos.

China es pionera a nivel regional y mundial en la definición, implementación y exportación de un enfoque de soberanía digital centrado en el Estado, caracterizado por un mayor control estatal de Internet y la localización de datos. Otros gobiernos, por ejemplo, Vietnam, parecen sentirse atraídos por este modelo y por las oportunidades para una mayor inversión en la capacidad estatal y la economía que ofrece la Iniciativa de la Franja y la Ruta de China.

China fue uno de los primeros países en articular el concepto de soberanía digital. En 2015, el presidente de China, Xi Jinping, definió la soberanía digital como el derecho de cada Estado nación a elegir su propio camino de ciberdesarrollo y su propio modelo de regulación y de políticas de Internet, sin interferencias de otros países.¹² Inusualmente, la Ley de Seguridad de Datos de China (2021), que tiene como objetivo salvaguardar los "intereses de soberanía, seguridad y desarrollo del Estado", afirma el alcance extraterritorial, asignando responsabilidad

11 En aras de la brevedad, usamos el término "políticas" para abarcar todas estas medidas y comunicaciones.

12 Ministerio de Relaciones Exteriores de la República Popular China, "Observaciones de Su Excelencia Xi Jinping, presidente de la República Popular China en la ceremonia de apertura de la Segunda Conferencia Mundial de Internet", 16 de diciembre de 2015, https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

legal a las entidades que violan las leyes e intereses de China en el curso del procesamiento de datos en el extranjero.¹³

China también ha puesto en práctica la soberanía digital a través de regímenes de localización de datos. Sus Reglamentos de nombres de dominio de Internet de 2017¹⁴ respaldan la creciente tendencia hacia la localización; específicamente, reglas que requieren que los operadores de servidores raíz y los registros y registradores de nombres de dominio tengan su sede en el país.¹⁵

El control estatal también se considera una forma de impulsar la economía digital nacional y brindar un trato preferencial a las empresas chinas.¹⁶

La Estrategia de Ciberseguridad 2020 de Australia tiene como objetivo estimular "nuevas empresas y capacidades cibernéticas australianas soberanas" y "promover la innovación en la investigación y el¹⁷ desarrollo¹⁸ de la seguridad cibernética soberana", pero el panorama general es un esfuerzo por equilibrar los intereses de seguridad nacional con una agenda comercial liberalizada. Australia aún tiene que exigir la localización de datos: su estrategia de alojamiento nacional no impone la propiedad y el control nacional o la localización de datos gubernamentales y se modificó recientemente para que las empresas con sede y propiedad no australianas puedan calificar.¹⁹

India quiere aumentar el poder estatal y el acceso a los datos, pero considera los intereses económicos, más que puramente de seguridad. Su proyecto de ley de localización de datos se ha archivado recientemente, y el enfoque del gobierno se enmarca en términos generales como

13 Congreso Nacional del Pueblo de la República Popular de China, "Data Security Law of the People's Republic of China", 10 de junio de 2021, <http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml>.

14 Centro de información de la red de Internet de China, "Internet Domain Name Regulations", 26 de octubre de 2017, https://www.cnnic.com.cn/PublicS/fwzxxqzcfq/201710/t20171026_69608.htm.

15 Rogier Creemers, "China's Approach to Cyber Sovereignty," Konrad-Adenauer-Stiftung, 2020, <https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537>.

16 Jane Li, "Beijing has a new legal architecture for sweeping control over user data," Quartz, 30 August 2021, <https://qz.com/2051268/china-aims-to-control-but-also-unleash-the-economic-power-of-data/>; and Rogier Creemers, "China's Approach to Cyber Sovereignty," Konrad-Adenauer-Stiftung, 2020, <https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537>.

17 Australia está considerando un régimen de localización de datos. Véase Justin Hendry, "Tech giants rally against data localisation in Australia," InnovationAus.com, 7 de septiembre de 2022, <https://www.innovationaus.com/tech-giants-rally-against-data-localisation-in-australia/>.

18 Gobierno de Australia, "Australia's Cyber Security Strategy 2020", <https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf>.

19 "Doble centro de datos estratégico certificado" de Joseph Brookes, InnovationAus.com, 20 de agosto de 2021, <https://www.innovationaus.com/certified-strategic-data-centres-double/>.

la protección de la infraestructura y los datos críticos a raíz de las filtraciones de datos y el refuerzo de la capacidad de alojamiento y la economía digital.

2.2 África

El concepto de soberanía digital en África es relativamente reciente, y va ganando importancia y uso en los últimos cinco años.

El discurso sobre la soberanía digital está moldeado por la historia colonial de África, en el contexto de la actual distribución desigual de la riqueza y el poder.

Muchos espacios digitales de los países africanos siguen dependiendo en gran medida de las empresas extranjeras, la mayoría occidentales, pero más recientemente también de China, y los países africanos tienen poco control sobre los datos y la infraestructura de la que dependen, y no se están beneficiando económicamente como se esperaba.²⁰

La soberanía digital, de la forma como la utilizan los gobiernos africanos, suele enmarcarse como una extensión de la soberanía nacional y tiene raíces firmes en la concepción política de la soberanía promovida por China.²¹ Hay relativamente pocos marcos políticos y reglamentarios o decisiones sobre soberanía digital en los 54 países de la región y, hasta el momento, la idea tiende a articularse a través de declaraciones políticas. Las políticas que lo hacen, como la Estrategia de Transformación Digital para África de la Unión Africana, el borrador de la política de Datos y Nube²² de Sudáfrica y la Política de Revolución de Datos²³ de Ruanda, enfatizan la autodeterminación económica al garantizar la propiedad local y el control sobre los datos generados localmente.

Existe una tendencia creciente a replicar el modelo de gobernanza de datos chino que requiere que todos los servidores estén ubicados dentro de las fronteras de un país, lo que brinda al

20 Centro de Estudios África-China de la Universidad de Johannesburgo, "Africa's digital sovereignty a timely and relevant debate" de David Monyae, 28 de septiembre de 2021 <https://www.uj.ac.za/news/africas-digital-sovereignty-a-timely-and-relevant-debate/>

21 Monyae, 2021

21 Unión Africana, "The Digital Transformation Strategy for Africa (2020-2030)"

22 Gobierno de Sudáfrica, Departamento de Comunicaciones y Tecnologías Digitales, "Invitation to Submit Written Submissions on the Proposed National Data and Cloud Policy", https://www.gov.za/sites/default/files/gcis_document/202104/44389qon206.pdf

23 "Rwanda National Data revolution and Big data", 2017 <http://statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data>

estado un acceso más fácil a la información. Los gobiernos de Nigeria y Senegal vinculan cada vez más la soberanía digital con la protección o el aumento del papel del Estado. Los gobiernos también buscan abordar sus propias preocupaciones sobre el control político y los beneficios económicos de Internet que fluyen fuera de sus países.

2.3 Europa, incluida Rusia

La región europea es el hogar de la Unión Europea (UE) y la Federación Rusa, dos potencias líderes con visiones distintas para el futuro de Internet. Los países o entidades analizados ejercen influencia internacional y han articulado e implementado una visión de soberanía digital. En la región se identificaron dos campos principales.

El primer campo, la Unión Europea y sus estados miembros, Francia, Alemania e Italia, enmarcan la soberanía digital principalmente en el contexto de la competitividad económica, el desarrollo de la industria local y la protección contra los ciberataques.

La soberanía económica puede significar reducir las dependencias de la cadena de suministro para que la infraestructura clave no dependa demasiado de los proveedores extranjeros y fomentar el desarrollo de alternativas a las empresas no europeas actualmente dominantes.

En menor medida, algunas políticas buscan potenciar la soberanía de un individuo sobre sus datos. La Ley de Servicios Digitales²⁴ y la Ley Europea de Datos²⁵ tienen como objetivo brindar a las empresas y las personas más opciones de servicio y control sobre los datos generados por los usuarios, respaldados por una medida regulatoria.

Si bien estos marcos tienden a ser iniciados por los gobiernos, no colocan exclusivamente a la autoridad estatal en el centro. Sus políticas de promulgación implican mayores roles para los reguladores, pero tienen el objetivo declarado de empoderar a las empresas o personas.

El segundo campo en esta región, con la Federación Rusa como el ejemplo más fuerte, equipara la soberanía digital con un mayor control estatal sobre el ámbito digital y la información que pasa a través de él, específicamente los datos que fluyen dentro del país.

24 Comisión Europea, "The Digital Services Act: ensuring a safe and accountable online environment", https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

25 Comisión Europea, "Data Act", <https://digital-strategy.ec.europa.eu/en/policies/data-act>

La Federación Rusa, no se refiere comúnmente a la "soberanía digital" en sus documentos políticos pero sí lo hace en los comunicados de prensa gubernamentales y las declaraciones públicas. Una regulación de 2019 llamada informalmente "Ley de Internet Soberana" tiene como objetivo garantizar la continuidad de la conectividad a Internet frente a un ataque a la infraestructura por parte de actores extranjeros.²⁶

III. Objetivos y resultados: Enfoques a la soberanía digital

Las políticas y medidas cubiertas en este informe están impulsadas explícitamente por la soberanía digital, pero varían en los objetivos declarados oficialmente y pueden permitir que diferentes actores, a veces no estatales, logren sus objetivos.

3.1 Cuatro objetivos principales de política

1. **Seguridad nacional y la capacidad de hacer cumplir las leyes:** estas políticas abordan las amenazas a la **seguridad nacional**, específicamente los ciberataques extranjeros y las vulnerabilidades en línea. A través de ellos, el estado pretende asegurar el dominio digital dentro de sus fronteras. Estos pueden abarcar la ciberseguridad de la infraestructura crítica hasta el uso de tecnologías de Internet en procesos y cambios políticos. Muchos gobiernos han encontrado fricciones al ejercer autoridad sobre los activos y servicios digitales que operan o están disponibles localmente y quieren reafirmar su **capacidad para establecer y hacer cumplir las leyes** dentro de su territorio. Generalmente esto caracteriza a las políticas que permiten el acceso legal a la información por parte de las agencias de cumplimiento de la ley, las autoridades de competencia y otros reguladores. Más allá de controlar los datos generados localmente, esta autoridad puede extenderse a cómo funcionan los servicios y el software en un contexto nacional específico.
2. **Autodeterminación económica:** estas políticas fortalecen el desarrollo de la industria local al crear más oportunidades para que las empresas nacionales compitan, a menudo en un entorno que se considera dominado por empresas de tecnología de los Estados Unidos y, cada vez más, en algunos países, China.²⁷ Algunas de las políticas intentan cumplir este objetivo a través de fuertes medidas proteccionistas,

26 'Федеральный закон от 01.05.2019 № 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации"', <http://publication.pravo.gov.ru/Document/View/0001201905010025>

27 Julia Pohle y Thorstein Thiel. Soberanía digital. Revisión de políticas de Internet, 9(4), 5 de diciembre de 2020. <https://doi.org/10.14763/2020.4.15321>

mientras que otras fomentan las fuerzas del mercado para crear un campo de juego más parejo.

3. **Proteger los derechos y empoderar a los ciudadanos/usuarios y comunidades:** estas políticas refuerzan la autonomía individual y colectiva frente a las plataformas tecnológicas con las que interactúan, específicamente al brindarles a los ciudadanos y las comunidades la capacidad de actuar y tomar decisiones relacionadas con sus datos y actividades digitales.
4. **Defender las normas y valores sociales:** estas políticas preservan las normas y tradiciones locales, o aquellas que un gobierno desea alentar, en medio de la afluencia de tecnologías, estándares y servicios que se considera que encarnan o promueven otros valores sociales, culturales y políticos. A menudo, esto es un objetivo secundario a los demás, es decir, rara vez es el objetivo dominante.

Las políticas a menudo tienen varios objetivos superpuestos: una política de localización de datos puede afirmar los derechos de los ciudadanos sobre sus datos y, al mismo tiempo, evitar que esos datos se almacenen en el extranjero por razones de seguridad. Las políticas también pueden tener objetivos implícitos; la localización de datos también puede permitir que los actores de inteligencia y las agencias del cumplimiento de la ley accedan más fácilmente a los datos de los ciudadanos o generen negocios para los centros de datos locales.

3.2 Actores empoderados para lograr los objetivos de la política

Las políticas con objetivos similares pueden afectar a Internet de manera diferente, según quién esté empoderado para lograrlas. Este puede ser (1) el Estado, aumentando la autoridad de sus instituciones; (2) actores económicos, fomentando un entorno justo y competitivo para las empresas; o (3) ciudadanos, tanto mediante la ampliación de sus derechos y beneficios, con el respaldo normativo para hacer valer su voluntad.

Estos objetivos y actores empoderados no son todos, ya que se extrajeron de políticas muestreadas en solo tres regiones. Reconocemos que las políticas sobre soberanía digital están surgiendo en todo el mundo y proponemos que el marco analítico presentado aquí pueda aplicarse a otras políticas sobre este asunto, en las regiones que estudiamos y en otras.

IV. Enfoques comunes de la soberanía digital y su impacto en Internet

La mayoría de los países tienen una combinación de objetivos de política y entidades empoderadas, pero después de evaluar 34 políticas, surgieron dos enfoques distintos de soberanía digital por encima de otros:

- (1) Seguridad nacional impulsada por un aumento en el control del estado y
- (2) Autodeterminación económica impulsada por actores económicos

Varias políticas tenían como objetivo aumentar la soberanía individual o comunitaria principalmente otorgando a los ciudadanos o grupos culturales más control sobre sus datos personales, pero no hubo suficientes ejemplos de su implementación para merecer una tercera distinción. Para obtener más información sobre la metodología y las políticas incluidas en el análisis, consulte el Apéndice III y IV.

Para analizar si la soberanía digital afecta Internet y cómo lo hace, usamos el kit de herramientas para la Evaluación del impacto en Internet (IIAT, Internet Impact Assessment Toolkit)²⁸ un marco que describe las condiciones que necesita Internet para existir y prosperar como bien público. Evaluamos cada tipo de política frente a cada propiedad esencial del "Modo Internet de interconectarse"²⁹ y los facilitadores³⁰ que sustentan una Internet abierta, conectada globalmente, segura y confiable. Ambos se articulan con mayor detalle en el Apéndice II.

Factores como el sistema político, el estado de derecho, las implementaciones técnicas previas o la protección de las libertades civiles pueden dar forma al efecto de una política, pero no forman parte de este análisis.

4.1 Enfoque 1: Seguridad nacional impulsada por un aumento del control estatal

Objetivo: Seguridad nacional y, en menor medida, la capacidad de hacer cumplir las leyes en el ámbito digital

Entidad empoderada: El Estado

Jurisdicciones relevantes: Australia, China, Nigeria, Rusia, Vietnam

Este enfoque se caracteriza por políticas de seguridad nacional que buscan reforzar la autoridad del Estado dentro de su territorio y su capacidad de hacer cumplir sus leyes en el ámbito digital. Enfatiza fuertemente el papel del Estado en la implementación e invariablemente aumenta el poder y, a menudo, la capacidad del Estado para impactar en Internet.³¹

28 Internet Society, "Internet Impact Assessment Toolkit", <https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/>

29 Internet Society, "The Internet Way of Networking", "Critical Properties", <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>

30 Internet Society, "Enablers of an Open, Globally Connected, Secure and Trustworthy Internet", <https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/>

31 Varias políticas expresaron el deseo de limitar la desinformación y la información errónea para fomentar una sociedad más cohesionada. A veces se han interpretado como esfuerzos para controlar el flujo de información dentro de las fronteras de

Impacto en el Modo Internet de interconectarse

La centralización del control de las infraestructuras es el impacto más común y preocupante en Internet de las políticas de seguridad nacional. Por lo general, buscan que el Estado controle las infraestructuras de redes clave, como nombres y direcciones, que están descentralizadas y distribuidas en Internet. Las políticas a menudo fortalecen la autoridad del Estado para dirigir las operaciones de la red y, en algunos casos, incluso para administrarlas.

Un ejemplo destacado son las "Reglas para la gestión centralizada de una red de comunicación pública" de Rusia, parte de la legislación conocida como "Ley Soberana de Internet" que pretende imponer un mayor control sobre los flujos de tráfico dentro del país. Al delegar autoridad a la agencia federal Roskomnadzor, ordena que se instalen servidores intermediarios para filtrar y monitorear el tráfico en las redes rusas. Esto interfiere directamente con la capacidad de los operadores de red rusos para administrar sus propias redes, obligándolos a cumplir con los requisitos de la política de enrutamiento de Roskomnadzor.

Disposiciones similares se encuentran en la "Ley sobre ciberseguridad" de Vietnam, que delega un poder significativo a la Autoridad de Ciberseguridad para restringir y suspender las operaciones de la red, incluido el filtrado de información que se considera que perturba la seguridad o el orden público.

La centralización se extiende a otras funciones técnicas. Las "direcciones de ciberseguridad CERT-In" de India amplían el control estatal para establecer la coordinación de tiempo de la red, al exigir que todas las entidades y servidores se conecten a los servidores del protocolo de tiempo de red (NTP) del gobierno.³² Estas leyes interfieren con la operación distribuida tanto del enrutamiento (a través del Protocolo de puerta de enlace fronteriza o BGP) como de la resolución de nombres (utilizando el Sistema de nombres de dominio o DNS).

Algunas políticas **restringen el despliegue voluntario de determinadas tecnologías y protocolos de infraestructura**, lo que puede afectar gravemente a la interoperabilidad. Por ejemplo, la "Ley de Ciberseguridad" de China y la "Ley sobre ciberseguridad" de Vietnam requieren que los intermediarios de Internet monitoreen el contenido. Esto evita que los intermediarios utilicen

una nación. Este informe se abstiene de adoptar estas interpretaciones para evitar suposiciones, centrándose estrictamente en los objetivos declarados de las políticas.

32 The Internet Society, "Internet Impact Brief: India CERT-In Cybersecurity Directions 2022", <https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-india-cert-in-cybersecurity-directions-2022/>

componentes básicos de seguridad desarrollados por la comunidad y ampliamente adoptados (por ejemplo, Seguridad de la capa de transporte o TLS 1.3) y otras mejores prácticas que se basan en el cifrado. Para rastrear o buscar contenido, los intermediarios de infraestructura pueden necesitar especializarse y adaptar sus servicios para acomodar tipos específicos de contenido, lo que causa un **daño significativo a la naturaleza tecnológicamente neutra y de propósito general de Internet**.

Las políticas de soberanía digital en la seguridad nacional a menudo interrumpen de forma directa las operaciones de Internet. Plantean riesgos significativos para Internet global al inducir una fragmentación de la red a través **de la interferencia con el conjunto compartido de identificadores de Internet**. Por ejemplo, la documentación de respaldo de la Ley de Internet Soberana de Rusia exige el uso de resolutores de DNS controlados por el gobierno. Exigir a los operadores rusos a usar solo estos resolutores de DNS permitirá que el gobierno modifique de forma unilateral la resolución de nombres en Rusia³³, creando potencialmente una alternativa rusa al DNS global.

En resumen, las políticas de soberanía digital en la seguridad nacional pueden tener graves impactos en el modelo de interconexión de Internet y hacer daño significativo a esta plataforma abierta y conectada globalmente.

Impacto en la Internet abierta, conectada a nivel global, segura y confiable

Además de perjudicar los atributos que hacen que Internet funcione correctamente, estas políticas también pueden afectar a los facilitadores más amplios de una Internet abierta, conectada globalmente, segura y confiable. Una de las bajas más claras es la **confiabilidad** de Internet, que disminuye con la interferencia en funciones básicas como nombres y direcciones. Si el aumento unilateral del control estatal no va acompañado de transparencia en la toma de decisiones, también puede degradar la **rendición de cuentas** en el entorno en línea. Si bien las leyes pueden complementarse con documentación más detallada sobre medidas de rendición de cuentas, no hemos podido localizar ninguna en las políticas que estudiamos.

Un elemento común en todas las políticas de esta naturaleza es la amplitud de actividades vagamente definidas que caen bajo la autoridad estatal ampliada, con pocos controles o condiciones sobre cómo se ejercen estos poderes. Las Instrucciones de ciberseguridad CERT-In revisadas de India³⁴ transforman el papel de CERT-In de una entidad autorizada en un sistema de

33 Принят закон о «суверенном интернете», <http://duma.gov.ru/news/44551/>

34 CERT-In. Equipo de Respuesta a Emergencias Informáticas de la India (CERT-In) del Ministerio de Electrónica y Tecnología de la Información (MeitY) del Gobierno de la India, 2022. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

colaboración voluntaria e intercambio de información, a un cuasi-regulador o incluso una agencia de cumplimiento de la ley.

Las técnicas de filtrado y seguimiento reducen la **confidencialidad e integridad de la información**. Esto se ejemplifica cuando Rusia impone equipos de interceptación para escanear y filtrar contenido.³⁵ Estos, junto con los requisitos de retención de datos extremadamente amplios en la India y la verificación de datos personales en Vietnam, amenazan gravemente la privacidad de los usuarios. El requisito de China de que los servicios obtengan el consentimiento al recopilar información personal podría mejorar la **privacidad** del usuario, pero se ve muy superado por las obligaciones de llevar a cabo una vigilancia masiva y denunciar el "comportamiento inaceptable" de los usuarios y su transmisión de "información prohibida".

El control centralizado sobre las funciones clave y la aplicación de medios técnicos para interceptar y monitorear el tráfico, también disminuye la **resiliencia, la disponibilidad y la confiabilidad** de los servicios en red. La propuesta de seguridad de tiempo (NTP) de India corre el riesgo de crear un punto único de falla que sea perjudicial para todos los servicios en el país, incluidas las tecnologías de cifrado que dependen de esta función. El uso de equipos de espionaje en la red por parte de Rusia puede causar interrupciones significativas en la red más amplias si esos dispositivos y su software asociado no funcionan correctamente. En efecto, ya han habido informes de dichas interrupciones³⁶ y la propia ley reconoce este riesgo al permitir eludir el equipo en caso de que no funcione correctamente.

Las políticas analizadas en general son perjudiciales para una Internet abierta y globalmente conectada. La **colaboración** entre actores, que ha sido la norma en el funcionamiento y la gobernanza de Internet, se reemplaza por el control estatal centralizado, que socava los importantes beneficios que ofrece el modelo de red. Las políticas para restringir y dirigir la **accesibilidad** en la red, incluida la interferencia con las decisiones de enrutamiento y DNS, limitan los recursos disponibles para los usuarios solo a aquellos permitidos por el gobierno. También hay consecuencias indirectas; los nuevos requisitos operativos y el aumento de los costos de cumplimiento plantean barreras para los operadores de red y los intermediarios, lo que en última instancia limita la **facilidad de acceso** a Internet.

35 Una introducción de diez minutos a los elementos intermedios
http://yuba.stanford.edu/~huangty/sigcomm15_preview/mbpreview.pdf

36 '«Суверенный интернет» засбоил. Проблемы с оборудованием привели к системным сбоям', 2021, https://kapital-rus.ru/articles/article/suverennyi_internet_zasboil_problemy_s_oborudovaniem_priveli_k_sistemnym_sb/

4.2 Enfoque 2: Autodeterminación económica impulsada por actores económicos

Objetivo: Autodeterminación económica, es decir, fortalecer a los actores de la economía nacional y garantizar la resiliencia de la cadena de suministro

Entidad empoderada: Actores económicos, típicamente empresas

Jurisdicciones importantes: Unión Europea, India, Ruanda, Sudáfrica

Este enfoque se caracteriza por políticas que afirman la autodeterminación económica mediante el fortalecimiento de la economía nacional. Su objetivo es reducir el dominio y la dependencia de los proveedores de tecnología y servicios extranjeros al (1) crear más oportunidades para que las empresas locales compitan, a veces con un grado de proteccionismo, y (2) promover la resiliencia de la cadena de suministro para el sector digital local. Si bien estas políticas a menudo buscaban extender la autoridad estatal, por ejemplo, aumentando el mandato de los reguladores de la competencia, también buscaban empoderar a los actores en la economía en general.

Impacto en el Modo Internet de interconectarse

Las políticas económicas que analizamos no interfieren directamente con las operaciones de red de Internet. Conscientes de las oportunidades creadas por una red global y sociedades conectadas, estas políticas se enfocan más a menudo en mejorar las condiciones que permiten a los actores locales aprovechar Internet.

En muchos casos, estas apuntan explícitamente a fortalecer importantes características del modelo de red. Por ejemplo, la “Estrategia de Transformación Digital de África (2020-2030)” de la Unión Africana promueve enfoques tecnológicamente neutrales para la interoperabilidad transfronteriza. La Política de centros de datos de la India insta de manera similar a la adopción voluntaria de estándares globales establecidos.

A primera vista, las políticas analizadas defienden la Internet abierta y global como un activo que debe ser apoyado y aprovechado para el progreso económico regional y nacional.

Facilitadores de una Internet abierta, conectada globalmente, segura y confiable

Las políticas de soberanía digital sobre la autodeterminación económica respaldan en gran medida a los facilitadores de una Internet abierta, conectada globalmente, segura y confiable. El

acceso y la reducción de las barreras de entrada se consideran clave para que Internet se convierta en una fuente de oportunidades. La “Estrategia de Transformación Digital de África (2020-2030)” de la Unión Africana busca hacer que los dispositivos y servicios sean más asequibles, enfatizando el papel de los gobiernos en el desarrollo de infraestructura para ampliar el acceso y la **capacidad**. Esto incluye Puntos de Intercambio de Internet (IXP) para mejorar la interconexión y el intercambio de tráfico, y un entorno regulatorio que respalda de manera proactiva las soluciones de acceso, como las redes comunitarias.³⁷ Más allá de implementar infraestructura, la Ley de datos de la UE busca reducir las barreras "legales, económicas y técnicas" para el acceso a los datos, en particular al exigir a los proveedores que tengan herramientas técnicas para que los usuarios controlen cómo se comparten sus datos con terceros. La Comisión Europea afirma que hacer que más datos estén disponibles para su reutilización agregará 270 000 millones de euros al PIB de la región para 2028.³⁸

Sin embargo, estas políticas también pueden limitar la flexibilidad en **la implementación técnica**. Por ejemplo, la Política de centros de datos de la India favorece el hardware y el software autóctonos para reducir las importaciones generales del país. La aplicación estricta puede limitar el uso de tecnologías potencialmente más rentables y adecuadas, pero no indias. Del mismo modo, el mandato de estándares específicos de la Ley de datos de la UE, destinado a fomentar una mayor interoperabilidad, puede impedir que las empresas desarrollen tecnologías innovadoras.

Sin embargo, estas políticas reconocen que la elección y la disponibilidad de tecnología son parte integral de un entorno digital **confiable y resiliente**.

Desde la India, que promueve un suministro de electricidad confiable a los centros de datos, hasta la Unión Europea, que apunala el suministro de componentes digitales y la Unión Africana, que respalda la seguridad de enrutamiento para mejorar la seguridad digital, muchas políticas fomentan la resiliencia de la cadena de

37 Plan de acción de Internet Society 2022, última modificación el 6 de septiembre de 2022, <https://www.internetsociety.org/action-plan/2022/community-networks/>

38 “Data Act: Commission proposes measures for a fair and innovative data economy”, 23 de febrero de 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

suministro como un aspecto clave de la soberanía digital económica.

A diferencia de las políticas de seguridad nacional, estas medidas centradas en la economía mantienen la **confidencialidad y la integridad** de la información, por ejemplo, al reforzar el cifrado fuerte. En la Estrategia de Transformación Digital de la Unión Africana, este énfasis se combinó con el fortalecimiento del control de los datos personales por parte del usuario y otras mejoras en la **privacidad**.

4.3 Otros enfoque de la soberanía digital

Un tercer enfoque alinea la soberanía digital con la soberanía individual o colectiva. Esto se manifiesta en medidas para mejorar los derechos de las personas o comunidades en relación con los datos sobre ellos o creados por ellos. En su guía de soberanía de datos³⁹, el gobierno de Nueva Zelanda pide a las instituciones que elijan servicios en la nube que respeten los derechos de datos de los indígenas maoríes. Defiende la Carta de soberanía de datos de los maoríes,⁴⁰ que insta a un mayor acceso y propiedad de los maoríes a los datos recopilados sobre ellos por otras entidades, y faculta a los maoríes para gobernar sus datos de acuerdo con sus costumbres y prioridades.⁴¹

De manera paralela, la Ley de datos de la UE pone los datos a disposición en diferentes sectores de la economía al otorgar a los propietarios de datos, tanto particulares como empresas, más control sobre cómo se comparten sus datos con terceros. Esto está muy cerca del concepto de “soberanía individual”, con autoridad descentralizada y delegada a las entidades propietarias de los datos, en línea con el principio de subsidiariedad de tomar decisiones lo más cerca posible de donde se siente su impacto.

Este enfoque parte del
concepto clásico de soberanía, centrado en el Estado y basado en el

39 Gobierno digital de Nueva Zelanda. “Data Sovereignty.” <https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/help/data-sovereignty/>

40 “Maori Data Sovereignty Charter.” <https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/5913020d15cf7dde1df34482/1494417935052/Te+Mana+Raraunga+Charter+%28Final+%26+Approved%29.pdf>

41 “Principles of Māori Data Sovereignty.” Octubre de 2018. <https://cdn.auckland.ac.nz/assets/psych/about/our-research/documents/TMR%2BM%C4%81ori%2BData%2BSovereignty%2BPrinciples%2BOct%2B2018.pdf>

territorio⁴², y avanza hacia dotar a los individuos de los medios para actuar y decidir de manera consciente, deliberada e independiente.

Al hacer esto, la Ley de datos facilita la disponibilidad, la portabilidad y el uso de datos, pero crea barreras de entrada para la tecnología fuera de la UE. Al aclarar las funciones y responsabilidades de las entidades en la cadena de valor, simplifica la rendición de cuentas y refuerza la confiabilidad de Internet. Pero la Ley de datos también contiene disposiciones más comúnmente asociadas con la soberanía estatal tradicional, como las restricciones de transferencia de datos internacionales o la interoperabilidad potencial y los mandatos de estándares específicos. Estos pueden tener un impacto negativo no solo en los habilitadores de Internet, sino también en la forma de trabajar en red de Internet.⁴³

Por último, un cuarto enfoque político se centra en salvaguardar las normas y valores culturales. Este objetivo se combinó con frecuencia con otros, como la seguridad nacional o la autodeterminación económica, y no ocupó un lugar destacado en las políticas de soberanía digital.

V. Conclusión

Como red global de redes, Internet no se ajusta a la noción de fronteras nacionales. Las redes pueden operar en ciertas jurisdicciones, pero su topología y puntos de interconexión están definidos por el objetivo de optimizar el tráfico, en lugar de seguir un mapa político. Las reglas de interconexión no están definidas por tratados, sino que se basan en procesos voluntarios que funcionan bien y en la colaboración entre redes.

Es en este contexto que encontramos la noción de soberanía, anterior a Internet, que se aplica cada vez más al ámbito digital. Las políticas de soberanía digital tienen una variedad de objetivos: desde mantener los datos dentro de las fronteras nacionales hasta aprovechar la tecnología para impulsar el desarrollo local, y sus efectos en Internet van desde pocos o ninguno, hasta potencialmente riesgosos, hasta dañar y fragmentar directamente la Internet global.

El concepto de soberanía digital en sí sigue siendo vago e inconexo, de ahí la dificultad para generalizar su impacto. Para comprender mejor sus numerosas facetas, este informe se enfoca

42 Julia Pohle y Thorstein Thiel. Soberanía digital. Revisión de la política de Internet, 5 de diciembre de 2020, <https://doi.org/10.14763/2020.4.1532>

43 Otra política a menudo asociada con un mayor control sobre los datos personales es el Reglamento General de Protección de Datos (GDPR) de la UE. Si bien el GDPR se hace eco de los sentimientos de soberanía individual, se excluyó del alcance de este documento debido al hecho de que el texto del reglamento no hace referencia a la soberanía digital y que el reglamento es anterior al uso del término en los documentos de estrategia de la UE.

en cómo se aplica la soberanía digital en la política pública. Al evaluar docenas de políticas emitidas por el Estado en diferentes países de Asia-Pacífico, Europa y África, identificamos cómo varios enfoques gubernamentales de la soberanía digital pueden tener un efecto diferente en Internet.

Las políticas que buscan reforzar la seguridad nacional a través de una mayor autoridad estatal concentran el control en el gobierno y limitan excesivamente la autonomía de las redes. Estas medidas corren el riesgo de dañar Internet al hacer cumplir requisitos técnicos específicos y confiar en un modelo de "mando y control", en lugar de en la colaboración y coordinación entre pares. Algunas políticas frustran directamente las propiedades esenciales que hacen que Internet funcione correctamente, como su gestión descentralizada y su uso de identificadores globales (nombre y direccionamiento). Los esfuerzos que cambian fundamentalmente la forma en que funciona Internet limitan el valor que podemos derivar de Internet como un recurso abierto y globalmente conectado.

Las políticas que persiguen la autodeterminación económica mediante el empoderamiento de los actores económicos tienden a centrarse en impulsar las economías digitales locales al nivelar el campo de juego y reducir las barreras de entrada al hacer que los recursos, como los datos, sean más accesibles. Estas políticas tienden a estar mejor alineadas con la forma en que funciona Internet, ya que no están reñidas con sus propiedades ni facilitadores. Sin embargo, algunas de las medidas cubiertas en este informe tienen elementos significativos de proteccionismo, por ejemplo, limitar la disponibilidad y la elección de productos y servicios. Pero, en general, es posible que estas políticas solo causen un daño mínimo y, en algunos casos, incluso puedan mejorar y reforzar la utilidad de Internet.

Un enfoque emergente y menos común, que se encuentra en la Ley de datos de la UE y las pautas de soberanía de datos de Nueva Zelanda, evoca la soberanía del individuo y de distintas comunidades, específicamente su capacidad de actuar y decidir por sí mismos cuando se trata de su presencia digital. Esta orientación parece estar más alineada con la forma en que funciona Internet y los principios que la sustentan: gestión descentralizada de redes, uso sin restricciones de tecnologías, accesibilidad sin restricciones y transparencia y responsabilidad en el uso de los recursos de Internet. Aunque los ejemplos de este enfoque son limitados, representa una visión de soberanía centrada en el usuario en el mundo digital.

Por lo general, las estrategias para la soberanía digital tienen una combinación de enfoques, aunque uno o dos suelen dominar. Destilar los objetivos políticos dominantes nos permitió evaluar el impacto que un enfoque específico de soberanía digital puede tener en la base de Internet.

La soberanía digital es un concepto en expansión, y la noción por sí sola nos dice poco sobre cómo puede remodelar el entorno en línea. En última instancia, son las políticas resultantes y los actores que centran y empoderan los que definen el impacto de la soberanía digital en Internet.

Como cualquier ecosistema vivo, Internet está en constante evolución. Esta continua evolución sin un plan o autoridad central apuntala su valor para el mundo. Pero a medida que Internet ha llegado a impregnar la mayor parte de nuestras vidas, los gobiernos y las empresas toman cada vez más decisiones que la afectan.

Cada nueva política que se proponga bajo el nombre de soberanía digital debe ser evaluada para que no dañe los elementos que hacen que Internet nos sea útil, ni nos acerque a una serie de redes fragmentadas y cerradas donde se pierden las oportunidades que surgen de la conexión global.

Este informe muestra cómo se puede hacer esa evaluación, tanto de las políticas que examinamos aquí como de las que están por venir.

Apéndice I — Tendencias regionales de la soberanía digital

A. Asia-Pacífico

La región de Asia-Pacífico incluye los países más poblados del mundo, China y la India, y algunos de los más pequeños. Los países que examinamos son grandes economías con una influencia geopolítica considerable en la región y a nivel mundial. Han elaborado o adoptado una o más políticas, leyes, reglamentos o estrategias que hacen referencia a la soberanía digital o términos similares,⁴⁴ pero muestran una gran variedad en la interpretación y puesta en práctica de la soberanía digital.

Australia: En Australia, las políticas impulsadas por la soberanía digital se centran en mejorar la ciberseguridad. Su estrategia de gobierno digital tiene como objetivo proteger y administrar la información pública con "controles apropiados de privacidad, soberanía y seguridad"⁴⁵ y está respaldada por una estrategia de alojamiento que aborda "los riesgos para la soberanía de los

44 Por ejemplo, Vietnam utiliza con frecuencia el término "soberanía nacional en el ciberespacio".

45 Agencia de Transformación Digital, Gobierno de Australia, "Digital Government Strategy", 2021, https://www.dta.gov.au/sites/default/files/2021-12/Digital%20Government%20Strategy_web-ready_FA.pdf.

datos almacenados en los centros de datos del gobierno australiano".⁴⁶ De manera tangencial, estas estrategias fomentan la construcción de centros de datos domésticos.

A pesar de la ausencia de requisitos obligatorios de localización de datos en Australia, informes oficiales recientes destacan niveles sin precedentes de interferencia extranjera destinados a socavar la soberanía nacional de ese país.⁴⁷ En respuesta, los investigadores han pedido más medidas de soberanía digital para salvaguardar tanto la seguridad nacional⁴⁸ como los intereses económicos,⁴⁹ junto con los requisitos de localización de datos para los datos del gobierno.⁵⁰

China: China, tras ser uno de los primeros en adoptar el concepto de soberanía digital, ha tenido el plazo más largo para poner en práctica su visión. Ejerce influencia en la definición de un enfoque específico de la soberanía digital en la región y en el mundo.

La perspectiva de China ha dado forma a muchas políticas y leyes en el país, aunque no siempre se establece explícitamente. El objetivo de defender la "soberanía cibernética o de Internet" se puede encontrar en la Ley de Seguridad Cibernética (2017), la Ley de Seguridad de Datos (2021) y la Estrategia Internacional de Cooperación en el Ciberespacio (2017). A través de tales medidas, y en narrativas políticas de alto nivel, China ve la soberanía digital como una forma de garantizar la seguridad nacional, proteger al país de las ciberamenazas⁵¹ y construir la economía digital local al brindar un trato preferencial a las empresas chinas.^{52 53}

Varias leyes afirman la intención de China de adoptar medidas extraterritoriales, como incluir en una lista negra a las empresas extranjeras que no cumplan con sus regulaciones. La Ley de Ciberseguridad (2017) requiere que los operadores de red en sectores fundamentales almacenen

46 Agencia de Transformación Digital, Gobierno de Australia, "Whole-Of-Government Hosting Strategy: Overview", <https://www.dta.gov.au/our-projects/hosting-strategy/overview>.

47 Monitor independiente de legislación de seguridad nacional, gobierno australiano, "Annual Report 2020-2021", 2021, https://www.inslm.gov.au/sites/default/files/2022-01/inslm-annual-report_2020-21.pdf.

48 Andrew Mitchell, "A sovereign Australian government data framework", Instituto Australiano de Política Estratégica, 11 de agosto de 2021, <https://www.aspistrategist.org.au/a-sovereign-australian-government-data-framework/>

49 "Australia's own assets can ensure national digital resilience" de Marcus Thompson, The Mandarin, 6 de mayo de 2022, <https://www.themandarin.com.au/188379-australias-own-assets-can-ensure-national-digital-resilience/>

50 "Cloud services and government digital sovereignty in Australia and beyond" de Andrew D. Mitchell y Theodore Samlidis, Revista internacional de derecho y tecnología de la información, enero de 2022, https://www.researchgate.net/publication/358197261_Cloud_services_and_government_digital_sovereignty_in_Australia_and_beyond

51 China.org.cn, "Full Text: International Strategy of Cooperation on Cyberspace", 7 de marzo de 2017, http://www.china.org.cn/chinese/2017-03/07/content_40424606_2.htm

52 Jane Li, "Beijing has a new legal architecture for sweeping control over user data," Quartz, 30 August 2021, <https://qz.com/2051268/china-aims-to-control-but-also-unleash-the-economic-power-of-data/>; and Rogier Creemers, "China's Approach to Cyber Sovereignty," Konrad-Adenauer-Stiftung, 2020, <https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537>

53 Congreso Nacional del Pueblo de la República Popular de China, "Data Security Law of the People's Republic of China", 10 de junio de 2021, <http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml>

dentro de China cualquier información que recopilen o produzcan en el país. La información comercial y los datos sobre ciudadanos chinos que se recopilan dentro de China deben mantenerse en servidores nacionales y no deben transferirse al extranjero sin permiso. Estas disposiciones se consolidan en la Ley de Protección de Datos Personales (2021).⁵⁴

India: Las medidas de soberanía digital relevantes en la India, limitadas a los requisitos y políticas de localización de datos que hacen referencia explícita al término, se encuentran principalmente en forma de borrador. Estas políticas priorizan la infraestructura fundamental y la protección de datos a raíz de los incumplimientos de datos y refuerzan la capacidad de alojamiento del país. La soberanía digital se cita como un impulsor del borrador de la Política de centros de datos de India (2020)⁵⁵ que, junto con los objetivos de seguridad, tiene como objetivo disminuir las dependencias en la cadena de suministro. Se alinea con la reciente iniciativa “Atmanirbhar Bharat” (traducida libremente como una India que es autodependiente y autosuficiente), cuyo objetivo es incentivar el desarrollo económico.

Vietnam: La soberanía digital, traducida como “soberanía nacional en el ciberespacio”, fue adoptada en la Ley de Ciberseguridad de Vietnam (2018). Alienta al Ministerio de Seguridad Pública a “prevenir y combatir el uso del ciberespacio para vulnerar la soberanía, los intereses y la seguridad nacional, y el orden y la seguridad social”.⁵⁶ Esto incluye abordar la desinformación y mejorar la defensa mediante la detección, la lucha contra y la prevención de ataques en el ciberespacio. La ley requiere que los proveedores extranjeros de servicios en línea localicen el almacenamiento de datos y tengan una oficina en el país. Los servicios de red en datos y contenidos pueden ser paralizados por orden de las autoridades. La ley alude a aumentar la “autonomía” en ciberseguridad y protección infantil, pero define el término vagamente y no especifica cómo se defenderá.

En otro lugar, la Estrategia para la Protección Nacional en el Ciberespacio de Vietnam⁵⁷ se refiere a la soberanía digital centrada en el Estado. El concepto también aparece en los discursos políticos.⁵⁸ Lo aplica el Ministerio de Defensa Nacional en el contexto militar de Vietnam, situándolo como central para la defensa contra amenazas externas. Vietnam estableció un

54 Digi China, Universidad de Stanford, "Translation: Personal Information Protection Law of the People's Republic of China — Effective Nov. 1, 2021", 7 de septiembre de 2021, <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.

55 MeitY, "Data Centre Policy 2020: Draft for Discussion", https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf.

56 Traducción no oficial de la Ley de Ciberseguridad, 12 de junio de 2018, <https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf>.

57 “Vietnam refuerza la protección de la soberanía nacional en el ciberespacio” de Anh Kiet, Hanoi Times, 9 de diciembre de 2021, <https://hanoitimes.vn/vietnam-tightens-national-sovereignty-protection-in-cyberspace-319495.html>.

58 ibídem.

Comando Cibernético para “proteger la soberanía nacional en el ciberespacio”.⁵⁹ En resumen, con algunos momentos de resistencia a la creciente influencia de China,⁶⁰ Vietnam está consolidando su marco y enfoque de soberanía digital a través de una variedad de leyes y políticas que se basan en el modelo de China.^{61 62}

B. África

Unión Africana: En 2020, la Estrategia de Transformación Digital para África de la Unión Africana estableció una estrategia económica de diez años que incluye garantizar la propiedad de África de las herramientas digitales mediante la localización de la infraestructura y el almacenamiento de datos.⁶³ Tiene la intención de reducir el dominio de las empresas tecnológicas, en su mayoría estadounidenses y europeas, mediante la construcción de infraestructura local, financiada por un fondo de soberanía digital,⁶⁴ que se espera reduzca los costos y la latencia en la conectividad internacional y aumente el control local sobre las comunicaciones, lo que en última instancia permitirá que África satisfaga sus propias necesidades. Requiere una infraestructura de centros de datos de África para alojar servidores y sistemas de misión crítica y aspira a localizar los datos personales de los ciudadanos.

Sudáfrica: El borrador de la Política de Datos y de la Nube⁶⁵ trata los datos como un activo que debe protegerse y explotarse, al mejorar la capacidad de análisis de datos del país y requerir que toda la “información crítica” se almacene y procese de manera local. Reivindica la propiedad sobre todos los datos generados en Sudáfrica⁶⁶ y aborda la soberanía digital como un medio para el desarrollo económico.

59 Ministerio de Defensa Nacional de Vietnam, “Cyber Command asked to safeguard national sovereignty in cyberspace”, 1 de septiembre de 2018, <https://vietnamnews.vn/politics-laws/420790/cyber-command-asked-to-safeguard-national-sovereignty-in-cyberspace.html>

60 “Control de Internet de Vietnam: ¿Siguiendo los pasos de China?” de Justin Sherman The Diplomat, 11 de diciembre de 2019, <https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/>.

61 “Control de Internet de Vietnam: ¿Siguiendo los pasos de China?” de Justin Sherman The Diplomat, 11 de diciembre de 2019, <https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/>.

62 “Digital Sovereignty: Protectionism or Autonomy?” de Deborah Elms Fundación Hinrich, septiembre de 2021, <https://www.hinrichfoundation.com/research/wp/digital/digital-sovereignty-protectionism-or-autonomy/>.

63 Unión Africana, “The Digital Transformation Strategy for Africa (2020-2030)” <https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf>

64 Crear un entorno armonizado necesario para garantizar la inversión y la financiación mediante la creación de un fondo de soberanía digital para cerrar la brecha de infraestructura digital y lograr una banda ancha accesible, asequible y segura, independientemente de la demografía, el género y la geografía, <https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf>

65 David Monyae, 2021

66 Departamento de Comunicaciones y Tecnologías Digitales, “Draft National Data and Cloud Policy”, 2021, https://www.gov.za/sites/default/files/qcis_document/202104/44389gon206.pdf

Ruanda: El gobierno de Ruanda fue uno de los primeros en apoyar explícitamente la soberanía digital, al afirmar la propiedad del país de todos los datos generados dentro de sus fronteras. Su "Política de revolución de datos de Ruanda" de 2017 ⁶⁷tiene como objetivo crear una industria habilitada para datos y localizar datos para seguridad y privacidad.

Nigeria: Una medida, la política de computación en la nube de Nigeria de 2019, invoca explícitamente la soberanía de los datos.⁶⁸ Fomenta la adopción de los servicios en la nube por parte del sector público y nuevos requisitos para el tratamiento de datos nacionales. La soberanía digital también ha ocupado un lugar destacado en la retórica política, especialmente después de la prohibición de Twitter en el país en 2021 - 2022⁶⁹. Preocupada de que los ciudadanos estuvieran usando redes privadas virtuales (VPN) para eludir la prohibición, la oficina de la presidencia de Nigeria discutió la construcción de un firewall de Internet con la Administración del Ciberespacio de China⁷⁰. La prohibición de Twitter se levantó después de que acordó pagar un "impuesto aplicable" y establecer una oficina local en el país.⁷¹

Senegal: Un pronunciamiento de alto nivel del presidente Macky Sall en 2021 ordenó al gobierno migrar todos los datos estatales de servidores extranjeros a un centro de datos nacional financiado por el gobierno chino,⁷² tras concluir que la mayoría de los datos generados en el país se almacenan en el extranjero.⁷³ Senegal parece estar adoptando una visión de soberanía digital centrada en el Estado, habilitada por la inversión de China y equipos de proveedores chinos. La política quiere capturar el valor económico de los datos y evitar el acceso extranjero a ellos, aunque no está claro cómo abordará la relativa falta de defensores digitales nacionales.

C. Europa, incluida Rusia

Unión Europea: La soberanía digital en la Unión Europea es una visión de alto nivel que no se incorpora directamente en las propuestas normativas y legislativas, lo que permite su aplicación

67 "Rwanda National Data revolution and Big data", 2017 <http://statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data>

68 Agencia Nacional de Desarrollo de Tecnologías de la Información, "Nigeria Cloud Computing Policy", 2019 https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf

69 "Nigeria bans Twitter after President's tweet is deleted", 5 de junio de 2021, The New York Times. <https://www.nytimes.com/2021/06/05/world/africa/nigeria-twitter-president.html>

70 "Presidency Meets With China's Cyber Regulator to Build Nigerian Internet Firewall" de Sócrates Mbamalu, 6 de junio de 2021, Fundación para el Periodismo de Investigación <https://fij.ng/article/exclusive-presidency-meets-with-chinas-cyber-regulator-to-build-nigerian-internet-firewall/>

71 "Nigeria, Twitter agreement risks collapse over global restructuring" de Adeyemi Adepotun, 8 de noviembre de 2022, The Guardian. <https://guardian.ng/news/nigeria-twitter-agreement-risks-collapse-over-global-restructuring/>

72 "Senegal aims for digital sovereignty with new China-backed data centre" Reuters, 22 de junio de 2021 <https://www.reuters.com/article/senegal-datacenter-idINL5N2O44D3>

73 "Le Sénégal ouvre un centre de données national au nom de la «souveraineté numérique»," Le Figaro, 22 de junio de 2021 <https://www.lefigaro.fr/flash-eco/le-senegal-ouvre-un-centre-de-donnees-national-au-nom-de-la-souverainete-numerique-20210622>

fluida en una amplia gama de objetivos políticos. No existe un único término acordado dentro de la formulación de políticas de la UE, y "soberanía digital",⁷⁴ "soberanía tecnológica"⁷⁵ y "economía digital europea soberana"⁷⁶ son términos utilizados en documentos de estrategia y declaraciones públicas sin una indicación clara de cómo pueden diferir, si lo hacen. La naturaleza abierta de la soberanía digital en el contexto de la UE se presta igualmente a una variedad de objetivos políticos en materia de ciberseguridad, competitividad económica, investigación, seguridad de la cadena de suministro y protección de datos.

"Una Europa apta para la era digital", una estrategia de 2019 para establecer la agenda digital de la UE, ve a la región como un emisor de estándares globales y enfatiza la necesidad de "fortalecer su soberanía digital".⁷⁷ La estrategia informó la Ley de Mercados Digitales (DMA),⁷⁸ la Ley de Servicios Digitales (DSA)⁷⁹ y la Ley Europea de Chips⁸⁰.

La Estrategia de Ciberseguridad de la UE de 2020 para la Década Digital dirige la inversión para mitigar los riesgos tecnológicos y geopolíticos para la seguridad de la UE. El documento pide "soberanía tecnológica y liderazgo"⁸¹, al tiempo que enfatiza el compromiso de la UE con una Internet global y abierta. Entre sus flujos de trabajo se encuentra un "Sistema de resolución de nombres de dominio europeo",⁸² llamado DNS4EU, para reforzar las redundancias en la infraestructura global de Internet. Estos proyectos⁸³ están destinados al uso voluntario para crear resiliencia y complementar las opciones globales existentes. Estas propuestas apuntan a una imagen multifacética de la soberanía digital que se puede dividir en cuatro temas:

Competencia económica: DMA y DSA tienen como objetivo reducir el dominio en los mercados tecnológicos, generalmente por parte de empresas estadounidenses que operan en la capa de

74 Comisión Europea, "A Europe fit for the digital age Empowering people with a new generation of technologies", https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

75 Comisión Europea, "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade", <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN>

76 Comisión Europea, "Data Act: Commission proposes measures for a fair and innovative data economy", https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

77 Comisión Europea, "A Europe fit for the digital age Empowering people with a new generation of technologies", https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

78 Comisión Europea, "Digital Markets Act", https://competition-policy.ec.europa.eu/sectors/ict/dma_en

79 Comisión Europea, "Digital Services Act Package", <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

80 Comisión Europea, "The European Chips Act", https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

81 Comisión Europea, "The EU Cybersecurity Strategy", <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

82 Unión Europea, "Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade", <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN>

83 Comisión Europea, Financiamento y Oportunidades de Licitación, "Equipping backbone networks with high-performance and secure DNS resolution infrastructures - Works TOPIC ID: CEF-DIG-2021-CLOUD-DNS-WORKS", <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works>

aplicación, incluidas los medios sociales, la búsqueda y la mensajería. La soberanía digital aquí significa crear las condiciones para que las empresas europeas compitan con proveedores extranjeros establecidos, tanto para mantener la influencia global de Europa como para garantizar los derechos fundamentales de sus ciudadanos. En este marco, la soberanía digital significa la capacidad de Europa para desarrollar sus propios proveedores digitales para que la región determine su propio futuro.

Resiliencia de la cadena de suministro: Las medidas como la Ley Europea de Chips y DNS4EU responden a la preocupación de que la dependencia excesiva de proveedores extranjeros en la cadena de suministro y la provisión de infraestructura es una vulnerabilidad estratégica. La Ley Europea de Chips tiene como objetivo reducir la dependencia de los chips semiconductores del extranjero, principalmente de China y Taiwán. La licitación de DNS4EU tiene como objetivo crear un sistema de resolución de nombres de dominio europeo voluntario como una alternativa a los servicios globales más grandes que la mayoría de los proveedores utilizan actualmente, y que algunos creen que podrían ser cuellos de botella para acceder en un ataque importante. Sin embargo, además de bloquear material como phishing y malware, como lo hacen habitualmente otros solucionadores de DNS, la licitación también requiere que los posibles proveedores bloqueen el "contenido ilegal" en todo el continente.⁸⁴ Notamos que el filtrado de DNS tiene inconvenientes potencialmente sustanciales, que deben tenerse en cuenta al elaborar políticas⁸⁵.

Protección contra ataques cibernéticos: La estrategia de ciberseguridad de la UE⁸⁶ está incorporada en medidas como la Directiva de seguridad de redes e información actualizada (NIS2)⁸⁷ para establecer un nivel común de seguridad y resiliencia de infraestructura digital en todos los Estados miembros, junto con una red de centros de operaciones que forman un "escudo de ciberseguridad" para la detección temprana de ciberataques.

Empoderamiento del individuo: El DSA tiene como objetivo proporcionar "un mayor control y supervisión democráticos sobre las plataformas sistémicas".⁸⁸ DNS4EU quiere proporcionar una resolución de DNS por parte de proveedores con sede en la UE que respeten la privacidad de los datos del usuario, evitando la monetización de las consultas de DNS de los europeos. Los

84 "The EU Wants Its Own DNS Resolver that Can Block "Unlawful" de Ernesto Van der Sar, Traffic, 19 de enero de 2022 <https://torrentfreak.com/the-eu-wants-its-own-dns-resolver-that-can-block-unlawful-traffic-220119/>

85 The Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering:", <https://www.internetsociety.org/wp-content/uploads/2018/10/Perspectives-on-Domain-Name-System-Filtering-en.pdf>

86 Comisión Europea, "New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient", https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

87 Thinktank, European Parliament briefing, The NIS2 Directive: A high common level of cybersecurity in the EU", [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2021\)689333](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333)

88 Comisión Europea, "The Digital Services Act: ensuring a safe and accountable online environment", https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

formuladores de políticas a menudo conectan este concepto de soberanía digital con el "capitalismo de vigilancia"⁸⁹ y señalan la necesidad de restablecer el equilibrio de poder entre los ciudadanos y las empresas.⁹⁰

La soberanía digital en la UE tiene diferentes significados, aplicaciones y objetivos. Dado que la UE es una potencia económica y política importante por derecho propio, en reuniones multilaterales, incluidos el G7 y el G20, y mediante la exportación de sus reglamentos a través del "efecto Bruselas"⁹¹, estos marcos pueden tener una influencia mundial.

Estados miembros de la UE: Francia, Alemania e Italia: Francia y Alemania son los primeros impulsores de la soberanía digital dentro de la Unión Europea y rápidamente les sigue Italia, que utiliza una retórica similar. El documento de posición franco-alemán Gaia-X 2020 quiere una "infraestructura de datos soberana" para que los Estados miembros de la UE intercambien datos de forma segura. Trata el aumento del volumen de datos compartidos y procesados entre empresas europeas como una fuente de innovación, valor y competitividad en el mercado digital global.⁹² También alude a la soberanía individual y hace referencia a la mayor capacidad de los "usuarios [para] conservar la soberanía sobre sus datos".⁹³

La soberanía digital de Italia se ve a través de una lente de seguridad nacional. Su Estrategia Nacional de Ciberseguridad 2022⁹⁴ tiene como objetivo proteger contra las actividades de actores estatales hostiles, el cibercrimen, el ciberespionaje y las campañas de desinformación que buscan polarizar la opinión pública.

Francia, Alemania e Italia son grandes economías, tienen grandes poblaciones e históricamente han ocupado posiciones ventajosas en la "influencia" al nivel de la UE. La soberanía digital no es una excepción a esta tendencia con Francia y Alemania articulando visiones de soberanía digital antes que la Comisión Europea.

Federación de Rusia: El término soberanía digital se usó con frecuencia durante las reuniones anuales del Foro de Internet más seguro de Rusia/China, incluida una intervención en 2016 de un

89 "Capitalismo de vigilancia" es un término popularizado por Shoshanna Zuboff en su ensayo de 2014, "A Digital Declaration: Big Data as Surveillance Capitalism" y el libro de 2019, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power". Se refiere a un sistema económico basado en la recopilación y mercantilización de datos sobre las personas, con fines de lucro económico, que conduce al crecimiento de empresas casi monopólicas con un poder económico, político y social global significativo y en gran medida libre de trabas.

90 [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)

91 "The Brussels Effect, How the European Union Influences the World", Anu Bradford, (2020) <https://global.oup.com/academic/product/the-brussels-effect-9780190088583?cc=au&lang=en&>

92 Posición franco-alemana sobre GAIA-X, https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=4

93 GAIA-X, última modificación el 6 de septiembre de 2022 <https://gaia-x.eu/>

94 Gobierno de Italia, "National Cybersecurity Strategy, 2022-2026", https://www.acn.gov.it/ACN_EN_Strategia.pdf

senador que instó al filtrado previo a nivel de proveedor para proteger la "soberanía digital rusa".⁹⁵

La soberanía digital en Rusia se enmarca principalmente como soberanía estatal en el ámbito digital, y las medidas pertinentes facultan exclusivamente a las instituciones estatales para protegerse contra amenazas reales o percibidas a la seguridad nacional, como la desinformación, el contenido terrorista y los ataques cibernéticos de actores estatales hostiles. Este enfoque ha resultado en políticas que separan cada vez más a Rusia de la Internet global a través del mandato de una infraestructura de Internet construida y controlada por el estado en Rusia.

La "Ley soberana de Internet" de 2019⁹⁶ y las "Reglas para la gestión centralizada de una red de comunicación pública"⁹⁷ relacionadas requerían que los operadores de red proporcionaran información técnica y acceso al regulador, Roskomnadzor,⁹⁸ para que pudiera "garantizar el funcionamiento de los recursos de Internet rusos en caso de que los operadores de telecomunicaciones rusos no puedan conectarse a servidores raíz [DNS] extranjeros".⁹⁹ Permitted al regulador cortar la conectividad o los servicios internacionales (por ejemplo, servicios en la nube) y aumentó su capacidad para interceptar y bloquear el tráfico. El concepto de una Internet soberana para Rusia es uno que no puede ser desconectado o interrumpido por actores extranjeros hostiles, pero su implementación permite un control significativo sobre los flujos de comunicación e información dentro de Rusia. También exige el uso de herramientas técnicas para filtrar y censurar contenido en línea en nombre de la lucha contra los "mensajes falsos" y el contenido terrorista.^{100 101}

Indirectamente, el Consejo Alemán de Relaciones Exteriores ha establecido un vínculo conceptual¹⁰² entre la comprensión de Rusia de la soberanía digital y la Ley de localización de datos modificada de 2014, así como las "Leyes Yarovaya" de Rusia de 2016,¹⁰³ que introdujeron

95 Foro de Internet seguro, Rusia, "Moscow Safer Internet Forum adopts Russia-China cybersecurity Cooperation roadmap", 19 de abril de 2021, <https://safeinternetforum.ru/en/novosti/moscow-safer-internet-forum-adopts-russia-china-cybersecurity-cooperation-roadmap.html>

96 "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'", 22 de abril de 2019, <http://publication.pravo.gov.ru/Document/Text/0001201905010025>.

97 Normas para la gestión centralizada de una red de comunicación pública, aprobadas por el Decreto del Gobierno N.º 127 del 12 de febrero de 2020: [Правила централизованного управления сетью связи общего пользования](#)

98 El Servicio Federal de Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación

99 'Принят закон о «суверенном интернете»', <http://duma.gov.ru/news/44551/>

100 'Федеральный закон от 06.07.2016 г. № 374-ФЗ', <http://kremlin.ru/acts/bank/41108>

101 'Федеральный закон от 06.07.2016 г. № 375-ФЗ', <http://kremlin.ru/acts/bank/41113>

102 Alena Epifanova y Philipp Dietrich, DGAP, Consejo Alemán de Relaciones Exteriores, "Russia's Quest for Digital Sovereignty Ambitions, Realities, and Its Place in the World", <https://dgap.org/en/research/publications/russias-quest-digital-sovereignty>

103 <https://pd.rkn.gov.ru/authority/p146/p191/>

capacidades de vigilancia masiva en nombre de la lucha contra el terrorismo y otras “ideologías” en línea.¹⁰⁴

El concepto de soberanía digital de Rusia es importante porque defiende su visión de control estatal directo de Internet en órganos de gobierno clave como la Unión Internacional de Telecomunicaciones. A medida que el concepto de soberanía digital gana terreno en todo el mundo, Rusia puede utilizar estas organizaciones para influir en la regulación de Internet a nivel mundial. También tiene influencia regional. Rusia, junto con China, tiene una influencia directa en los miembros de Eurasia, incluidos Kazajstán, Kirguistán y Tayikistán, a través de la Organización de Cooperación de Shanghai. El acuerdo de cooperación en seguridad cibernética de 2015 de la organización tiene como objetivo limitar el uso de tecnologías diseñadas “para interferir en los asuntos internos de los Estados; socavar la soberanía, la estabilidad política, económica y social; [y] alterar el orden público”.¹⁰⁵

104 Alena Epifanova y Philipp Dietrich, DGAP, Consejo Alemán de Relaciones Exteriores, “Russia's Quest for Digital Sovereignty Ambitions, Realities, and Its Place in the World”, <https://dgap.org/en/research/publications/russias-quest-digital-sovereignty>

105 <https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/>

Apéndice II: El Modo Internet de interconectarse

El Modo Internet de Interconectarse

Propiedad esencial	Beneficios
1. Una infraestructura accesible con un protocolo común que sea abierta y tenga pocas barreras de acceso	El acceso sin restricciones y los protocolos comunes brindan conectividad global y fomentan el crecimiento de la red. A medida que se conectan más y más participantes, el valor de Internet aumenta para todos.
2. Arquitectura abierta de componentes básicos interoperables y reutilizables basada en procesos de desarrollo de estándares abiertos adoptados voluntariamente por una comunidad de usuarios	La arquitectura abierta crea servicios interoperables comunes, que brindan innovación rápida y sin necesidad de permisos en todas partes. El proceso de estandarización inclusiva y la adopción impulsada por la demanda garantizan que se adopten cambios útiles, mientras que los que son innecesarios desaparecen.
3. Gestión descentralizada y un único sistema de enrutamiento distribuido que es escalable y ágil	El enrutamiento distribuido ofrece una red resiliente y adaptable de redes autónomas, lo que permite optimizaciones locales, al mismo tiempo que se mantiene la conectividad mundial.
4. Identificadores globales comunes que son inequívocos y universales	Un conjunto de identificadores comunes ofrece una direccionalidad uniforme y una visión coherente de toda la red, sin fragmentación ni fracturas.
5. Una red de uso general y neutralidad tecnológica que es simple y adaptable	La generalidad brinda flexibilidad. Internet atiende continuamente a una comunidad diversa y en constante evolución de usuarios y aplicaciones. No requiere cambios significativos para respaldar este entorno dinámico.

Para obtener más información sobre cómo realizar una evaluación del impacto de Internet, consulte nuestra guía en línea: **Cómo realizar un resumen del impacto de Internet** utilizando el **kit de herramientas de evaluación del impacto de Internet**.¹⁰⁶

106 Internet Society, "How to Conduct an Internet Impact - Brief Internet Impact Assessment Toolkit", <https://www.internetsociety.org/resources/doc/2021/how-to-conduct-an-internet-impact-brief/>



Facilitadores de una Internet abierta, conectada a nivel mundial, segura y confiable

Apoyar una Internet abierta	
Acceso fácil y sin restricciones	Es fácil formar parte de Internet, tanto para las redes como para los usuarios. Eso significa que para los usuarios Internet es asequible y los servicios de Internet accesibles, y que las redes pueden convertirse fácilmente en parte de Internet, sin barreras reglamentarias o comerciales innecesarias para ambos grupos.
Uso e implementación sin restricciones de tecnologías de Internet	Las tecnologías y los estándares de Internet están disponibles para su adopción sin restricciones. Este facilitador se extiende a los puntos de enlace: las tecnologías utilizadas para conectarse y utilizar Internet no requieren permiso de un tercero, proveedor de sistema operativo (SO), proveedor de red o cualquier otro tercero. La infraestructura de Internet está disponible como recurso para cualquiera que desee utilizarla. Las tecnologías existentes se pueden combinar y utilizar para crear nuevos productos y servicios que amplíen las capacidades de Internet.
Desarrollo, gestión y gobernanza colaborativos	Las tecnologías y los estándares de Internet se desarrollan, administran y rigen de manera abierta y colaborativa. Esta colaboración abierta se extiende a la construcción y operación de Internet y los servicios construidos sobre Internet. El proceso de desarrollo y mantenimiento se basa en la transparencia y el consenso, y tiene como objetivo la optimización de la infraestructura y los servicios en beneficio de los usuarios de estas tecnologías.
Apoyar una Internet conectada a nivel mundial	
Accesibilidad ilimitada	Los usuarios de Internet tienen acceso a todos los recursos y tecnologías disponibles en Internet y pueden hacer que los recursos estén disponibles. Una vez que un recurso ha sido puesto a disposición por su propietario de alguna manera, no hay bloqueo del uso y acceso legítimo a ese recurso por parte de terceros.
Disponible Capacidad	La capacidad de Internet es suficiente para satisfacer la demanda de los usuarios. Nadie espera que la capacidad de Internet sea infinita,

	pero hay suficiente capacidad de conexión (puertos, ancho de banda, servicios) para satisfacer las demandas de los usuarios.
Apoyar una Internet segura	
Confidencialidad de datos de información, dispositivos y aplicaciones	La confidencialidad de los datos, que generalmente se logra con herramientas como el cifrado, permite a los usuarios finales enviar información confidencial a través de Internet para que los intrusos y atacantes no puedan ver el contenido o saber quién se está comunicando. Permitir la transferencia de información confidencial ayuda a crear una Internet segura. La confidencialidad de los datos también se extiende a los datos en reposo en aplicaciones y dispositivos. (Nótese: la "confidencialidad" también contribuye a la privacidad, que es parte de una Internet digna de confianza)
Integridad de la información, aplicaciones y servicios	La integridad de los datos enviados a través de Internet y almacenados en aplicaciones no se ve comprometida. Es decir, la información enviada a través de Internet no debe modificarse en tránsito, a menos que lo indiquen las partes que se comunican (por ejemplo, un bot de subtítulos puede ser útil para convertir las palabras habladas en texto).
Apoyar una Internet confiable	
Confiabilidad, resistencia y disponibilidad	Internet es confiable cuando existen tecnologías y procesos que permiten la prestación de servicios según lo prometido. Si, por ejemplo, la disponibilidad de un servicio de Internet es impredecible, los usuarios lo observarán como poco confiable. Esto puede reducir la confianza no solo en un único servicio, sino en la propia Internet. La resiliencia está relacionada con la confiabilidad: una Internet resiliente mantiene un nivel de servicio aceptable incluso frente a errores, comportamientos maliciosos y otros desafíos para sus operaciones normales
Responsabilidad	La rendición de cuentas en Internet brinda a los usuarios la seguridad de que las organizaciones e instituciones con las que interactúan actúan directa o indirectamente de manera transparente y justa. En una Internet responsable, se pueden identificar entidades, servicios e información y las organizaciones involucradas serán responsables de sus acciones.

Privacidad	La privacidad en Internet es la capacidad de las personas y los grupos de poder comprender y controlar qué información sobre ellos se recopila y cómo, y controlar cómo se usa y se comparte. La privacidad a menudo incluye aspectos de anonimato, eliminando los vínculos entre los datos, los dispositivos y las sesiones de comunicación y las identidades de las personas a las que pertenecen.
-------------------	--

Para obtener más información sobre cómo realizar una evaluación del impacto de Internet, consulte nuestra guía en línea: **Cómo realizar un resumen del impacto de Internet** utilizando el **kit de herramientas de evaluación del impacto de Internet**.¹⁰⁷

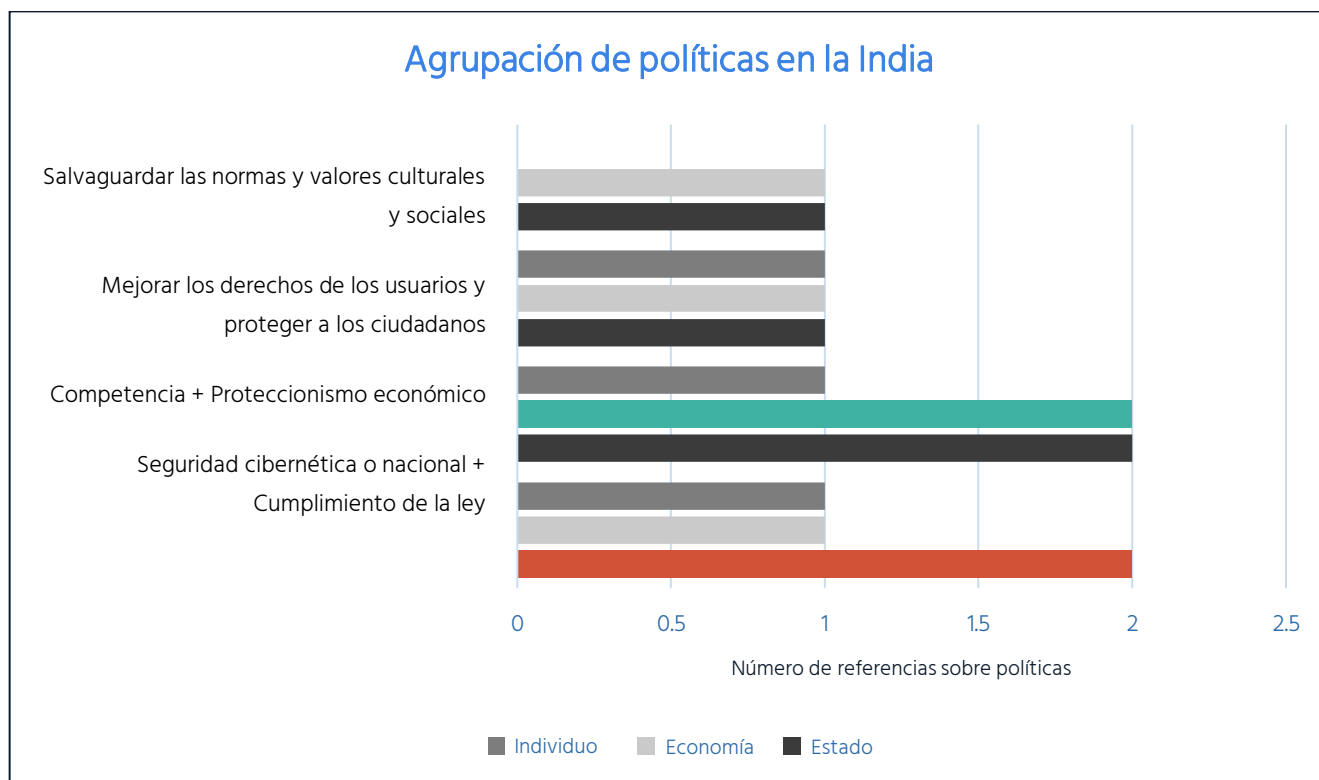
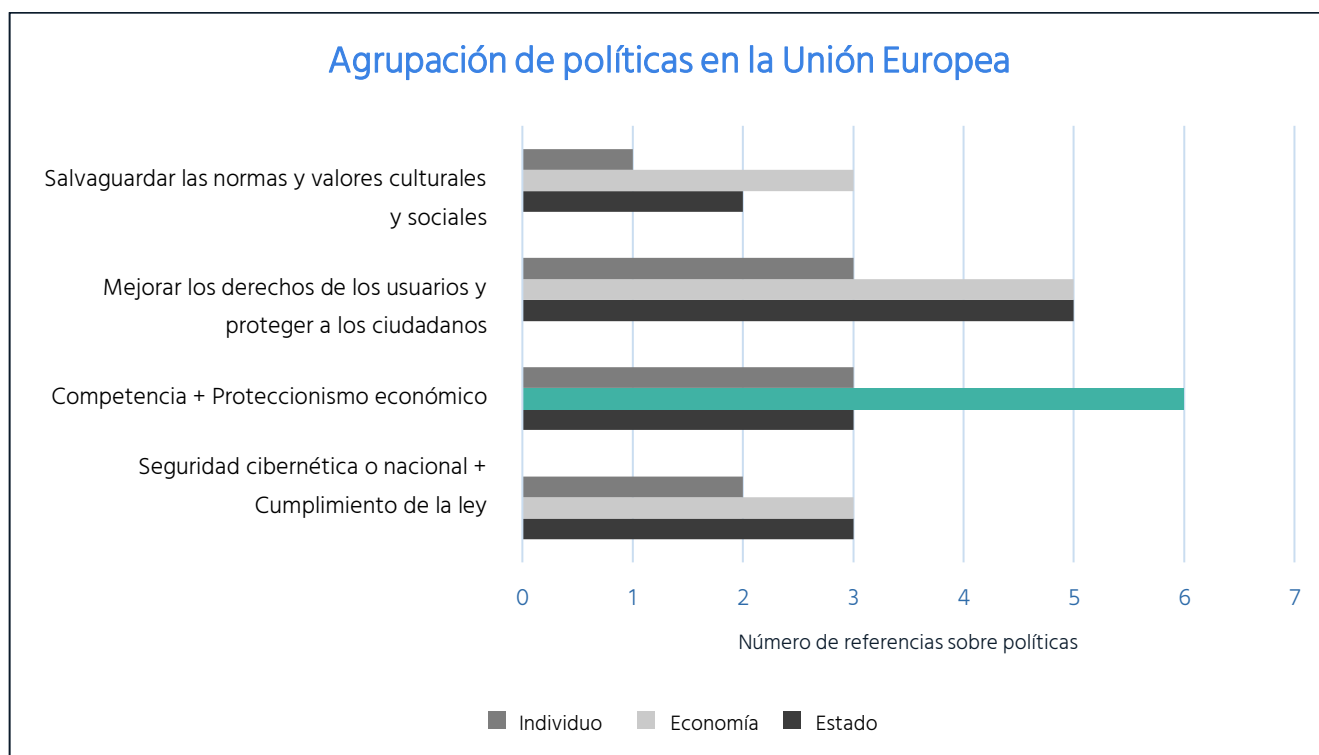
Apéndice III: Metodología de investigación para tipos de soberanía digital

Este estudio analizó treinta y cuatro políticas en tres regiones en función de las dos categorías transversales de objetivos de política y actores empoderados. Cada política se traza en el gráfico en función de lo que (a) quiere lograr y (b) a quién empodera para lograr la política. Por ejemplo, si una política tiene como objetivo la Seguridad Nacional y empodera al Estado, agregamos un punto a la celda Seguridad Nacional*Estado. Si la misma política también empodera al individuo, agregamos un punto a la celda Seguridad Nacional*Individuo. Si otra política en esta jurisdicción también tiene como objetivo la Seguridad Nacional y empodera al Estado, agregamos otro punto a la celda correspondiente y lo sumamos a 2.

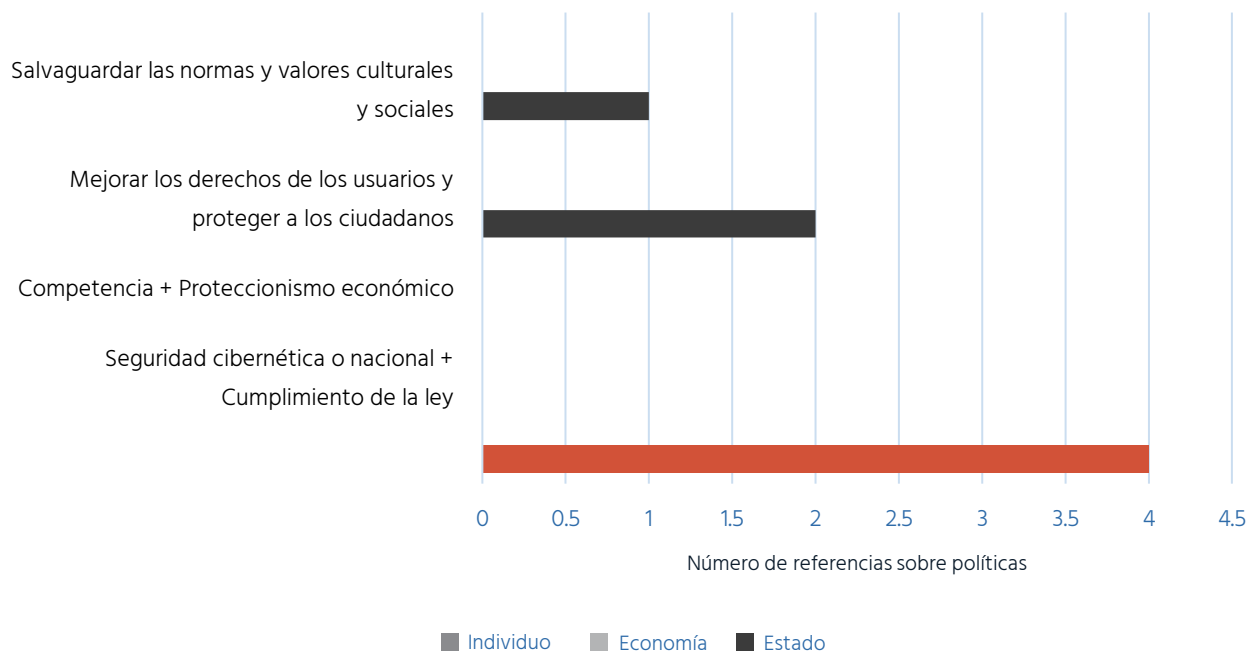
El gráfico inmediatamente inferior muestra que las políticas se agrupan en distintas áreas, según sus objetivos. El análisis de estos grupos por parte de entidades facultadas, mostró grupos aún más estrictos que nos permitieron identificar los tipos de políticas clave; un grupo distinto de políticas cae en celdas de Seguridad Nacional/Estado y Cumplimiento de la Ley/Estado, mientras que las políticas del tipo “enfocadas en la economía” están más centradas en Competencia/Economía y Normas/Sociedad). Es importante señalar que algunos de los países muestran una mezcla de los dos tipos dominantes, mientras que otros tienen un tipo que se destaca. El primer gráfico muestra varios países donde estos patrones y los tipos correspondientes son más visibles.

¹⁰⁷ Internet Society, "How to Conduct an Internet Impact - Brief Internet Impact Assessment Toolkit", <https://www.internetsociety.org/resources/doc/2021/how-to-conduct-an-internet-impact-brief/>

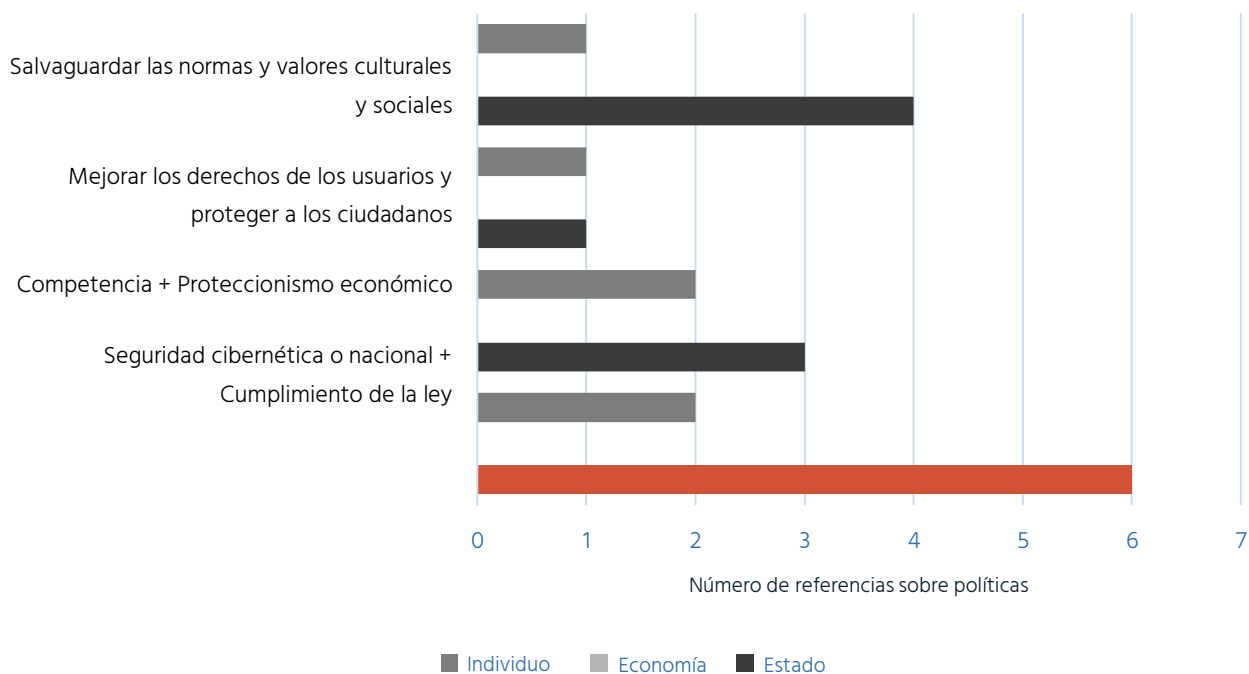
Patrones de políticas en diferentes países que exponen 2 tipos distintos de soberanía digital, marcados en rojo y verde.



Agrupación de políticas en Rusia



Agrupación de políticas en China



Anexo IV: Cuadros de Políticas y Propuestas Analizadas

Políticas del Tipo Seguridad Nacional

Seguridad Nacional y Estado de derecho por Estado

Estrategia de Transformación digital de África (2020 -2030)

Unión Africana: Convenio de Malabo: Convenio sobre Ciberseguridad y Protección de Datos Personales

Australia: Estrategia de seguridad cibernética (2020)

Australia: Estrategia de Transformación Digital (2018)

Australia: Marco de certificación de alojamiento (2021)

China: Estrategia Internacional de Cooperación en el Ciberespacio (2017)

China: Ley de Protección de Información Personal (2021)

Regulaciones de nombres de dominio de Internet de China (2017)

China: Ley de Ciberseguridad (2017)

China: Ley de seguridad de datos (2021)

UE: Ley de datos (propuesta de 2022)

UE: La estrategia de ciberseguridad de la UE para la década digital (2020)

UE: Ley de Servicios Digitales (propuesta de 2022)

India: Certificado en Direcciones de ciberseguridad

India: Proyecto de ley de protección de datos (2021)

Indonesia: Reglamento del Gobierno (71/2019)

Italia: Estrategia Nacional de Ciberseguridad (2022)

Rusia: "Leyes Yarovaya" (2016): Ley Federal "Sobre la Lucha contra el Terrorismo" y "Código Penal de la Federación Rusa y Código de Procedimiento Penal de la Federación Rusa"

Rusia: Ley de Localización de Datos (modificación de 2014)

Rusia: Reglas para la gestión centralizada de una red de comunicación pública (2019), ampliamente conocida como "Ley soberana de Internet de Rusia"

Ruanda: Política de revolución de datos (2017)

Sudáfrica: Política Nacional de Datos y de la Nube (propuesta)

Vietnam: Ley de Ciberseguridad (2018)

Vietnam: Establecimiento del Comando Cibernético (2018)

Políticas del Tipo Fortalecimiento de la Economía

Fortalecimiento de la economía a través de la competencia

Unión Africana: Estrategia de transformación digital de África (2020 - 2030)

UE: Ley de datos (propuesta - 2022)

UE: Ley de datos, comentarios de Thierry Breton, Comisario de Mercado Interior

UE: Ley de Mercados Digitales (propuesta de 2022)

UE: Nube europea (Discurso sobre el estado de la unión de la presidenta de la CE, Ursula von der Leyen, 2020) (2020)

UE: GAIA-X (2020)

UE: Dando forma al futuro digital de Europa (2019)

India: Política de Centros de Datos (2020)

India: Proyecto de Ley de Protección de Datos (2021)

Nigeria: Política de Computación en la Nube (2019)

Sudáfrica: Política Nacional de Datos y de la Nube (propuesta)