EDICIONES COMPLUTENSE

Geopolítica(s). Revista de Estudios sobre Espacio y Poder
ISSN: 2172-3958

ARTÍCULO

Internet en la agenda de seguridad nacional rusa: RuNet y la soberanía digital

Abdiel Hernández Mendoza
Profesor de Tiempo Completo en la Escuela Nacional de Estudios Superiores Unidad Juriquilla, Universidad Nacional Autónoma de México
e-mail: abdielhernandez@comunidad.unam.mx
ORCID: https://orcid.org/0000-0002-5484-647X

http://dx.doi.org/10.5209/geop.95098 Recibido: 17/03/2024 • Aceptado: 17/09/2025

Resumen. El presente artículo examina el proyecto *RuNet* —componente estratégico de la agenda de seguridad nacional rusa—, analizando su papel en la construcción de soberanía digital frente a las dinámicas de fragmentación de Internet global. Se realiza a través de un diseño cualitativo exploratorio-descriptivo con triangulación metodológica y enfoque transductivo, se estudió la implementación de la Ley Federal 90-FZ (2019) y su arquitectura institucional. A su vez, se implementó un análisis bibliométrico de 457 fuentes académicas (2020-2025), legislación oficial rusa y reportes técnicos especializados. Los resultados revelan que *RuNet* trasciende la mera respuesta defensiva ante sanciones occidentales, constituyendo un modelo exportable de resistencia tecnológica hacia el espacio euroasiático y países BRICS. La investigación identifica una triada operativa Estado-academia-industria que configura el espacio digital como territorio de poder geopolítico. Al final del artículo, se reflexiona que la soberanía digital rusa representa un paradigma de fragmentación controlada de Internet que desafía la hegemonía occidental en el ciberespacio, proyectando alternativas de gobernanza digital para la construcción de órdenes regionales alternativos al sistema liberal dominante.
Palabras clave. Rusia; RuNet; soberanía digital; internet; ciberseguridad.

EN The Internet on Russia's National Security Agenda: RuNet and Digital Sovereignty

Abstract. This article examines the RuNet project—a strategic component of Russia's national security agenda—analysing its role in building digital sovereignty in response to the fragmentation dynamics of the global Internet. Using an exploratory–descriptive qualitative design with methodological triangulation and a transductive approach, it studies the implementation of Federal Law 90-FZ (2019) and its institutional architecture. A bibliometric analysis of 457 academic sources (2020–2025), official Russian legislation, and specialized technical reports was also conducted. The results reveal that RuNet transcends a mere defensive response to Western sanctions, constituting an exportable model of technological resistance across the Eurasian space and BRICS countries. The research identifies an operational triad—state, academia, and industry—that shapes the digital space as a territory of geopolitical power. In conclusion, the article reflects that Russian digital sovereignty represents a paradigm of controlled fragmentation of the Internet that challenges Western hegemony in cyberspace, projecting alternative models of digital governance for the construction of regional orders distinct from the dominant liberal system.
Keywords. Russia; RuNet; digital sovereignty; Internet; cybersecurity.

PT A internet na agenda de segurança nacional russa: RuNet e a soberania digital

Resumo. Este artigo examina o projeto *RuNet* – um componente estratégico da agenda de segurança nacional da Rússia – analisando seu papel na construção da soberania digital diante da dinâmica de fragmentação da internet global. Utilizando um delineamento qualitativo exploratório-descritivo com triangulação metodológica e uma abordagem transdutiva, estudou-se a implementação da Lei Federal 90-FZ (2019) e sua arquitetura institucional. Também foi realizada uma análise bibliométrica de 457 fontes acadêmicas (2020-2025), legislação oficial russa e relatórios técnicos especializados. Os resultados revelam que o *RuNet* transcende uma mera resposta defensiva às sanções ocidentais, constituindo um modelo exportável de resistência tecnológica para o espaço eurasiano e os países do BRICS. A pesquisa identifica uma tríade operacional Estado-academia-indústria que configura o espaço digital como um território de poder geopolítico. Ao final do artigo, reflete-se que a soberania digital russa representa um paradigma de fragmentação controlada da Internet que desafia a hegemonia ocidental no ciberespaço, projetando alternativas de governança digital para a construção de ordens regionais alternativas ao sistema liberal dominante.
Palavras-chave. Rússia; RuNet; soberania digital; internet, segurança cibernética.

Cómo citar. Hernández Mendoza, A. (2025). Internet en la agenda de seguridad nacional rusa: RuNet y la soberanía digital. *Geopolítica(s). Revista de Estudios sobre Espacio y Poder*, *16*(2), 239-259

> *En 1957 se lanzó al espacio un objeto fabricado por el hombre y durante varias semanas circundó la Tierra según las mismas leyes de gravitación que hacen girar y mantienen en movimiento a los cuerpos celestes: Sol, Luna y estrellas. Claro está que el satélite construido por el hombre no era ninguna luna, estrella o cuerpo celeste que pudiera proseguir su camino orbital durante un período de tiempo que, para nosotros, mortales sujetos al tiempo terreno, dura de eternidad a eternidad. Sin embargo, logró permanecer en los cielos; habitó y se movió en la proximidad de los cuerpos celestes como si a modo de prueba, lo hubieran admitido en su sublime compañía*.
>
> Hannah Arendt (2016).

Introducción y Metodología

En enero de 2019 entró en vigor la denominada «Ley de Internet soberana» de la Federación Rusa. Este hecho constituyó un hito jurídico en la disputa geopolítica característica del siglo XXI, en el marco de la cuarta revolución industrial. Esta normativa refleja la relevancia de las tecnologías de la información como recursos geoestratégicos clave para la consolidación del poder ruso en la construcción de un nuevo orden mundial que dicho país concibe.

La evolución de estas tecnologías se vincula a la moderna disputa geoeconómica entre Estados Unidos (EE UU) y China, cuyos intereses están manifestados —entre otros actores— por gigantes tecnológicos estadounidenses *Google-Macintosh* y chinos *Huawei-TikTok*. El análisis de esta confrontación revela que las guerras complejas del siglo XXI involucrarán a todos los agentes vinculados a las tecnologías digitales avanzadas; en dichos escenarios, la obtención de metadatos se convierte en un objetivo fundamental para garantizar ventajas.

En este contexto, el presidente ruso, Vladimir Putin, anunció la creación de una Internet soberana con capacidad para operar una red 5G autónoma. Dicha iniciativa constituye —en términos

oficiales— un esfuerzo por proteger los metadatos generados por sus usuarios nacionales y así, mantener la operatividad nacional ante una eventual desconexión de la red global.

Tras el anuncio, Occidente, cuestionó los alcances estatales de dicha ley, argumentando su potencial para silenciar la disidencia política. Sin embargo, este marco legal representa un obstáculo para los mecanismos de extracción ilegal de datos —denominados puertas traseras (López Delgado, 2007, p. 11)— en la nación rusa.

A partir de este punto, las grandes potencias tecnológicas perfilan estrategias que integran instrumentos legales, militares, financieros, entre otros en una contienda que abarca desde el dominio ultraterrestre hasta el ciberespacio. En consecuencia, la ciberseguridad en un componente fundamental para la Seguridad Nacional de Rusia.

Ante este escenario, el presente artículo busca examinar el papel del proyecto *RuNet* dentro de la agenda de seguridad nacional rusa, sobre todo en el marco del conflicto armado con Ucrania. Esta premisa sugiere que el Estado ruso considera el control de Internet como una cuestión de Seguridad Nacional enmarcando su acción jurídica en el paradigma de la soberanía digital.

Así, se tiene por objetivo analizar el alcance del proyecto *RuNet* y su relación con la soberanía digital, esto mediante la evaluación de las medidas adoptadas por Rusia orientadas a asegurar una infraestructura de Internet autónoma; que le garantice su independencia de los sistemas globales —como los Nombres de Dominio (DNS, por las siglas en inglés de *Domain Name System*)—, permitiendo así comprender sus implicaciones para la seguridad nacional rusa.

Por lo que, la presente investigación se basó en un diseño cualitativo exploratorio-descriptivo con triangulación metodológica, el cual se orientó a realizar un análisis crítico de la soberanía digital rusa como fenómeno geopolítico contemporáneo.

El estudio se fundamenta en un enfoque transductivo que, partiendo de lo conocido, «articula lo nuevo en lo conocido» (Montañés y Martín, 2017, p. 43), conceptualizando el objeto de estudio —la soberanía digital rusa— como una práctica social generadora de realidad, sustentada en un «objeto posible que podemos emplear junto con las actividades más convencionales de deducción e inducción» (Lefebvre, 2003, p. 5).

Bajo este enfoque se examinó que el proyecto *RuNet* va más allá de un fenómeno técnico-jurídico, es posible comprenderlo como un ejemplo contemporáneo de la reconfiguración de la soberanía nacional en la era digital, donde la autonomía tecnológica se erige a manea de instrumento de proyección de poder geopolítico.

A partir de ello, se consideró un caso instrumental —*RuNet*—, a ser abordado desde una perspectiva sistémico-histórica que identificara las interdependencias entre los actores estatales, académicos e industriales en la configuración de la soberanía digital rusa. Esta aproximación se considera fundamental para caracterizar el actual contexto mundial en el que se disputa la hegemonía digital y el control de sus interconexiones, generando procesos de retroalimentación permanente debido a la agencia de los operadores de subsistemas. El análisis diacrónico —acorde a la transducción— de larga duración permite comprender la tecnología como dispositivo de dominación geopolítica.

A continuación, se describen las tres categorías principales en torno a las fuentes analizadas:

1. Primarias y oficiales: legislación rusa (Ley Federal 90-FZ, decretos presidenciales), documentos técnicos de Roskomnadzor, discursos oficiales del Kremlin y reportes de organismos estatales rusos. Cabe señalar que los criterios de inclusión se basaron en una temporalidad 2019-2025, accesibilidad pública y relevancia directa con *RuNet*.
2. Literatura académica especializada, con 457 documentos extraídos de *Web of Science* (2020-2025) mediante palabras clave como «Runet», «Russian sovereign internet», «sovereign internet Russia» y «Russia Internet strategy», complementados con búsquedas en *Lens* y *OpenAlex*, limitándose a artículos *peer-reviewed*, capítulos de libro y libros académicos en español, inglés y ruso publicados entre 2020-2025.
3. Fuentes técnicas y corporativas: reportes de ciberseguridad (*Kaspersky*), documentos de foros especializados (*Russian Internet Governance Forum*) y análisis de consultoras internacionales (*McKinsey & Company*).

Entre las herramientas de análisis empleadas se utilizó el *software VOSviewer* para generar el análisis bibliométrico y la visualización de redes de conocimiento; de la misma manera: el análisis crítico del discurso para la deconstrucción de narrativas políticas, el análisis sistémico para la identificación de interdependencias entre actores y la perspectiva diacrónica para el análisis histórico de transformaciones institucionales.

Para estudiar la forma en que esta dinámica global configuró agendas securitizadas bajo un esquema de división hemisférica, se parte de una revisión de la literatura en el apartado 1 la cual se apoya de un análisis bibliométrico. En el apartado 2, llamado «Revoluciones industriales y seguridad nacional», se desarrolla una de las tesis centrales de Miguel García Reyes (2007), relativa a la articulación del eje: revolución energética – revolución industrial – orden geopolítico – amenaza a la seguridad.

A partir de los resultados de ese análisis inicial, se examinó el panorama geopolítico contemporáneo. En este marco, el apartado 3, titulado: «Confrontación geopolítica en la era de la digitalización», muestra cómo el factor tecnológico y la concentración de poder asociada constituyen ejes centrales de rivalidad entre potencias del siglo XXI. Esta dinámica conduce al análisis de las acciones rusas en la coyuntura actual, abordado en el apartado 4, nombrado: «Ley rusa de Internet Soberana. TI y Seguridad nacional», que aborda la estrategia del Kremlin para proteger sus intereses nacionales en escenarios de guerra digital.

En la reflexión final, se plantea: «¿Qué perspectivas enfrenta Rusia en la era de la digitalización?» Se llega a comprender la revitalización de políticas económicas planificadas con horizonte de lago plazo en la nación euroasiática; en este caso específico, en el ámbito digital; ahora, el Estado busca neutralizar amenazas potenciales mediante el control estratégico de este espacio.

Esta investigación retoma el contexto de la fragmentación digital global y el surgimiento de modelos alternativos de gobernanza de Internet que desafían la hegemonía occidental en el ciberespacio. El caso de *RuNet* adquiere relevancia paradigmática no solo como respuesta defensiva a las sanciones internacionales, sino como modelo exportable hacia el espacio euroasiático y los países BRICS, configurando una arquitectura de resistencia tecnológica que trasciende las fronteras nacionales rusas.

Esta dinámica se inserta en el marco teórico de la soberanía digital como dimensión que deben seguir abordando los estudios de la seguridad nacional, donde el control de infraestructuras críticas de información se convierte en instrumento de proyección de poder geopolítico y construcción de órdenes regionales alternativos al sistema liberal occidental.

1. Revisión de la literatura

El análisis de la Ley de Internet Soberano de Rusia, *RuNet,* parte de un estudio de la bibliografía desarrollada en el lapso 2020-2025 cuyo fin es identificar tendencias de investigación, así como interpretar el panorama académico que sustenta este caso de estudio y destacando su importancia estratégica desde una perspectiva geopolítica.

Para esta tarea se examinaron patrones de coautoría, redes institucionales y colaboraciones entre países, desde donde se localizaron tendencias de investigación que son utilizadas en los apartados subsecuentes desde sus implicaciones geopolíticas. La investigación bibliométrica se realizó con datos extraídos de la base de *Web Of Science* (WoS en Clarivate, 2025) utilizando las palabras clave: («Runet» OR «Russian sovereign internet» OR «sovereign internet Russia» OR «Russia Internet strategy»).

Se obtuvieron 457 resultados en una delimitación temporal entre 2020 y 2025, la cual se basó solo en artículos, capítulos de libro y libros. Los datos fueron analizados mediante la herramienta *VOSviewer* (Van Eck y Waltman, 2010)) pero se complementó con búsqueda en *Lens* (2025) y *OpenAlex* (2025), que se descartaron por arrojar menos resultados. El enfoque combinó técnicas cuantitativas con interpretación cualitativa para destacar la relevancia de temas como la soberanía digital en lo general y *RuNet* en lo particular.

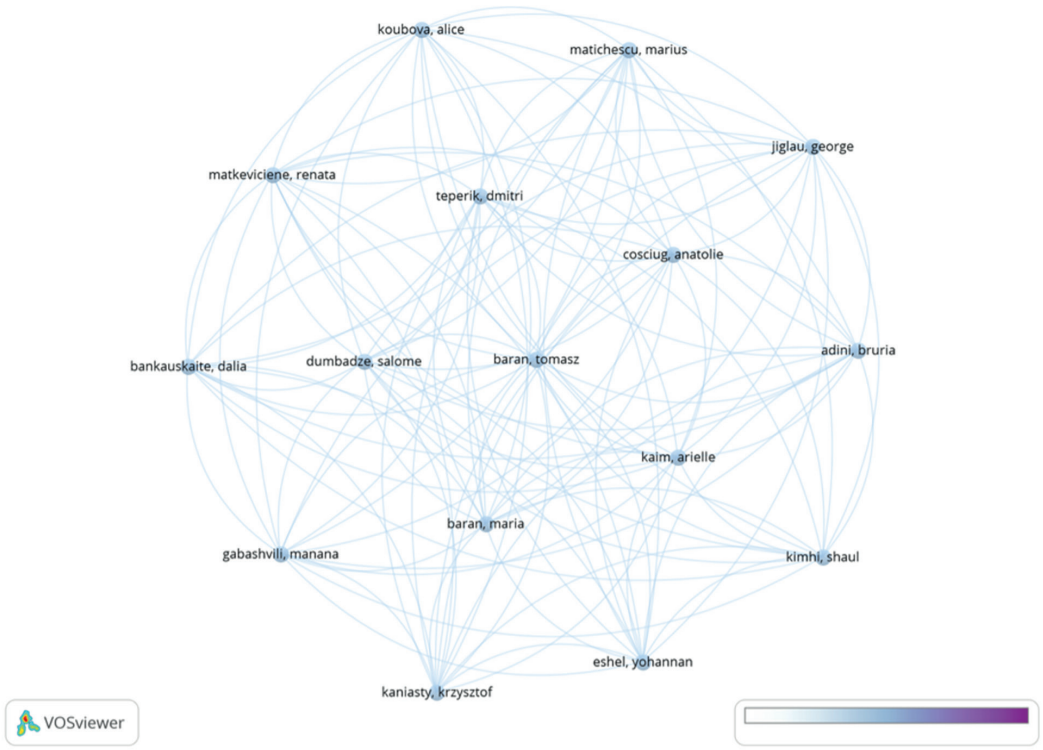
Respecto a las obras halladas, el estudio mostró un conjunto principal de ocho autores, con métricas de producción idénticas: 2 documentos, 8 citas y una fuerza total de enlace de 30 (Tabla 1

y Figura 1). Debido a esta homogeneidad se realizó una revisión detallada de los perfiles académicos destacados, mostrados en la Tabla 1.

En este clúster académico se encuentra la Profesora Bruria Adini, de la Universidad de Tel Aviv, especialista en gestión de desastres y en resiliencia de sistemas de salud, autora de «Impact of the war in Ukraine on resilience, protective, and vulnerability factors» (Kimhi, Eshel, Marciano y Adini, 2023); de Lituania, perteneciente a la Universidad de Vilna se encuentra Dalia Bankauskaité, experta en comunicación estratégica y resiliencia social en la región Báltica, ella escribe desde la *Lithuania's Total Defense Review* (Bankauskaité y Šlekys, 2023); ambas autoras se relacionan con los estudios de mayor fuerza de enlace, junto con Maria Baran y Tomasz Baran (Kimhi *et al*., 2024), psicólogos enfocados en la resiliencia social y la adaptación en contextos de conflicto; sus estudios enfatizan el estrés derivado de la guerra en curso.

Este hallazgo permitió identificar la complejidad del control de la información y el papel de la desconexión digital como tácticas de control vinculadas con la política digital y temas de seguridad humana, las cuales no se disocian de elementos como «Covid-19», factor exógeno asociado a momentos de crisis, presente en las palabras clave de este estudio.

Figura 1. Grafo de coocurrencia de autores con mayor fuerza de enlace



Nota. Elaboración propia con base en datos de *WoS* y el uso de *VOSviewer*.

Tabla 1. Autores con mayor fuerza total de enlace

Nº.	*Autor*	*Adscripción*	*Docs.*	*Citas*	*Fuerza total del enlace*
1	Adini, Bruria	Tel Aviv University	2	8	30
2	Bankauskaite, Dalia	Center for European Policy	2	8	30
3	Baran, Maria	SWPS University, Polonia	2	8	30
4	Baran, Tomasz	(Coautor) SWPS University	2	8	30
5	Cosciug, Anatolie	University of Bucharest,	2	8	30
6	Dumbadze, Salome	Georgian Institute of Public Affairs	2	8	30

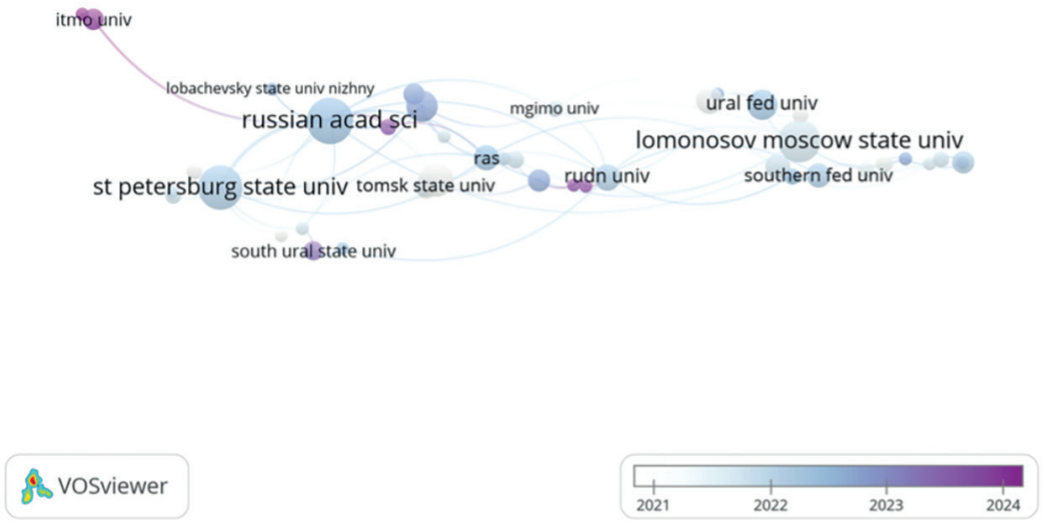
Nota. Elaboración propia con base en datos de *WoS* y el uso de *VOSviewer*.

En la Figura 2 y en el Tabla 2 se muestra la primacía de las instituciones rusas en la producción de conocimiento en torno a *RuNet*, siendo la Academia Rusa de las Ciencias (RAS), la Universidad Estatal de San Petersburgo, la Universidad Estatal de Moscú (Lomonosov) y la Escuela Superior de Economía las principales. Este hecho refleja una estrategia nacional rusa integral que vincula a la academia con los intereses nacionales rusos.

Cabe hacer unas precisiones en torno a esta simbiosis academia-Estado. La RAS es un centro de investigación que provee «informes analíticos y otros materiales a las autoridades estatales, instituciones y organizaciones» de Rusia según el *Institute of Europe* de la RAS (2025).

Situación similar se aprecia con la Universidad Estatal de Moscú (MGU), la cual es concebida como una institución federal del gobierno ruso, desde donde se forma a especialistas para adquirir práctica en los niveles más altos del gobierno, entre ellos la Duma Estatal y la Administración Presidencial (Moscow State University, 2025).

Figura 2. Grafo de coocurrencia para universidades desde donde más producción académica se realiza



Nota. Elaboración propia con base en datos de *WoS* y el uso de *VOSviewer*.

Tabla 2. Universidades con mayor fuerza de enlace en la producción de literatura

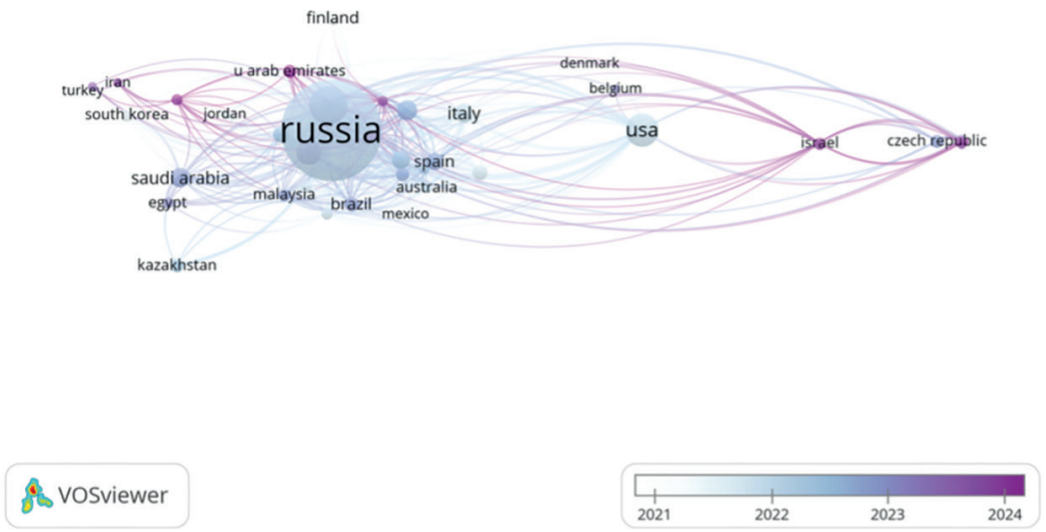
N°.	*Organización*	*Documentos*	*Citas*	*Fuerza total del enlace*
1	Russian Acad Sci	34	50	22
2	St Petersburg State Univ	31	54	13
3	Lomonosov Moscow State Univ	28	67	12
4	Nati Res Univ Higher Sch Econ	18	310	11
5	RAS	10	38	10
6	RUDN Univ	11	124	10
7	Hse Univ	15	59	7
8	Financial Univ Govt Russian Federation	4	9	6

Nota. Elaboración propia con base en datos de *WoS* y el uso de *VOSviewer*.

Por su parte, en la Figura 3 y Tabla 3, los datos bibliométricos revelan el papel central que desde Rusia se le da a la producción de conocimiento en este tema. Esta situación muestra que el elevado número de documentos producidos (363) es acorde con una estrategia de Estado sistematizada para la construcción de un marco teórico y técnico que sustente su modelo de gobernanza digital autónoma.

Mientras China, con menor producción, pero alta influencia por cita (1026/54), proyecta un modelo de alcance global. India, con una posición intermedia (501/24), están presentes para aportar a estos estudios. La presencia de Occidente (EE UU, Italia, Inglaterra, Francia y Alemania) con alta influencia por publicación sugiere que, pese a la fragmentación geopolítica, el conocimiento occidental mantiene relevancia en temas de la gobernanza digital.

Figura 3. Grafo de coocurrencia para países desde donde más producción académica se realiza



Nota. Elaboración propia con base en datos de *WoS* y el uso de *VOSviewer*.

Tabla 3. Países con mayor producción de literatura académica

No.	*País*	*Documentos*	*Citas*	*Fuerza total del enlace*
1	Rusia	363	2278	235
2	Rep. Popular China	54	1026	125
3	Estados Unidos	40	846	91
4	India	24	501	72
5	Italia	14	440	63
6	Inglaterra	15	235	62
7	Francia	10	521	57
8	Alemania	12	268	52

Nota. Elaboración propia con base en datos de *WoS* y el uso de *VOSviewer*.

Para finalizar este estudio de la literatura bajo un análisis bibliométrico, la Figura 4 y el Tabla 4 resultaron reveladores. Se identificó una evolución conceptual significativa en el estudio del espacio digital ruso. Así, al observar una transición terminológica desde palabras clave genéricas como «redes sociales» o «digitalización» hacia conceptos estratégicos como «censura rusa», «cibernética» y «manipulación», da muestra de una maduración del discurso académico que ahora se enfoca en las dimensiones de seguridad nacional y soberanía digital.

Con esta reorientación se comprende que *RuNet* no es solo una infraestructura tecnológica, es posible decir que se configura como un instrumento de política estatal diseñado para garantizar la autonomía estratégica de Rusia en un contexto de confrontación informacional global. La coocurrencia de términos también evidencia que la investigación se centra en los mecanismos de defensa del espacio digital nacional, en línea con la doctrina oficial de protección contra amenazas externas.

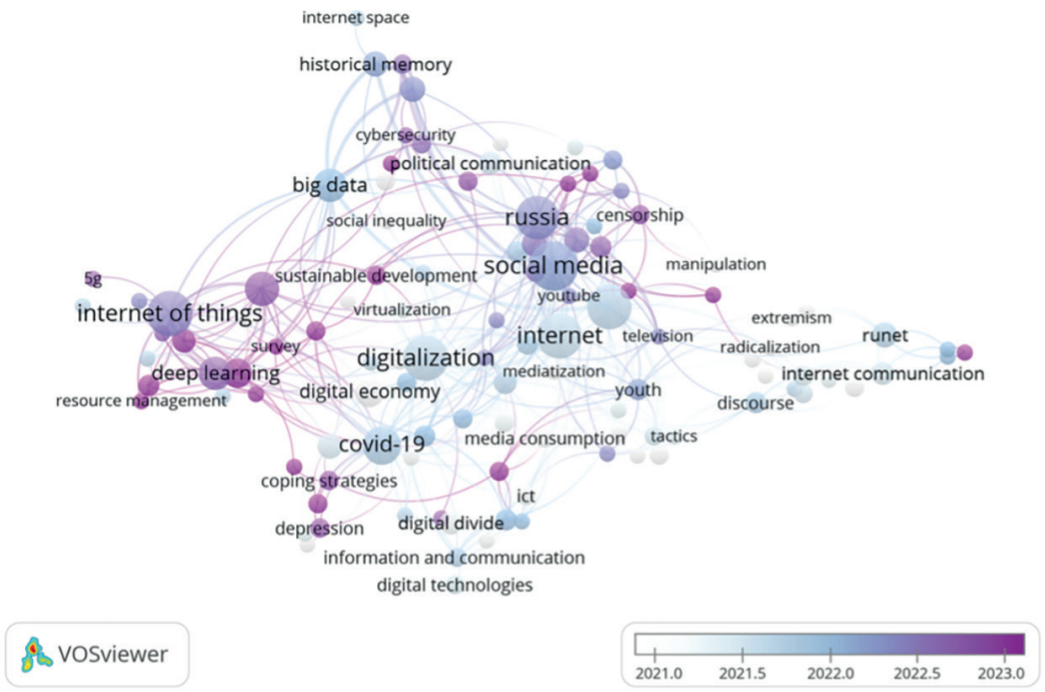
Cabe destacar que, las implicaciones geopolíticas de la estrategia *RuNet* van más allá del ámbito nacional, constituyen un caso paradigmático de la fragmentación controlada de Internet (*splinternet*). Esta iniciativa representa una reafirmación de la soberanía estatal en el ciberespacio, donde Rusia —desde una posición *de jure*— establece fronteras digitales y regula –desde una posición *de facto*— los flujos de datos transnacionales.

La arquitectura paralela desarrollada mediante leyes de localización de datos y equipos TSPU (por sus siglas en inglés, *Point of Presence* o Punto de Acceso) no debe reducir su interpretación a la mera censura, permite aquí pensar en una estrategia de interés nacional de desconexión controlada que, permite a Moscú mantener la estabilidad social y contrarrestar campañas informativas externas. La migración de sistemas autónomos en regiones como Donbás confirmaría el por qué la infraestructura digital se ha convertido en una extensión de la soberanía territorial, proyectando poder estatal en el ciberespacio conforme a los intereses nacionales rusos.

Con los datos obtenidos se visibiliza que la investigación sobre *Runet* se desarrolla sobre todo en instituciones académicas rusas estatales, las cuales funcionan centros de desarrollo académico para teorizar la soberanía digital. Esta relación intrínseca Estado-academia refleja un enfoque coherente con la visión estratégica rusa de la gobernanza de Internet, donde la soberanía digital se concibe como componente esencial de la seguridad nacional.

Este ejercicio permitió comprender que, para futuras investigaciones, sería pertinente un análisis comparativo de los modelos de Internet soberano en el espacio eurasiático, examinando cómo estas iniciativas contribuyen a la formación de un orden internacional multipolar en el ciberespacio, siempre desde una perspectiva analítica libre de sesgos ideológicos.

Figura 4. Grafo de coocurrencia para palabras clave de autor más utilizadas



Nota. Elaboración propia con base en datos de *WoS* y el uso de *VOSviewer*.

Tabla 4. Palabras clave de autor más utilizadas

No.	*Palabra clave*	*Ocurrencias*	*Fuerza total del enlace*
1	Social media	26	46
2	Social networks	21	45
3	Internet	22	39
4	Digitalization	22	36
5	Internet of things	22	36
6	Russia	20	36
7	Big data	12	34
8	Covid -19	16	29

Nota. Elaboración propia con base en datos de *WoS* y el uso de *VOSviewer*.

2. Revoluciones industriales y seguridad nacional

La Revolución Industrial europea (siglo XVII) transformó desde su estructura la evolución humana al modificar patrones cotidianos: desde sistemas alimentarios hasta constructos culturales, hábitos, pasatiempos y relaciones laborales, entre otras costumbres que persisten en el siglo XXI. Para comprender este proceso, resulta esencial examinar los modos de producción surgidos en ese período.

Desde entonces, se observa que la capacidad inventiva industrializada establece una conexión simbiótica entre innovación tecnológica y los recursos energéticos empleados en motores, otor-

gándole sentido político con tendencia a la expansión global. Esta premisa se sustenta en hitos tecnológicos clave: desde la máquina de vapor impulsada por carbón mineral hasta los transistores, circuitos integrados, microprocesadores, biotecnología y nanotecnología, entre otros que se siguen produciendo en la actual revolución digital. Todos estos desarrollos dependen de matrices energéticas basadas en hidrocarburos (petróleo, carbón mineral y gas natural) y fuentes alternativas (eólica, mareomotriz, geotérmica y solar).

La operatividad de estos hitos tecnológicos requiere garantizar el acceso a los recursos crítico-estratégicos (The White House, 2021). Así, minerales y fuentes de energía constituyen elementos fundamentales que no solo son objeto de prospección global, sino también de disputa geopolítica para materializar tecnologías definitorias del devenir humano. Hasta 2025, la propia existencia de la inteligencia artificial demanda producir energía y explotar yacimientos (petróleo, hierro, oro, litio, entre otros), para producir y dar funcionalidad a los dispositivos.

La relación entre revolución industrial y explotación de recursos pone en evidencia una complejización progresiva, generando problemas adicionales: accesibilidad industrial, distribución mediante redes globales de valor y crisis civilizatorias como el colapso ambiental (Ornelas, 2013). Surgen entonces dos cuestiones centrales: ¿qué actores poseen capacidad de acceso a los recursos? Y ¿quiénes detentan el conocimiento para su aprovechamiento industrial? Se identifican así agentes con poder para implementar producciones estratégicas que disputan la hegemonía global (Ceceña y Barreda, 1995, pp. 15-51), expandiendo sus modalidades de explotación de recursos y organización política mundial, basadas en valores intrínsecos al sistema de producción capitalista.

Como es conocido, el término «Geopolítica» (León Hernández, 2016) fue marginado en los foros públicos durante cinco décadas posteriores a la Segunda Guerra Mundial (1945-1995), debido a su asociación con el expansionismo nazi. Ello derivó en una agenda dentro del marco de la nueva organización mundial establecida por Estados Unidos y la Unión de Repúblicas Socialistas Soviéticas (URSS), orientada a identificar desafíos a la paz —objetivo fundacional de las Naciones Unidas (ONU)—. En este contexto emergieron los conceptos de *seguridad nacional* e *internacional*, vinculados desde el principio a los intereses de los Estados vencedores (China, Estados Unidos, Francia, Reino Unido y la URSS), miembros permanentes del Consejo de Seguridad de la ONU. Con el tiempo, estos conceptos se segmentaron, especialmente en el ámbito estadounidense tras el fin de la Guerra Fría.

El análisis de la relación entre tecnología y energía desde la perspectiva de la disputa por el poder y las acciones geopolíticas orientadas a materializar una red Internet soberana. Cabe destacar que los Estados con mayores capacidades militares, tecnológicas, económicas y culturales diseñan estrategias de imposición y apropiación transnacionales.

En lo que respecta al ámbito político, los modelos de organización basados en valores —como la democracia liberal— constituyen elementos frecuentes de imposición. En lo económico, predomina la hegemonía del modo de producción capitalista y la implementación de sus técnicas. Asimismo, en la esfera cultural, la mercantilización del conocimiento (patentes, derechos de autor, marcas registradas, denominaciones de origen, entre otros) se presenta como discurso universalista con pretensión democratizadora, mientras funciona como mecanismo de hegemonía cultural que expande una cosmovisión única (Gramsci, 1975, p. 100).

En este sentido, la apropiación constituye un eje analítico para la comprensión de los procesos autónomos implementados por países como Rusia para evitar dependencias externas. Esta trasciende el ámbito militar, manifestándose en esferas comerciales, financieras, industriales y en prácticas de obsolescencia tecnológica programada —que restringen el acceso a bienes esenciales como medicamentos—. Tales prácticas suelen reforzarse mediante embargos económicos occidentales, los cuales facilitan el despojo de los recursos crítico-estratégicos (*in situ* y *ex situ*) y la explotación laboral (Harvey, 2004).

De esta manera, la integración de la triada tecnología-energía-geopolítica revela cómo los Estados centrales del sistema-mundo justifican intervenciones en terceros invocando seguridad nacional, replicando la lógica organicista del *espacio vital* como atributo inherente a las potencias. Estas justificaciones se han adaptado al discurso humanitario (O'Reilly, 2019, p. 119-140), contrastando con la evidencia cotidiana en desastres socioambientales derivados de la crisis civilizatoria.

Derivado de lo anterior, es fundamental analizar la cuarta revolución industrial (*4.0*) y su vínculo con la transición energética. Cada revolución industrial ha estado asociada a transformaciones en el panorama energético mundial, resulta esencial examinar la articulación de esta relación industria-energía. Asimismo, los cambios geopolíticos contemporáneos muestran cómo la producción y uso de las tecnologías constituyen asuntos de seguridad nacional. Destacan dos factores apremiantes:

1. la expansión de mercados tecnológicos, y
2. su protección frente a productores extranjeros.

Dichas dinámicas generan consecuencias observables en la ocupación de espacios estratégicos y el control de sus cadenas productivas; en Eurasia, por ejemplo, con la iniciativa —también digital— *Nueva Ruta de la Seda*.

El éxito de proyectos de esta envergadura requiere de tecnologías innovadoras respaldadas por telecomunicaciones robustas y sistemas de interconexión que garanticen la transmisión remota de información, comunicación e inteligencia operativa. En este contexto, intervenciones en las tecnologías de la información comprometerían no solo la estabilidad económica, también desencadenarían disrupciones sistémicas irreversibles. Por esta razón, el control de redes Internet seguras, estables y autónomas –soberanas– constituye un asunto de seguridad nacional para los Estados, al tiempo que adquiere relevancia como dimensión crítica de la seguridad internacional contemporánea.

3. Confrontación geopolítica en la era de la digitalización

Las amenazas contemporáneas a la seguridad internacional responden a una agenda jerarquizada cuyos componentes vulneran no solo a los Estados particulares, sino al sistema capitalista. En tiempos recientes, el terrorismo continúa señalándose como responsable de múltiples problemáticas globales (Ishchuk, 2022, p. 75). Este concepto, sin embargo, abarca manifestaciones diversas: *narcoterrorismo*, *terrorismo de Estado* y *ciberterrorismo*. Resulta significativo que estos fenómenos suelen emerger en las periferias del sistema-mundo, mientras los centros —autopercibidos como víctimas— suelen no asumir responsabilidad o minimizar su participación en tales dinámicas y también negar-invisibilizar los hitos de otras naciones,

Esta negación resulta familiar en la experiencia rusa. Hanna Arendt (2016) ejemplifica este fenómeno con satélite *Sputnik 1*, cuyo valor simbólico fue subestimado por Occidente pese a constituir un hecho histórico para la humanidad, en especial dentro de las telecomunicaciones. Patrones similares de negación, normalización e invisibilización se repitieron en otros eventos clave: el primer ser vivo en órbita (Laika) y los pioneros humanos en el espacio exterior (Yuri Gagarin, Valentina Tereshkova y Alexei Leonov), logros fundamentales en la exploración cósmica que recibieron escaso reconocimiento occidental.

Esta minimización contrasta con la dimensión identitaria que la cultura rusa otorga a dichos logros, consolidándolos como núcleo simbólico incluso en su dimensión artística que acompaña su cotidianidad como un reforzador identitario. Esto lo evidencia Lukyanenko (2024, p. 23-29), al considerar que el cosmos se instituyó como elemento constitutivo de la identidad cultural soviética vía la producción masiva de objetos cotidianos (porcelanas, pinturas, esculturas, entre otras) que celebran las victorias espaciales. La omnipresencia de estas representaciones —que incluyen estatuillas de Gagarin como «regulador cósmico» hasta vajillas conmemorativas— sigue siendo un dispositivo de memoria colectiva, utilizado para resignificar la exclusión occidental.

En la actualidad, estos acontecimientos continúan siendo objeto de reexamen crítico en la política rusa, a través de una reivindicación activa. Durante una reunión sobre temas de defensa nacional en mayo de 2021, el presidente Vladimir Putin citó al emperador Alexandr III para ilustrar este proceso en tono retórico: «Todos temen nuestra grandeza» (RT, 2021). El presidente ruso enfatiza la percepción de subestimación por parte de Occidente a la historia e intereses rusos; esto contribuye a comprender la construcción de la narrativa geopolítica rusa en el siglo XXI.

No obstante, resulta crucial reconocer que el mundo —más allá de la esfera digital— mantiene interconexiones sistémicas donde la interdependencia entre actores del sistema-mundo es innegable. Tras emerger como sujeto de Derecho Internacional el 1 de enero de 1992, Rusia persiguió de manera constante la aceptación occidental. Esta búsqueda constituyó una constante gubernamental, incluso durante algunos períodos de la presidencia de V. Putin, hasta evidenciarse su relegación a un papel periférico que rehusó a asumir; implementando políticas en torno a «nuevas áreas de producción, alta tecnología y servicios, y la ampliación de la gama de actividades económicas» orientadas al fortalecimiento ruso a 2030 (Presidencia de Rusia, 2025).

Con acciones en ese sentido, Rusia ha pretendido superar los intentos de marginación intensificados mediante la agenda de seguridad jerarquizada por Occidente, la cual interpreta los logros estratégicos y tecnológicos rusos como amenazas al orden liberal liderado por EE UU, impidiendo el avance hacia un sistema multipolar. En un estudio de Vyas (2025), se identifica que la diplomacia transaccional de D. Trump, de nuevo presidente estadounidense desde 2025, instrumentalizó relaciones con aliados y adversarios mediante cálculos costo-beneficio inmediatos, socavando la confianza institucional occidental —vistos en la Organización del Tratado Atlántico Norte— y generando vacíos de poder que Rusia aprovechó para reafirmar su autonomía estratégica. Este paradigma hegemónico ignoró las capacidades rusas en ciberseguridad y modernización militar, consolidando así una percepción rusa de marginalización periférica (Vyas, 2025).

Esta reconfiguración económica es resultado de una fractura geopolítica: hasta 2021 solo Alemania, Estados Unidos e Italia destacaban como socios comerciales significativos (World Bank, 2021). Sin embargo, tras la escalada de sanciones derivadas del conflicto con Ucrania, entre enero y octubre de 2024 China (33.8%), India, Turquía y Bielorrusia se convirtieron en sus principales socios comerciales, consolidando un giro estratégico hacia Eurasia (RBC, 2025) vigente hasta la cumbre de la Organización de Cooperación Shanghái de 2025 en China.

De esta manera, Rusia protagoniza junto a otros actores, entre ellos Brasil, China e India, una transformación epocal del orden internacional —heredado del liderazgo estadounidense del siglo XX— que transita hacia un sistema multipolar donde Moscú y Beijín actúan como agentes clave en su producción. Este desplazamiento del centro de gravedad geopolítico tiene la posibilidad de replicar el declive histórico del Mediterráneo, según Eric Hobsbawm (2003, p. 9), «el más importante centro de influencia económica y política» en su momento.

En este marco, resulta fundamental desarrollar los complejos científico-industriales adaptados a la digitalización y la competencia mercantil. Se desarrolla así una geopolítica específica en torno al espacio infraestructural de Internet y los dispositivos habilitantes de este. En particular, la red 5G representa un elemento clave en las disputas del siglo XXI, especialmente en regiones donde la conectividad integra macroproyectos como la *Internet Euroasiática* (*Eurasischen*), donde otros actores como Alemania desempeñan un papel geoestratégico (Rau, 2021).

Cabe destacar, también, que el control de los espacios de conectividad no solo protege los espacios nacionales, sino que a su vez garantiza el funcionamiento de los sectores estratégicos rusos con independencia de la llamada «red de redes». A través de esta última, es posible que se materialicen ataques —según se muestra en el monitoreo diario de amenazas digitales implementado por la empresa rusa *Kaspersky* (2025)—. Esto confirma que la geopolítica digital implica contener ataques cibernéticos, tarea que requiere capacidades tecnológicas ausentes en diferentes actores dentro de la división digital del trabajo.

Aunado a ello, el dominio de las tecnologías de la información exige asegurar los recursos esenciales para producir los dispositivos digitales del siglo XXI. Esto adquiere relevancia en escenarios de demanda creciente. Según el reporte sobre el Panorama de Tendencias Tecnológicas que presentó *Mckinsey & Company* se refuerza el planteamiento de la simbiosis energía-tecnología:

> se están integrando en una vasta gama de dispositivos y aplicaciones, desde smartphones y electrodomésticos hasta camiones y equipos industriales [...] la demanda global de capacidad de centros de datos podría aumentar entre un 19% y un 22% anual desde 2023 hasta 2030, más del triple de la demanda actual (Yee, Chui, Roberts y Smit, 2025, pp. 22, 45*)*.

Por lo tanto, gestionar dicha coyuntura se convierte en un objetivo prioritario para los actores que buscan controlar las TI como factor geoestratégico de dominio. Ante esto, es esencial examinar las concepciones del espacio digital en el pensamiento ruso contemporáneo, lo cual enriquecerá el análisis de su disputa geopolítica (Ver Tabla 5).

Tabla 5. Concepciones desde la academia rusa del espacio digital

Nº.	*Autor(a)*	*Concepto*
1	A. A. Ivin	El espacio es un concepto fundamental del pensamiento humano, que revela el carácter multilateral de la existencia del mundo como un todo único, así como su licuación.
2	S. N. Ikonnikova y V. P. Bolshakov	[...] un tipo de realidad absolutamente nuevo, que se asemeja en muchos aspectos al término «realidad virtual». Su constante transformación y extensión a nuevos grupos sociales y territorios, por lo que podemos concluir que el espacio digital tiene un carácter definitivamente transnacional.
3	S. E. Zuev	Realidad de la información. Espacio informativo: la realidad informativa expresada en las reglas del juego, un nuevo tipo de actores en el campo de la información. Actúa como un factor de cambios globales en todos los niveles de la modernización social para construir una estrategia de actividad y política en el campo de la información.
4	S. A. Modestov	El proceso de competencia en un entorno específico, relacionado con los segmentos de la comunidad internacional económica, política, militar, social.
5	G. M. Niyazova, T. F. Berestova y A. I. Nenashev	El espacio de información es un sistema funcional complejo y de campo de estratificación de signos lingüísticos y no lingüísticos dentro del enfoque funcional. El espacio informativo es multidimensional. Es un proceso de formación dinámica de barreras de información en la cultura.
6	A. I. Nenashev	Formula la definición del espacio informativo en la ciencia filosófica como un aspecto de la difusión de la información en la sociedad establecida, que tiene un reflejo en los factores culturales, económicos, políticos, tecnológicos y otros.
7	V. D. Popov	Por espacio informativo entiende un número indeterminado de flujos que interactúan con la reproducción, percepción, evaluación, elaboración, actitudes, disposición y posición hacia la información, formando en general el comportamiento social y la motivación de un individuo.
8	I. A. Dobrovolskaya	El concepto de espacio digital está en consonancia con el concepto de espacio informativo.

Nota. Elaboración propia, con base en el documento «El concepto de espacio digital y sus características. Oportunidades y amenazas para el uso del espacio digital» (Traducción libre del ruso) (Sidorova, 2020).

Como es visible en la Tabla 5, la academia rusa conceptualiza el espacio digital no como herramienta neutra, la concibe como realidad estructurante de la existencia humana (Ivin, en Sidorova, 2020), capaz disolver fronteras físicas y simbólicas. A su vez, la visión rusa le define como «realidad transformadora» transnacional (Ikonnikova y Bolshakov, en Sidorova, 2020), capaz de reconfigurar la realidad misma, trascendiendo su función comunicativa. Esta percepción da fundamento a la concepción de *RuNet* —a analizar en el siguiente apartado— como espacio vital nacional que demanda protección frente a agresiones externas, en específico de las influencias occidentales.

A la par, el espacio digital opera como sistema de poder y control cultural; siendo un campo de estratificación de signos lingüísticos y no lingüísticos donde se construyen barreras culturales (Niyazova *et al*., en Sidorova, 2020). Según Popov (en Sidorova, 2020), este ámbito moldea comportamientos sociales y motivaciones individuales mediante flujos informativos que interactúan con procesos de percepción, evaluación y disposición de contenidos. Así, acciones como apagones digitales (bloqueos, filtros de inspección profunda de paquetes, DPI) trasciende objetivos de seguridad, orientándose a eliminar amenazas nacionales.

A nivel mundial existen casos similares, como *Cambridge Analytica*, que evidenció el uso de estos flujos para incidir en el comportamiento sociopolítico, electoral y participativo tanto en las

elecciones de EE UU como en el referéndum sobre la salida de Reino Unido de la Unión Europea (Bastos y Mercea, 2018). Frente a eso, la protección de infraestructuras digitales (*hardwares*, redes) y recursos digitales (procesos, tecnologías sociales) por parte de Rusia, responde a la comprensión del espacio digital como terreno de disputa geopolítica, desde donde convergen tres elementos estratégicos: infraestructura, los recursos digitales y su base material.

La academia rusa concibe entonces al espacio digital como arena de competencia geopolítica donde, según Modestov (en Sidorova, 2020), se desarrollan conflictos estratégicos en los ámbitos económico, militar y político internacionales. Por su parte, Zuev (en Sidorova, 2020) complementa esta perspectiva al definirlo como campo de juego reglado con actores específicos, catalizador de transformaciones globales. Desde este marco teórico se sustenta la necesidad de autonomía técnica de *RuNet* (DNS nacional, protocolos de seguridad de la capa de transporte, TLS propios) como acto geopolítico tripartito: resistir sanciones internacionales, exportar modelos de gobernanza digital a países aliados, presentándose como una alternativa.

De manera paralela, este espacio funciona como esfera multidimensional para el control nacional. Nenashev y Zuev (en Sidorova, 2020) destacan su carácter polifacético —económico-tecnológico-político— y su función en procesos de modernización social dirigidos estatalmente. Como se observa en las modificaciones realizadas a la Ley Federal «Sobre la Información» en su artículo 15-3:

> en la parte 1, después de las palabras «realizado en violación del procedimiento establecido», añadir las palabras «información socialmente significativa no fiable difundida bajo la apariencia de mensajes fiables que crea una amenaza de daño a la vida y (o) la salud de los ciudadanos, la propiedad, una amenaza de alteración masiva del orden público y (o) la seguridad pública, o una amenaza de crear interferencia con el funcionamiento o la terminación del funcionamiento de las instalaciones de soporte vital, la infraestructura de transporte o social, las instituciones de crédito, las instalaciones energéticas, industriales o de comunicaciones» (Presidencia de Rusia, 2019).

Esta dimensión jurídica se materializa en la alineación de producción de infraestructuras digitales rusas con objetivos de control vertical que recaen sobre la población: migración obligatoria (coercitiva) de usuarios hacia plataformas estatales (*VKontakte*, *Rutube*) para cumplir con los objetivos de interés nacional rusos en este rubro (protección de datos).

Cabe destacar que estas pugnas responden al control del espacio digital que deja el orden posbélico forjado por EE UU, cuyo declive anticipó Immanuel Wallerstein (1995). Esto ha sido identificado por el grupo en el poder que apoyó el regreso al poder de Donald Trump para un segundo periodo presidencial en 2025, personaje que tiene entre sus objetivos reorganizar a la OTAN, tras su debacle afgana, reafirmarse mediante su intervención directa en el espacio postsoviéticos a través del conflicto ruso-ucraniano y, entre otros, buscar su preponderancia en la carrera digital a través de su iniciativa *IA Action Plan* (The White House, 2025).

4. Ley rusa de Internet Soberana. TI y Seguridad nacional

En el contexto de las relaciones internacionales de las primeras décadas del siglo XXI, Rusia ha experimentado un incremento sostenido de medidas restrictivas multilaterales (sanciones). Estas acciones, promovidas desde Occidente, se fundamentan en torno a acciones geopolíticas clave, una de ellas es el cambio de estatus de Crimea en 2014 y en interpretaciones sobre la seguridad regional europea (Kapoguzov, Pakhalov y Sheresheva, 2024).

Además, se observa una instrumentalización de discursos normativos vinculados a los derechos humanos y libertades civiles como herramientas de presión estratégica dentro del escenario internacional (Kramin e Imasheva, 2024; Amnistía Internacional, 2024). Este entorno refleja un patrón documentado en la economía política global donde «la coerción económica acelera procesos de innovación institucional orientados a reducir vulnerabilidades sistémicas» (Kapoguzov *et al*., 2024, p. 136).

La relación geopolítica Rusia-Occidente involucra episodios en la historia reciente que intensificaron tensiones bilaterales. En 2018, por ejemplo, incidentes como el envenenamiento de Serguéi Skripal en Reino Unido —atribuido a agentes rusos por el uso de *novichok*— generaron nuevas sanciones (Kapoguzov *et al*., 2024). Aunado a ello, se reportaron acusaciones sobre confrontaciones navales en el estrecho de Kerch y operaciones cibernéticas atribuidas, consolidando un patrón donde los discursos de securitización se instrumentalizan como herramientas de presión geopolítica (Kramin e Imasheva, 2024, p. 119). Estos eventos, sumados a las tensiones ucranianas post-2014, actuaron como catalizadores para ampliar el alcance de las medidas coercitivas.

Al respecto, dos sectores estratégicos han concentrado estas medidas, el energético y el financiero. En el primero, las sanciones sectoriales implementadas desde 2014 alteraron patrones históricos de interdependencia energética global (Yakimova, 2024), impulsando incluso medidas arancelarias secundarias, atípicas a quienes comercien con Rusia. En el ámbito financiero, durante 2022 se materializaron iniciativas para excluir entidades rusas del sistema *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) —previamente anunciadas en 2020—, generando disrupciones en los flujos de pagos transnacionales e inestabilidad en mercados emergentes (Kramin e Imasheva, 2024, p. 118).

Ante estas presiones, el gobierno ruso desarrolló contramedidas institucionales centradas en la creación del Sistema de Mensajería Financiera (SPFS), diseñado para «integrar actores euroasiáticos y proveer autonomía operativa frente a infraestructuras occidentales» (Kramin e Imasheva, 2024, p. 121). Este mecanismo refleja una estrategia de resistencia financiera mediante la internalización de riesgos que le ha servido para mostrar que otra red de mensajería financiera, lejos del dominio occidental, es posible.

En este sentido, la respuesta rusa trasciende el ámbito financiero, articulándose en una política integral de soberanía tecnológica. Entendida, según el marco conceptual ruso, como la capacidad para «reproducir de manera sostenible, bajo control nacional, tecnologías críticas que garanticen la realización de los intereses del Estado y la sociedad» (Kapoguzov *et al*., 2024, p. 130). Esta estrategia combina desarrollo endógeno con cooperación selectiva en bloques alternativos como los BRICS (Brasil, Rusia, India, China y Sudáfrica), evitando tanto la dependencia como el aislamiento absoluto (Kapoguzov *et al*., 2024, p. 134). Así, los avances en infraestructuras digitales domésticas y la priorización de cadenas de suministro internalizadas muestran cómo las restricciones externas tienden a catalizar procesos de innovación institucional orientados a la autonomía estructural.

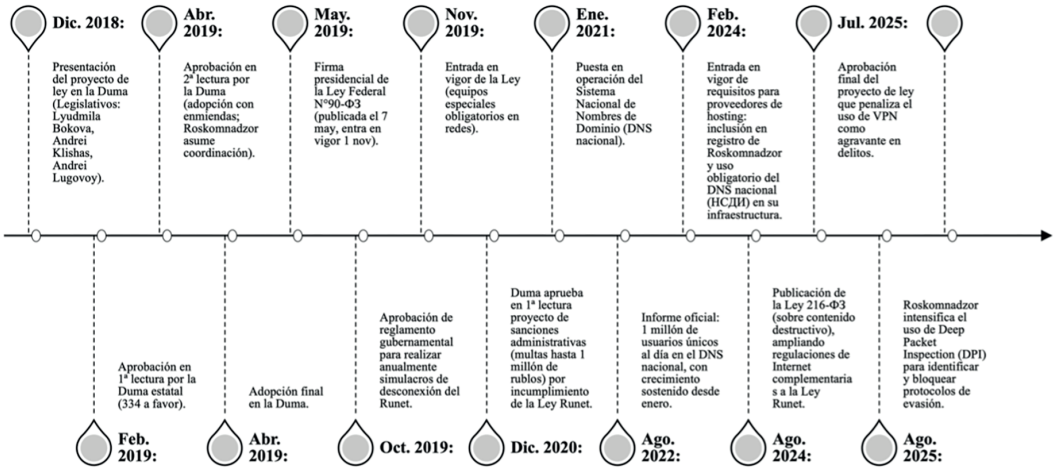
Frente a este escenario, el gobierno ha interpretado las sanciones como componentes de una estrategia occidental para limitar la influencia global de la nación euroasiática. Esta percepción aceleró políticas de preparación para escenarios de contingencia extrema, incluyendo posibles «desconexiones totales de infraestructuras digitales globales» (Kapoguzov *et al*., 2024, p. 134). La respuesta institucional combinó dos dimensiones: 1) fortalecimiento de narrativas de resiliencia nacional, y 2) inversiones aceleradas en soberanía tecnológica.

La materialización de estas políticas incluyó a *RuNet*: Red nacional con capacidades de operación autónoma diseñada para mantener servicios digitales esenciales durante aislamientos tecnológicos (Yakimova, 2024, p. 108). En este sentido, el desarrollo de la Ley sobre Internet Soberano (Figura 5), presentada ante la Duma Estatal rusa por los senadores Lyudmila Bokova y Andrei Klinshas, junto con el diputado Andrei Lugovoy, materializa institucionalmente las concepciones teóricas del espacio digital: campo de competencia geopolítica y proyecto de modernización de su complejo científico-tecnológico-militar. Esto se formalizó en 2019, momento en que Vladímir Putin promulgó la Ley de Internet Soberna *RuNet*, la cual opera en dos dimensiones clave:

1. Mecanismo de soberanía tecnológica (Modestov, citado en Sidorova, 2020): mantiene su infraestructura autónoma (DNS nacional, protocolos TLS propios), respondiendo a dinámicas de competencia en segmentos estratégicos internacionales, al tiempo que proporciona resistencia operativa frente a contingencias externas.
2. Instrumento de coordinación social vertical (Nenashev y Zuev, citados en Sidorova, 2020): en este punto, desempeñan un papel importante los ejercicios periódicos de desconexión y la transición hacia plataformas nacionales (*VKontakte, RedTube*), con lo cual se imple-

menta la visión del espacio digital como ámbito de modernización centralizada. Esto bajo el objetivo de garantizar autonomía técnica para consolidar marcos de seguridad nacional en torno a la interacción social.

Figura 5. Línea del tiempo: Ley de Internet soberana *RuNet*



Nota. Elaboración propia, adaptado de fuentes oficiales rusas y reportes internacionales: Stadnik (2019), Roskomnadzor (2025), RBC (2020), Global Digital Forum (2025), RIGF (2025) y Gobierno de Rusia (2025).

Aquí, la arquitectura institucional que sustenta la Ley de Internet Soberana rusa, *RuNet*, revela una triada operativa: Estado-academia-industria, actores que convergen en la búsqueda de su soberanía digital (ver Tabla 6). Es posible observar que el entramado va más allá de una coordinación funcional, representa una sinergia estructural que reconfigura el espacio digital como territorio de poder:

1. En el sector gubernamental, Roskomnadzor —uno de los actores— es eje ejecutor con capacidades de vigilancia excepcionales: incluyendo el bloqueo autónomo de infraestructuras; mientras la Duma Estatal modifica la legislación mediante tipificaciones elásticas («extremismo», «desestabilización»). Ambos, instituyen un régimen de excepción tecnoadministrativo que trasciende la mera regulación.
2. El sector científico-tecnológico –representado por mecanismos políticos de alto nivel como el *Russian Internet Governance Forum* (RIGF) y el Foro Económico Internacional de San Petersburgo, entre otros– provee la doble legitimación requerida: 1) construye narrativas geopolíticas que enmarcan la ciberautarquía como defensa existencial, y 2) desarrolla capacidades técnicas endógenas (criptografía, DNS nacional) que anclan la soberanía en dispositivos materiales.
3. El sector industrial evidencia la intervención corporativa mediante actores como *Yandex* o *Kaspersky*, cuyas plataformas internalizan lógicas de censura proactiva. Los proveedores de Internet, en tanto ejecutores forzosos de restricciones, completan este modelo de gobernanza público-privada donde la infraestructura deviene instrumento de control espacial.

Tabla 6. Actores y su participación en la Ley de Internet Soberana (Ley *RuNet*)

Complejo	*Actor*	*Función en RuNet*
Gubernamental	Servicio Federal de Supervisión de Telecomunicaciones (Roskomnadzor)	Regulación, supervisión y ejecución técnica. Actúa como administrador centralizado en amenazas: puede desconectar Internet global, bloquear contenido sin orden judicial, coordinar simulacros de red e imponer multas. Representa el interés nacional.
	Ministerio de Desarrollo Digital, Comunicaciones y Medios	Diseño normativo, coordinación de infraestructura nacional y requisitos técnicos. Promueve digitalización y sustitución de importaciones de software.
	Duma Estatal (Asamblea Federal)	Aprobó la Ley Federal 90-FZ (2019) y enmiendas posteriores que criminalizan búsquedas de «contenido extremista».
Científico-Tecnológico	Russian Internet Governance Forum	Legitimación de la «soberanía digital» y formación de élites en políticas de ciberseguridad.
	Universidad Estatal de Moscú (Facultad de Computación)	Investigación en ciberseguridad y formación de cuadros técnicos alineados con la doctrina estatal.
Industrial	Yandex	Coopera con el Estado en un «acto de equilibrio»: permite acceso de Roskomnadzor a metadatos de usuarios, a pesar de objeciones iniciales.
	Laboratorios Kaspersky	Provee tecnologías de ciberseguridad; acusado por gobiernos occidentales de colaborar con inteligencia rusa al cumplir leyes de entrega de datos.
	MegaFon, Beeline, MTS, Rostelecom (ISP)	Instalación obligatoria de equipos DPI/TSPU, redirección de tráfico a servidores estatales y participación en simulacros de desconexión global.

Nota. Elaboración propia, adaptado de fuentes oficiales rusas y reportes internacionales: Stadnik (2019), Roskomnadzor (2025), RBC (2020), Global Digital Forum (2025), RIGF (2025) y Gobierno de Rusia (2025).

A partir de la articulación mostrada, es posible señalar que *RuNet* representa una política estratégica que moviliza a diversos actores en torno a su seguridad nacional y la soberanía digital de Rusia. La Ley de Internet Soberana responde a la amenaza tangible de una desconexión de Internet global por parte de Occidente, que va más allá del tema de Ucrania; por lo tanto, el gobierno ruso busca asegurar el control de datos críticos.

Cabe destacar que el DNS y la gestión de claves de acceso a nodos centrales refleja una lógica de dominación geopolítica espacial; aquí, los recursos digitales operan como mecanismos de poder. No obstante, Rusia no persigue un aislamiento total. La ley no es prohibitiva ni autárquica; como es de observar en la Tabla 6, está diseñada para proteger los intereses del Estado en un contexto donde la gestión gubernamental depende intrínsecamente de Internet.

Cabe subrayar que no solo las actividades estatales, sino todas las dimensiones de la cotidianidad humana están interconectadas al espacio digital. Esta saturación relacional permite distinguir entre una *Internet convencional*, una *Internet de las cosas* y una *Internet estratégica* que involucra a las anteriores. Ello requiere garantías operativas tanto para actividades diarias como para esferas gubernamentales (incluidas las militares), industriales, científicas, financieras y tecnológicas.

Esta problemática adquiere relevancia crítica en el marco de la disputa hegemónica permanente entre EE UU y China por el control del ciclo de producción de la infraestructura y los recursos digitales. Ambas potencias poseen capacidades suficientes para contender por la primicia en un ecosistema digital (Bezrukov, Ivanov, Petrov y Smirnov, 2021) donde EE UU impuso inicialmente a sus gigantes tecno-corporativos.

Frente a este contexto, Rusia decidió dar prioridad al reforzamiento de su soberanía digital, requiriendo capacidades político-técnicas para desconectar —a discreción— su red de infocomu-

nicaciones, *RuNet*, de la Internet global. Pero, reconoce que dicha acción generaría dificultades de acceso a usuarios informativos externos. Por lo tanto, el Servicio Federal de Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación (*Roskomnadzor*) implementó un programa gradual para gestionar este proceso.

En el primer semestre de 2025 el escenario previo a la Cumbre del 15 de agosto fue de confrontación absoluta (Lokshina, 2025). Las acciones alrededor de la OTAN y el conflicto en Ucrania obligan a Rusia a mantener un estado de alerta permanente en torno al incremento de sanciones. En consecuencia, Moscú busca consolidar un ecosistema digital autónomo (Bezrukov *et al*., 2021), mediante el despliegue de infraestructura crítica y marcos legales que permitan al Estado ejercer un control efectivo sobre este ámbito estratégico.

En torno a ello, la estrategia rusa pretende mitigar al menos cuatro riesgos críticos:

1. Ciberataques contra recursos en línea gubernamentales y sistemas de gestión de redes.
2. Vulneración de infraestructuras críticas (servicios públicos y de seguridad)
3. Sustracción de datos estratégicos.
4. Dependencia tecnológica externa que comprometa la autonomía y la seguridad nacional.

Reflexión final: ¿Qué perspectivas enfrenta Rusia en la era de la digitalización?

Comprender que el control de Internet es un campo de disputa permite retomar la reflexión de Arendt sobre el *Sputnik* como artefacto humano que «habitó la proximidad de los cuerpos celestes» al simbolizarla paradoja central de la soberanía digital contemporánea: *los Estados buscan dominar espacios digitales que, aunque construidos tecnológicamente, operan con lógicas sistémicas que trascienden el control unilateral.* Este análisis reveló que *RuNet* pretende ir más allá de la respuesta a amenazas de desconexión, pretende constituir una arquitectura de resistencia geopolítica desde donde convergen tres elementos:

1. Mecanismos legales y técnicos que blindan infraestructuras críticas.
2. Estrategias (plural) de autarquía digital que replican patrones históricos adaptados a la fragmentación global.
3. Contradicciones estructurales entre autonomía declarada y dependencia tecnológica real (Bezrukov *et al*., 2021).

El espacio digital, pese a su disputa hegemónica entre EE UU y China, depende materialmente de ámbitos terrestres, marítimos y aéreos para su existencia. Rusia explota esta multidimensionalidad mediante el control de cadenas de suministro y desarrollo de tecnologías post-5G, intentando consolidar un ecosistema autónomo. Sin embargo, persisten riesgos críticos no resueltos: vulnerabilidad ante ciberataques, extracción de datos estratégicos y dependencia de hardware extranjero.

Así, la creación tecnológica implica habitar espacios trascendentes pero sometidos a leyes ajenas. *RuNet* encarna esta tensión: proyecto de reterritorialización digital que, mientras desafía la hegemonía liberal, reproduce lógicas de dominación espacial. Su evolución definirá la viabilidad de modelos soberanos en un Internet crecientemente balcanizado.

Agradecimientos

Esta investigación ha sido realizada gracias al Programa UNAM-PAPIIT<IA300922>.

Referencias bibliográficas

Amnistía Internacional. (2024). *Deben eliminarse las leyes de censura de guerra en Rusia*. Recuperado de https://www.amnesty.org/es/petition/russias-war-censorship-laws-must-go/

Arendt, H. (2016) *La condición humana* (1ª ed). España: Paidos.

Bastos, M., y Mercea, D. (2018). The public accountability of social platforms: lessons from a study on bots and trolls in the Brexit campaign. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, *376*(2128), p. 20180003. https://doi.org/10.1098/rsta.2018.0003

Bankauskaité, D., y Šlekys, D. (2023). Lithuania's Total Defense Review. *PRISM*, *10*(2), 54-77. https://www.jstor.org/stable/48718173

Bezrukov, A. O., Ivanov, S. V., Petrov, V. L., y Smirnov, A. A. (2021) Russia in the Digital World: International Competition and Leadership. *Russia in Global Affairs*, *19*(2), 64-85. https://doi.org/10.31278/1810-6374-2021-19-2-64-85

Ceceña, A. E., y Barreda, A. (1995). *Producción estratégica y hegemonía mundial* (1ª ed.). Ciudad de México, México: Siglo XXI.

García Reyes, M. (2007). *La nueva revolución energética: el impacto en la geopolítica y la seguridad internacional.* Ciudad de México, México: CIGEMA, García-Goldman-Koronovski, Universidad Lomonosov.

Global Digital Forum. (2025). *Runet es una poderosa herramienta para el desarrollo tecnológico, social y cultural del país*. Recuperado de https://gdfconf.com/ru/news/3

Gobierno de Rusia. (2025). *Runet: Sistema Nacional de Información de Rusia*. Recuperado de http://government.ru/

Gramsci, A. (1975). *Cuadernos de la Cárcel*. Buenos Aires, Argentina: Editorial Nueva Visión.

Harvey, D. (2004). *El nuevo imperialismo* (1ª ed.). Madrid, España: Akal.

Hobsbawm, E. (2003). *En torno a los orígenes de la Revolución Industrial*. México: Siglo XXI.

Ishchuk, Ya. G. (2022). Tendencias del terrorismo y extremismo digital durante la pandemia de COVID-19 [Тенденции цифрового терроризма и экстремизма в период пандемии COVID-19]. *Pravovoe Gosudarstvo: Teoriya i Praktika*, *2*(68), 71-82. https://doi.org/10.33184/pravgos-2022.2.8

Kapoguzov, E. A., Pakhalov, A. M., y Sheresheva, M. Y. (2024). Russian discourses on technological sovereignty (evidence from expert survey). *Sotsiologicheskie issledovaniya,* (12), 24-37. https://doi.org/10.31857/S0132162524120037

Kimhi, S., Eshel, Y., Marciano, H., y Adini, B. (2023). Impact of the war in Ukraine on resilience, protective, and vulnerability factors. *Frontiers in public health*, *11*, 1053940. https://doi.org/10.3389/fpubh.2023.1053940

Kimhi, S., Kaim, A., Bankauskaite, D., Baran, M., Baran, T., Eshel, Y., ... & Adini, B. (2024). A full-scale Russian invasion of Ukraine in 2022: Resilience and coping within and beyond Ukraine. *Applied Psychology: Health and Well-Being*, *16*(3), 1005-1023. https://doi.org/10.1111/aphw.12466

Kaspersky Lab. (2025). *Kaspersky Cyberthreat real-time map*. Recuperado de https://cybermap.kaspersky.com/

Kramin, T. V., e Imasheva, I. (2024). The impact of digital infrastructure on regional development in Russia. *Terra Economicus*, *22*(3), 115-127. https://doi.org/10.18522/2073-6606-2024-22-3-115-127

Lefebvre, H. (2003) *The Urban Revolution*. Minneapolis, MN: University of Minnesota Pres.

León Hernández, E. (2016). *Geografía crítica. Espacio, teoría social y geopolítica* (1ª ed.). Ciudad de México: UNAM / Ítaca.

Lens. (2010). («Runet» OR «Russian sovereign internet» OR «sovereign internet Russia» OR «Russia Internet strategy»). https://www.lens.org/

Lokshina, T. (2025). The First Step in Negotiations with Russia Freeing Detained Ukrainians Can Smooth the Way for More Difficult Talks. *Foreign* Affairs. Recuperado de http://foreignaffairs.com/russia/first-step-negotiations-russia

López Delgado, M. (2007). *Análisis forense digital* (2a. ed.). Madrid, España: CriptoRed. Recuperado de https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf.

Lukyanenko, E. V. (2024). Fijación de la identidad cultural rusa: artefactos artísticos como espejo de las victorias cósmicas de la URSS [Фиксация российской культурной идентичности: художественные артефакты как зеркало космических побед СССР]. *KANT: Social Science & Humanities*, *4*(20), 23-29. https://doi.org/10.24923/2305-8757.2024-20.3

Montañés Serrano, M., y Martín Gutiérrez, P. (2017). De la IAP a las Metodologías Sociopráxicas. *Habitat y Sociedad, 10*, 35-52. https://doi.org/10.12795/HabitatySociedad.2017.i10.03.

Moscow State University. (2025). *Faculty of Political Science*. Recuperado de http://openday.msu.ru/polit-en

O'Reilly, G. (2019). *Aligning Geopolitics, Humanitarian Action and Geography in Times of Conflict* (1st ed.). Switzerland: Springer.

OpenAlex. (2025). («Runet» OR «Russian sovereign internet» OR «sovereign internet Russia» OR «Russia Internet strategy»). https://openalex.org/

Ornelas, R. (2013). *Crisis Civilizatoria y superación del capitalismo* (1ª ed.). México: UNAM IIEc, Aviso de Incendio.

Presidencia de Rusia. (2019). *Ley Federal de 18.03.2019 No. 31-FZ* [Федеральный закон от 18.03.2019 г. № 31-ФЗ]. Recuperado de http://kremlin.ru/acts/bank/44084

Presidencia de Rusia. (2025). *Sesión plenaria del Foro Económico Internacional de San Petersburgo* [Пленарное заседание Петербургского международного экономического форума]. Recuperado de http://kremlin.ru/events/president/news/77222

RAS. (2025). *About. Instituto de Europa*. Recuperado de https://en.instituteofeurope.ru/30let-ie-ras/about

Rau, J. (2021). Sobre las nuevas tendencias geopolíticas a raíz de la transición tecnológica 5G (2013-2021) [О новых геополитических тенденциях в связи с переходом на технологии 5G (2013-2021)]. Современная научная мысль, (3), 117-126. https://doi.org/10.24412/2308-264X-2021-3-117-126

RBC. (2020). *Mincinfra aplaza por tercera vez el ejercicio de resiliencia Runet.* Recuperado de https://www.rbc.ru/rbcfreenews/5f684ef69a7947217cf7e3a2

RBC. (2025). *Las aduanas revelaron los 10 principales socios comerciales de Rusia* [Таможня раскрыла топ-10 торговых партнеров России]. Recuperado de https://www.rbc.ru/economics/02/01/2025/676fd1eb9a7947cb9e223e39

RIGF. (2025). *Runet: A powerful tool for Russia's technological, social and cultural development*. Recuperado de https://rigf.ru/en/press/runet-moshchnyy-instrument-dlya-tekhnologicheskogo-sotsialnogo-i-kulturnogo-razvitiya-strany/

Rozkomnadzor. (2025). *Runet: Sistema Nacional de Información de Rusia*. Recuperado de https://rkn.gov.ru/

RT. (2021). *Putin, sobre los que quieren «arrancarle» algo a Rusia: «Deben saber que les sacaremos los dientes para que no puedan morder». RT en Español*. Recuperado de https://actualidad.rt.com/actualidad/392701-putin-querer-arrancarle-rusia-saber-sacar-dientes

Sidorova, A. P. (2020) El concepto de espacio digital y sus características. Oportunidades y amenazas del uso del espacio digital [Понятие цифрового пространства и его характеристики. Возможности и угрозы использования цифрового пространства], *Diálogo Científico: Joven Científico*, 48-55. https://doi.org/10.18411/spc-22-05-2020-11

Stadnik, I. (2019). Sovereign RUnet: What does it mean? *Internet Governance Project*, 12. Recuperado de https://www.internetgovernance.org/wp-content/uploads/IGPWhitePaper_STADNIK_RUNET-1.pdf

The White House. (2021). *Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth.* Recuperado de https://bidenwhitehouse.archives.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf?utm_source=sfmc%E2%80%8B&utm_medium=email%E2%80%8B&utm_campaign=20210610_Global_Manufacturing_Economic_Update_June_Members

The White House. (2025). *White House Unveils America's AI Action Plan*. Recuperado de https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/

Van Eck, N. J., y Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, (84), 523-538. https://doi.org/10.1007/s11192-009-0146-3

Vyas, A. (2025). Transactional Diplomacy and the Russia-Ukraine Conflict: A U.S. Foreign Policy Shift During the Trump Era. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5223629

Wallerstein, I. (1995) *Después del liberalismo*. Ciudad de México: UNAM CEIICH / Siglo XXI.

World Bank. (2021). *Federación de Rusia: Resumen del comercio. World Integrated Trade Solution*. Recuperado de https://wits.worldbank.org/CountryProfile/es/Country/RUS/Year/LTST/Summary

Yakimova, V. A. (2024). Models for forecasting the emergence of innovative and digital ecosystems in border regions of Russia. *Terra Económicus*, *22*(3), 96-114. https://doi.org/10.18522/2073-6606-2024-22-3-96-114

Yee, L., Chui, M., Roberts, R., y Smit, S. (2025). *McKinsey Technology Trends Outlook 2025*. Recuperado de https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech