EDITORIAL ANDES COGNITIO



RELACIONES INTERNACIONALES 6.0

GEOPOLÍTICA INTELIGENTE, GOBERNANZA GLOBAL Y TRANSFORMACIÓN DEL PODER EN LA ERA DIGITAL

Adriana Yamilet Herrera Granizo
Norelyn Tatiana Mejia Basantes
Jhonathan Alexis Meneses Flores
Marlene Isabel Coronel Grados
Danny Fernando Chiriboga Barba

Editorial Andes Cognitio

RELACIONES INTERNACIONALES 6.0: Geopolítica Inteligente, Gobernanza Global y Transformación del Poder en la Era Digital

© Autores

Adriana Yamilet Herrera Granizo
Correo: ayherrera@espe.edu.ec
Orcid: https://orcid.org/0000-0001-5090-5981
Institución: Universidad de las Fuerzas Armadas ESPE. Sangolquí, Ecuador

Norelyn Tatiana Mejia Basantes
Correo: norelyn.mejia@fatimas.edu.ec
Orcid: https://orcid.org/0009-0008-3357-7953
Institución: Unidad Educativa Nuestra Señora de Fátima. Riobamba, Ecuador

Jhonathan Alexis Meneses Flores
Correo: jhonathan.meneses505@comunidadunir.net
Orcid: https://orcid.org/0009-0007-4244-8291
Institución: Investigador independiente

Marlene Isabel Coronel Grados
Correo: micoronel4@espe.edu.ec
Orcid: https://orcid.org/0000-0001-7293-1902
Institución: Universidad de las Fuerzas Armadas ESPE. Sangolquí, Ecuador

Danny Fernando Chiriboga Barba
Correo: dfchiriboga1@espe.edu.ec
Orcid: https://orcid.org/0000-0003-3009-3917
Institución: Universidad de las Fuerzas Armadas ESPE. Sangolquí, Ecuador

Editorial "ANDES COGNITIO EDAC S.A.S."
DEPARTAMENTO DE EDICIÓN

Editado y Distribuido por:

Editorial:	Andes Cognitio
Sello Editorial:	978-9942-7408
Teléfono:	0995805659
Web:	https://andescognitio.org
ISBN:	978-9907-9566-7-2
DOI:	https://doi.org/10.64230/pdtq4n40

© Primera Edición
© Noviembre 2026

Impreso en Ecuador

Revisión de Ortografía
Lcda. Cristina Paola Chamorro Ortega

Diseño de Portada
Ing. Pamela Rosa Taco Hernández Mgs

Diagramación
Ing. Yoselyn Andrea Rogel Gaibor

Director Editorial
Ec. Juan F. Villacis U. Mgs.

Aviso Legal
El contenido de este libro incluyendo textos, imágenes, gráficos, tablas, cuadros y referencias bibliográficas es de exclusiva responsabilidad del/ de los autor (es). Las opiniones, datos y criterios expresados no representan necesariamente la postura institucional ni el pensamiento de la Editorial Andes Cognitio.

Derechos de Autor ©

Este documento se publica bajo los términos y condiciones de la Licencia Creative Commons Reconocimiento – No Comercial – Compartirlgual 4.0 Internacional (CC BY-NC-SA 4.0).



Todos los derechos de autor y de propiedad intelectual e industrial relativos al contenido de esta publicación pertenecen exclusivamente a la "Editorial Andes Cognitio" y a sus respectivos autores. Queda expresamente prohibida, bajo las sanciones establecidas por la legislación vigente, la reproducción total o parcial de esta obra, su almacenamiento en sistemas informáticos, su tratamiento digital, así como cualquier forma de distribución, transmisión o comunicación pública por medios electrónicos, mecánicos, ópticos, químicos, de grabación o fotocopia sin la debida autorización previa y por escrito de los titulares del copyright.

Se exceptúan únicamente los usos con fines académicos o de investigación científica, siempre que no persigan propósitos comerciales y se realicen de forma gratuita, debiendo citarse en todo momento a la fuente editorial correspondiente. Las opiniones vertidas en los distintos capítulos son de exclusiva responsabilidad de los autores y no reflejan necesariamente la postura institucional de la editorial.

Comité Científico Académico

Dr. Jorge Gualberto Paredes Gavilanez PhD.
Universidad Técnica Estatal de Quevedo

Dr. Oscar Patricio López Solís PhD.
Universidad Técnica de Ambato

Ec. Carlos Roberto López Paredes PhD.
Escuela Superior Politécnica de Chimborazo Extensión Orellana

Dr. Héctor Enrique Hernández Altamirano PhD.
Universidad Técnica de Ambato

Dr. Carlos Arturo Jara Santillán PhD.
Escuela Superior Politécnica de Chimborazo

Dr. Guillermo Carrillo Espinosa PhD,
Universidad Autónoma de Chapingo - México

Dra. Doris Coromoto Pernía Barragán PhD,
Universidad de los Andes Tachira Venezuela

Ec. María Gabriela González Bautista PhD.
Universidad Nacional de Chimborazo

My. Efraín Arguello Arellano, Mgs.
Tecnológico Universitario ARGOS – Policía Nacional del Ecuador

Ing. Liliana Priscila Campos Llerena Mgs.
Universidad Técnica de Ambato

Dr. Mario Humberto Paguay Cuvi Mgs.
Escuela Superior Politécnica de Chimborazo

Ec. Oswaldo Javier Jácome Izurieta Mgs.
Universidad Técnica de Ambato

Ec. Juan Carlos Pèrez Briceño Mgs.
Instituto Superior Universitario Bolivariano

Dr. Luís Fernando Paz Villaeeoel Mgs.
Universidad Técnica Particular de Loja

Dra. Daysi Graciela Astudillo Condo Mgs.
Universidad Nacional de Chimborazo

Ec. Ligia Ximena Tapia Hermida Mgs.
Universidad Nacional de Chimborazo

Eco. Ángel Geovanny Carrión Gavilanes MBA.
Pontificia Universidad Católica del Ecuador sede Ambato

Ing. Paula Alejandra Abdo Peralta Mgs.
Escuela Superior Politécnica de Chimborazo

Ing. Milton Gabriel Del Hierro Mosquera Mgs.
Universidad Politécnica Estatal del Carchi

Ing. Catherine Gabriela Frey Erazo Mgs.
Escuela Superior Politécnica de Chimborazo

Ing. Juan Enrique Ureña Moreno Mgs.
Escuela Superior Politécnica de Chimborazo

Ing. José Fernando Esparza Parra Mgs.
Escuela Superior Politécnica de Chimborazo

Ing. Alexis Gabriel Reinoso Haro Mgs.
Universidad Estatal de Bolívar

Eco. Jaime Fernando Andrade Guamán Mgs.
Universidad Amawtay Wasi

Eco. Alejandro Carlos Lalama Freire Mgs.
Universidad Nacional de Chimborazo

Eco. Doménica Estefania Zabala Tapia
Universidad Nacional de Chimborazo

Constancia de Arbitraje

La Editorial Andes Cognitio, hace constar que este libro proviene de una investigación realizada por los autores, siendo sometido a un arbitraje bajo el sistema de doble ciego, de contenido y forma por jurados especialistas. Además, se realizó una revisión del enfoque, paradigma y método investigativo; desde la matriz epistémica asumida por los autores, aplicándose las normas APA, Séptima Edición, proceso de anti plagio en línea Compilatio, garantizándose así la cientificidad de la obra.

Comité Editorial

Eco. Juan Federico Villacis Uvidia Mgs.
Director de la Editorial Andes Cognitio

Lcda. Andrea Damaris Hernández Allauca PhD.
Editora de Andes Cognitio

PRÓLOGO

El escenario internacional del siglo XXI atraviesa una transformación profunda que trasciende las concepciones tradicionales del poder, la soberanía y la gobernanza mundial. La revolución digital, el desarrollo de la inteligencia artificial, la expansión de las infraestructuras tecnológicas y la creciente interdependencia económica han configurado nuevas dinámicas de competencia y cooperación entre los Estados y los actores globales. Comprender esta realidad exige renovar las perspectivas desde las cuales se estudian las relaciones internacionales.

En este contexto, *Relaciones Internacionales 6.0: Geopolítica inteligente, gobernanza global y transformación del poder en la era digital* constituye una propuesta académica orientada a interpretar las principales transformaciones del orden mundial contemporáneo. La obra articula fundamentos teóricos de las relaciones internacionales con los aportes de la geopolítica, la geoeconomía y la economía política internacional, incorporando el análisis de los datos, la inteligencia artificial y las capacidades tecnológicas como nuevos recursos estratégicos.

A través de sus cinco capítulos, el libro examina la evolución del sistema internacional, la competencia tecnológica, la transformación del poder económico, los desafíos de la soberanía digital y la construcción de mecanismos de gobernanza global. Asimismo, aborda las implicaciones de la diplomacia digital, la ciberseguridad, las operaciones de influencia y los conflictos en entornos tecnológicos, destacando la importancia de la cooperación y la responsabilidad internacional.

Esta obra invita a estudiantes, docentes, investigadores y profesionales a desarrollar una comprensión crítica e interdisciplinaria de un mundo cada vez más interconectado. Su principal aporte radica en reconocer que el poder ya no se expresa exclusivamente mediante capacidades territoriales, militares o económicas, sino también a través del conocimiento, la innovación, el control de la información y la capacidad de establecer reglas.

Leer este libro significa aproximarse a los desafíos del presente y reflexionar sobre las decisiones que configurarán el futuro de la sociedad internacional.

ÍNDICE GENERAL

PRÓLOGO **2**

ÍNDICE GENERAL **3**

INTRODUCCIÓN **6**

CAPÍTULO I **9**

RELACIONES INTERNACIONALES 6.0: FUNDAMENTOS PARA COMPRENDER LA TRANSFORMACIÓN DEL ORDEN MUNDIAL **9**

1.1. Evolución del sistema internacional: soberanía, interdependencia y configuración del orden mundial 9

1.2. Realismo, liberalismo y constructivismo ante la transformación digital 14

1.3. Economía política internacional: tecnología, acumulación y relaciones de dependencia 22

1.4. Conceptualización de las Relaciones Internacionales 6.0: alcances, dimensiones y límites analíticos 28

1.5. Reconfiguración de los actores internacionales: Estados, organismos multilaterales, empresas tecnológicas y redes transnacionales 36

1.6. Poder material, institucional y simbólico: articulación con las capacidades digitales 43

1.7. Métodos de investigación del poder internacional: análisis comparado, redes y prospectiva estratégica 51

CAPÍTULO II **60**

GEOPOLÍTICA INTELIGENTE: DATOS, INTELIGENCIA ARTIFICIAL Y COMPETENCIA ESTRATÉGICA **60**

2.1 Geopolítica inteligente: integración del análisis territorial, tecnológico y de información 61

2.2 Inteligencia artificial y capacidades estatales para la toma de decisiones estratégicas 66

2.3 2.3. Datos, capacidad de cómputo y talento especializado como recursos de poder 73

2.4 Semiconductores, centros de datos y servicios en la nube: dependencias y vulnerabilidades estratégicas 81

2.5 Cables submarinos, satélites y redes de telecomunicaciones en la disputa por la conectividad 83

2.6 Minerales críticos, energía y condiciones materiales de la transformación digital 85

2.7 Inteligencia estratégica y anticipación de conflictos: utilidad, incertidumbre y límites de los modelos predictivos 87

CAPÍTULO III 91

TRANSFORMACIÓN DEL PODER Y GEOECONOMÍA EN LA ERA DIGITAL 91

3.1 Poder estructural y capacidad de influencia en la economía digital internacional 91

3.2 Plataformas tecnológicas y relaciones de autoridad entre Estados y corporaciones 93

3.3 Cadenas globales de valor: concentración tecnológica, relocalización y autonomía estratégica 95

3.4 La economía y la tecnología como instrumentos del poder geopolítico 98

3.5 Comercio digital y flujos transfronterizos de datos: apertura, regulación y soberanía 121

3.6 Infraestructuras de pago, monedas digitales y competencia monetaria internacional 130

CAPÍTULO IV 140

GOBERNANZA GLOBAL Y SOBERANÍA DIGITAL: INSTITUCIONES, NORMAS Y RESPONSABILIDADES 140

4.1 Gobernanza de la transformación digital: legitimidad, representación y coordinación internacional 140

4.2 Soberanía digital y jurisdicción: tensiones entre autoridad estatal y redes transfronterizas 144

4.3 Gobernanza internacional de la inteligencia artificial: seguridad, transparencia y rendición de cuentas 146

4.4 Protección de datos, privacidad y derechos humanos en el entorno digital ... 149

4.5 Regulación de plataformas: competencia económica, responsabilidad y supervisión pública ... 153

4.6 Estándares tecnológicos y poder regulatorio en la configuración de mercados internacionales ... 155

4.7 Cooperación multilateral y participación del Sur Global en la definición de reglas digitales ... 157

CAPÍTULO V ... 161

DIPLOMACIA, CIBERSEGURIDAD Y CONFLICTOS EN ENTORNOS DIGITALES ... 161

5.1 Diplomacia digital: negociación, representación y comunicación estratégica ... 161

5.2 Inteligencia artificial en la actividad diplomática: aplicaciones y responsabilidad de las decisiones ... 167

5.3 Ciberseguridad internacional: amenazas, atribución de operaciones y protección de infraestructuras críticas ... 175

5.4 Disuasión y escalada en el ciberespacio: desafíos para la estabilidad internacional ... 186

5.5 Operaciones de influencia, desinformación y contenidos sintéticos en las disputas de poder ... 194

5.6 Sistemas autónomos y usos militares de la inteligencia artificial: control humano y dilemas jurídicos ... 203

5.7 Prevención de conflictos y construcción de confianza: diplomacia preventiva, cooperación técnica y gestión de crisis ... 213

REFERENCIAS BIBLIOGRÁFICAS ... 228

INTRODUCCIÓN

La configuración del sistema internacional contemporáneo atraviesa un proceso de transformación impulsado por la convergencia entre globalización, revolución tecnológica, competencia económica y reestructuración de las relaciones de poder. Durante las últimas décadas, los avances en tecnologías de información y comunicación han modificado las formas de interacción entre los Estados, las organizaciones internacionales, las empresas transnacionales y las sociedades. En este escenario, el poder ya no se encuentra determinado exclusivamente por la capacidad militar, territorial o económica, sino también por el dominio de los datos, la infraestructura digital, la inteligencia artificial, los sistemas de comunicación y la capacidad de generar conocimiento estratégico.

Estas transformaciones plantean nuevos desafíos para el estudio de las relaciones internacionales. Los enfoques tradicionales, aunque conservan su relevancia para explicar la cooperación, el conflicto y la distribución del poder, requieren incorporar dimensiones que permitan comprender la creciente influencia de los recursos tecnológicos en la política mundial. La competencia por los semiconductores, el control de las plataformas digitales, la protección de las infraestructuras críticas, la regulación de los flujos internacionales de datos y el desarrollo de sistemas de inteligencia artificial evidencian que la tecnología se ha convertido en un componente fundamental de la geopolítica y de la seguridad internacional.

En respuesta a esta realidad, el presente libro propone el enfoque de las *Relaciones Internacionales 6.0*, entendido como una perspectiva integradora que permite analizar la interacción entre poder digital, capacidades tecnológicas, gobernanza institucional, competitividad geoeconómica e influencia internacional. Su planteamiento parte de reconocer que la transformación digital no representa únicamente un cambio en las herramientas utilizadas por los actores internacionales, sino una modificación de las estructuras mediante las cuales se producen, distribuyen y ejercen las capacidades de poder. Por tanto, comprender el orden mundial emergente exige analizar simultáneamente sus dimensiones políticas, económicas, tecnológicas, jurídicas y estratégicas.

El propósito de esta obra es proporcionar fundamentos conceptuales y herramientas de análisis para interpretar las nuevas dinámicas del sistema internacional, considerando tanto las oportunidades derivadas de la innovación tecnológica como las tensiones asociadas a la dependencia digital, la concentración de capacidades y las desigualdades entre países. Asimismo, busca promover una reflexión crítica sobre la necesidad de construir mecanismos de cooperación que permitan orientar el desarrollo tecnológico hacia objetivos compatibles con la estabilidad internacional, los derechos humanos y el desarrollo sostenible.

Para alcanzar este propósito, el libro se organiza en cinco capítulos complementarios. El primero desarrolla las generalidades y fundamentos de las Relaciones Internacionales 6.0, examinando la evolución del sistema internacional, los principales enfoques teóricos, la transformación de los actores y las nuevas expresiones del poder. El segundo aborda la geopolítica inteligente, con especial atención a los datos, la inteligencia artificial, las capacidades estatales y las infraestructuras tecnológicas como factores de competencia estratégica. El tercero analiza la transformación del poder económico internacional desde la perspectiva de la geoeconomía digital, las plataformas tecnológicas, las cadenas globales de valor y las nuevas formas de influencia económica. El cuarto estudia la gobernanza global y la soberanía digital, considerando las instituciones, los marcos regulatorios, la protección de datos, la responsabilidad tecnológica y la participación del Sur Global. Finalmente, el quinto examina la diplomacia, la ciberseguridad y los conflictos en entornos digitales, incorporando los desafíos de la negociación internacional, las operaciones de influencia, los sistemas autónomos y la prevención de crisis.

La perspectiva adoptada reconoce que los desafíos digitales superan las fronteras nacionales y requieren respuestas coordinadas entre gobiernos, organismos multilaterales, empresas, universidades y sociedad civil. En consecuencia, la cooperación internacional, la capacidad regulatoria y la construcción de confianza constituyen elementos indispensables para evitar que las asimetrías tecnológicas profundicen las tensiones existentes.

EDITORIAL ANDES COGNITIO

CAPÍTULO I

RELACIONES INTERNACIONALES 6.0: FUNDAMENTOS PARA COMPRENDER LA TRANSFORMACIÓN DEL ORDEN MUNDIAL



CAPÍTULO I

RELACIONES INTERNACIONALES 6.0: FUNDAMENTOS PARA COMPRENDER LA TRANSFORMACIÓN DEL ORDEN MUNDIAL

1.1. Evolución del sistema internacional: soberanía, interdependencia y configuración del orden mundial

La evolución del sistema internacional constituye uno de los ejes centrales de las Relaciones Internacionales, ya que permite comprender cómo las estructuras de autoridad, legitimidad y poder han cambiado a lo largo del tiempo en respuesta a transformaciones políticas, económicas, sociales y tecnológicas. Desde la consolidación del sistema westfaliano en el siglo XVII hasta la actual revolución digital impulsada por la inteligencia artificial, los datos masivos y las plataformas globales, el orden mundial ha experimentado sucesivas reconfiguraciones que han redefinido el papel de los Estados y la naturaleza de las relaciones entre actores internacionales (Krasner, 1999; Ikenberry, 2018).

Tradicionalmente, el sistema internacional se ha estructurado en torno al principio de soberanía estatal, entendido como la autoridad suprema que ejerce un Estado sobre su territorio y población (Jackson, 2007). Sin embargo, la creciente interdependencia económica, tecnológica y comunicacional ha puesto en cuestión las concepciones tradicionales de soberanía, generando nuevos debates sobre gobernanza global, regulación transnacional y soberanía digital (Keohane & Nye, 2012; Farrell & Newman, 2019).

1.1.1 El sistema westfaliano y la construcción de la soberanía moderna

La firma de los Tratados de Westfalia en 1648 es ampliamente considerada el punto de partida del sistema internacional moderno. Aunque algunos autores cuestionan la interpretación tradicional de Westfalia como origen absoluto de la soberanía contemporánea, existe consenso en reconocer que este acontecimiento consolidó principios fundamentales como la autoridad territorial, la independencia política y la no intervención en asuntos internos (Osiander, 2001; Krasner, 1999).

La Guerra de los Treinta Años (1618-1648), que devastó gran parte de Europa Central, evidenció los riesgos de la fragmentación política y religiosa, impulsando la búsqueda de un nuevo equilibrio institucional basado en el reconocimiento mutuo entre autoridades territoriales. Como resultado, los acuerdos de Westfalia establecieron las bases para la consolidación del Estado moderno como principal unidad política del sistema internacional (Teschke, 2003).

Según Krasner (1999), la soberanía puede analizarse a partir de cuatro dimensiones:

1. Soberanía interna.
2. Soberanía internacional legal.
3. Soberanía westfaliana.
4. Soberanía de interdependencia.

Estas dimensiones reflejan que la soberanía no constituye una condición fija e inmutable, sino una construcción histórica sujeta a continuas transformaciones.

Tabla 1.1

Dimensiones de la soberanía según Krasner (1999)

Dimensión	Características
Soberanía interna	Capacidad de ejercer autoridad dentro del territorio
Soberanía internacional legal	Reconocimiento por otros Estados
Soberanía westfaliana	Exclusión de actores externos
Soberanía de interdependencia	Control de flujos transfronterizos

Fuente: Elaboración autores

La consolidación del sistema westfaliano permitió la expansión progresiva de un orden internacional basado en la coexistencia de unidades políticas formalmente iguales, aunque materialmente desiguales (Bull, 2012).

1.1.2 Equilibrio de poder y orden internacional europeo

Tras el Congreso de Viena de 1815, las potencias europeas desarrollaron un sistema de equilibrio de poder orientado a evitar la hegemonía de cualquier Estado sobre el

continente. Este mecanismo buscó preservar la estabilidad internacional mediante alianzas flexibles y negociaciones diplomáticas permanentes (Kissinger, 2014).

El equilibrio de poder se convirtió en uno de los principios fundamentales del pensamiento realista. Desde esta perspectiva, la estabilidad internacional depende de que ninguna potencia acumule suficientes capacidades para dominar al resto del sistema (Morgenthau, 2006).

Durante este período, la distribución del poder estuvo determinada principalmente por variables materiales como:

- Población.
- Territorio.
- Capacidad militar.
- Producción industrial.
- Control de rutas comerciales.

La tecnología, aunque importante, todavía era considerada un factor subordinado respecto a los instrumentos tradicionales de poder estatal (Kennedy, 1989).

1.1.3 Revolución Industrial y expansión de la economía mundial

La Revolución Industrial transformó profundamente las bases materiales del poder internacional. El desarrollo de nuevas tecnologías productivas, medios de transporte y sistemas de comunicación incrementó la capacidad de los Estados industrializados para proyectar influencia más allá de sus fronteras (Hobsbawm, 1999).

La industrialización fortaleció particularmente a Reino Unido, Alemania, Francia y posteriormente Estados Unidos, cuya expansión económica estuvo estrechamente vinculada al acceso a recursos naturales, mercados internacionales y capacidades tecnológicas superiores (Kennedy, 1989).

Wallerstein (2004) sostiene que la expansión del capitalismo industrial consolidó una estructura jerárquica internacional basada en la diferenciación entre economías centrales, semiperiféricas y periféricas. Esta configuración dio lugar a relaciones de dependencia que continúan influyendo en la distribución global de riqueza y capacidad tecnológica.

1.1.4 El orden liberal internacional después de 1945

La Segunda Guerra Mundial produjo una reestructuración profunda de la gobernanza internacional. Como respuesta a los efectos devastadores del conflicto, se creó una nueva arquitectura institucional destinada a promover la cooperación económica y la estabilidad política (Ikenberry, 2018).

Entre las principales instituciones destacan:

- Organización de las Naciones Unidas (ONU).
- Fondo Monetario Internacional (FMI).
- Banco Mundial.
- Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT).

Estas organizaciones reflejaron la creciente importancia de la cooperación institucional para gestionar problemas cuya resolución superaba las capacidades individuales de los Estados (Keohane, 1984).

Ikenberry (2018) argumenta que el orden liberal internacional se sustentó en tres pilares fundamentales:

1. Multilateralismo.
2. Apertura económica.
3. Liderazgo estadounidense.

No obstante, la expansión de instituciones internacionales también comenzó a modificar el ejercicio tradicional de la soberanía, introduciendo mecanismos de gobernanza supranacional que condicionaban parcialmente la autonomía estatal (Slaughter, 2004).

1.1.5 Interdependencia compleja y globalización

A finales del siglo XX, la aceleración de la globalización transformó significativamente la naturaleza de las relaciones internacionales. Keohane y Nye (2012) desarrollaron el concepto de interdependencia compleja para describir un contexto caracterizado por múltiples canales de interacción entre Estados, empresas, organismos internacionales y actores no estatales.

Según estos autores, la interdependencia compleja presenta tres características fundamentales:

- Existencia de múltiples canales de relación.
- Ausencia de una jerarquía clara entre temas internacionales.
- Menor relevancia del uso de la fuerza militar en determinadas áreas.

La expansión de la globalización generó niveles sin precedentes de integración económica y financiera. Entre 1990 y 2020, los flujos internacionales de comercio, inversión extranjera directa y datos digitales crecieron exponencialmente, incrementando la conectividad global y reduciendo la capacidad de los Estados para controlar completamente los procesos transnacionales (Baldwin, 2016).

Como consecuencia, el concepto tradicional de soberanía comenzó a coexistir con nuevas formas de gobernanza internacional basadas en redes, instituciones y mecanismos de cooperación multinivel (Held & McGrew, 2007).

1.1.6 La revolución digital y la redefinición de la soberanía

El surgimiento de Internet, las plataformas digitales y la inteligencia artificial representa uno de los cambios estructurales más importantes desde la Revolución Industrial. Castells (2010) argumenta que la sociedad contemporánea se organiza crecientemente en torno a redes digitales globales donde la información constituye el principal recurso estratégico.

En esta nueva etapa histórica, la capacidad para recopilar, procesar y explotar datos se ha convertido en un factor decisivo de poder económico y político (Zuboff, 2019). Como resultado, los Estados enfrentan crecientes desafíos para ejercer control sobre infraestructuras tecnológicas transnacionales que operan fuera de las lógicas territoriales tradicionales.

Farrell y Newman (2019) introducen el concepto de **interdependencia armada (weaponized interdependence)** para explicar cómo los actores que controlan nodos estratégicos de redes globales pueden utilizar dicha posición para ejercer influencia geopolítica. Este enfoque resulta particularmente relevante para comprender las disputas contemporáneas en torno a:

- Inteligencia artificial.
- Semiconductores.
- Servicios en la nube.
- Redes 5G.
- Plataformas digitales.

En consecuencia, surge el concepto de **soberanía digital**, entendido como la capacidad de una sociedad para gobernar sus datos, infraestructuras tecnológicas y ecosistemas digitales de manera autónoma y segura (Floridi, 2020).

1.1.7 Hacia un nuevo orden mundial digital

El sistema internacional contemporáneo se encuentra inmerso en una transición caracterizada por la convergencia de factores tecnológicos, económicos y geopolíticos. La competencia entre Estados Unidos y China por el liderazgo en inteligencia artificial, computación avanzada y semiconductores refleja la emergencia de nuevas formas de poder cuya lógica difiere sustancialmente de las dinámicas tradicionales del siglo XX (Allison, 2017; Bremmer, 2022).

La posesión de recursos estratégicos ya no depende exclusivamente del control territorial o militar. Actualmente, elementos como los datos, la capacidad de cómputo, el talento científico y la innovación tecnológica constituyen componentes fundamentales de la capacidad estatal y la influencia internacional (Nye, 2024).

Por tanto, la evolución del sistema internacional evidencia una transformación progresiva desde un orden basado principalmente en la soberanía territorial hacia un entorno donde la soberanía digital, la interdependencia tecnológica y la gobernanza global desempeñan un papel cada vez más relevante. Esta transición constituye el fundamento sobre el que se desarrollan las Relaciones Internacionales 6.0.

1.2. Realismo, liberalismo y constructivismo ante la transformación digital

La transformación digital constituye uno de los fenómenos más disruptivos para la teoría de las Relaciones Internacionales desde el final de la Guerra Fría. La expansión de la inteligencia artificial, el análisis masivo de datos, la computación en la nube, las plataformas digitales y las infraestructuras globales de información ha modificado las

bases materiales y simbólicas sobre las cuales se estructura el poder internacional. Sin embargo, estas innovaciones no implican necesariamente la obsolescencia de las teorías clásicas de las Relaciones Internacionales. Por el contrario, el realismo, el liberalismo y el constructivismo continúan proporcionando herramientas analíticas esenciales para interpretar las nuevas dinámicas del sistema internacional, aunque requieren adaptaciones conceptuales que permitan comprender fenómenos emergentes asociados al entorno digital.

Las Relaciones Internacionales 6.0 parten de la premisa de que las tecnologías digitales no operan en un vacío político. Su desarrollo, difusión y regulación están condicionados por relaciones de poder, intereses estratégicos, instituciones y construcciones normativas que continúan siendo explicadas, al menos parcialmente, por los principales paradigmas teóricos de la disciplina. En consecuencia, comprender la geopolítica de la inteligencia artificial, la gobernanza de los datos o la competencia tecnológica global exige revisar críticamente las contribuciones y limitaciones de estas perspectivas tradicionales.

1.2.1. El realismo y la competencia tecnológica como nueva expresión del poder

El realismo ha sido históricamente una de las corrientes teóricas más influyentes de las Relaciones Internacionales. Desde esta perspectiva, el sistema internacional se caracteriza por la ausencia de una autoridad superior capaz de garantizar la seguridad de los Estados, generando una condición de anarquía que impulsa la competencia permanente por el poder y la supervivencia (Waltz, 1979; Mearsheimer, 2001).

Para los realistas, los Estados siguen siendo los actores fundamentales del sistema internacional, mientras que la tecnología constituye un instrumento que puede modificar la distribución relativa de capacidades entre las potencias. En consecuencia, la revolución digital debe interpretarse como una nueva dimensión de la competencia estratégica interestatal.

Según Mearsheimer (2001), las grandes potencias buscan maximizar su poder relativo con el objetivo de evitar vulnerabilidades frente a posibles rivales. Esta lógica resulta particularmente evidente en la actual rivalidad tecnológica entre Estados Unidos y China, donde la inteligencia artificial, los semiconductores avanzados, las redes de

telecomunicaciones y la computación cuántica se han convertido en activos estratégicos comparables al poder naval o nuclear del siglo XX.

Desde una perspectiva neorrealista, la competencia tecnológica no responde únicamente a objetivos económicos, sino que constituye un componente central de la seguridad nacional. La capacidad para desarrollar sistemas de inteligencia artificial avanzados, procesar grandes volúmenes de datos o controlar infraestructuras digitales críticas puede traducirse en ventajas militares, económicas y diplomáticas significativas (Allison, 2017).

Figura 1.1

Interpretación realista de la transformación digital



Fuente: Elaboración autores

La creciente importancia de los semiconductores ilustra claramente esta lógica. Actualmente, la producción mundial de chips avanzados se encuentra altamente concentrada en un reducido grupo de países y empresas, generando dependencias estratégicas que afectan la seguridad nacional de múltiples Estados (Miller, 2022).

1.2.2. La reinterpretación realista del poder en la era digital

La revolución digital obliga a ampliar la concepción tradicional del poder propuesta por el realismo clásico. Si durante gran parte de la historia moderna los recursos estratégicos estuvieron asociados al territorio, la industria y la capacidad militar, en el siglo XXI emergen nuevas fuentes de influencia vinculadas al control de datos e infraestructuras tecnológicas.

Nye (2024) sostiene que el poder contemporáneo depende cada vez más de la combinación entre recursos materiales e intangibles. En este contexto, la capacidad de desarrollar algoritmos avanzados, controlar plataformas digitales y acceder a sistemas de cómputo de alto rendimiento constituye un determinante fundamental de la influencia internacional.

Tabla 1.2

Evolución realista de los recursos estratégicos

Periodo histórico	Recurso dominante
Siglo XVII	Territorio
Siglo XIX	Industria
Siglo XX	Poder militar
Finales del siglo XX	Capital financiero
Siglo XXI	Datos e inteligencia artificial

Fuente: Elaboración autores

La denominada "carrera tecnológica" entre Estados Unidos y China refleja precisamente una disputa por la acumulación de estos nuevos recursos estratégicos. Desde una visión realista, el liderazgo tecnológico no representa únicamente una ventaja económica, sino una condición imprescindible para mantener posiciones de poder dentro del sistema internacional.

1.2.3. Liberalismo: cooperación internacional e instituciones digitales

A diferencia del realismo, el liberalismo sostiene que la cooperación internacional es posible incluso bajo condiciones de anarquía. La interdependencia económica, las instituciones internacionales y las normas compartidas reducen los incentivos para el conflicto y facilitan la coordinación entre actores (Keohane, 1984).

Desde esta perspectiva, la revolución digital crea nuevos desafíos globales cuya resolución requiere mecanismos de cooperación internacional. Ningún Estado posee la capacidad suficiente para gestionar de forma aislada cuestiones como la ciberseguridad global, la regulación de la inteligencia artificial, la gobernanza de datos o la protección de infraestructuras digitales transnacionales.

Keohane y Nye (2012) argumentan que la creciente interdependencia transforma las relaciones internacionales al multiplicar los canales de interacción entre actores estatales y no estatales. La expansión de Internet, las plataformas digitales y las cadenas globales de valor tecnológicas representan manifestaciones contemporáneas de esta dinámica.

Figura 1.2

Perspectiva liberal de la transformación digital



Fuente: Elaboración autores

Los organismos internacionales desempeñan un papel cada vez más relevante en este contexto. Instituciones como las Naciones Unidas, la Unión Internacional de Telecomunicaciones (UIT), la OCDE y la UNESCO participan activamente en la formulación de principios relacionados con la gobernanza digital, la ética de la inteligencia artificial y los derechos digitales.

1.2.4. Gobernanza digital y cooperación tecnológica

La expansión de tecnologías emergentes ha impulsado el desarrollo de nuevas formas de gobernanza global. Según Slaughter (2004), los problemas transnacionales requieren redes de cooperación multinivel que involucren gobiernos, organismos internacionales, empresas privadas y sociedad civil.

La inteligencia artificial constituye un ejemplo paradigmático. Los riesgos asociados a la discriminación algorítmica, la vigilancia masiva, la desinformación automatizada o las aplicaciones militares autónomas han generado crecientes demandas de regulación internacional (Floridi, 2014).

Desde una visión liberal, los marcos regulatorios internacionales no limitan necesariamente la soberanía estatal, sino que contribuyen a gestionar problemas colectivos que ningún actor puede resolver por sí solo. Esta lógica explica el creciente interés por construir mecanismos globales de cooperación tecnológica basados en principios compartidos de transparencia, seguridad y responsabilidad.

1.2.5. Constructivismo: ideas, identidades y poder digital

El constructivismo introduce una perspectiva diferente al sostener que la política internacional no está determinada exclusivamente por factores materiales, sino también por ideas, normas e identidades socialmente construidas (Wendt, 1999).

Desde este enfoque, la transformación digital no debe analizarse únicamente como un cambio tecnológico, sino también como una transformación cultural y normativa que redefine las percepciones de legitimidad, autoridad y poder.

Wendt (1999) resume esta posición mediante una de las afirmaciones más influyentes de la disciplina: la anarquía es lo que los Estados hacen de ella. Esta premisa implica que los

efectos de la revolución digital dependen de las interpretaciones sociales y políticas que los actores asignan a las nuevas tecnologías.

Por ejemplo, conceptos como:

- Inteligencia artificial responsable.
- Derechos digitales.
- Ciudadanía digital.
- Soberanía tecnológica.
- Ética algorítmica.

no poseen significados universales preexistentes. Su contenido emerge a través de procesos de interacción, negociación y construcción normativa entre múltiples actores.

Figura 1.3

Enfoque constructivista sobre la transformación digital



Fuente: Elaboración autores

1.2.6. La batalla por las narrativas tecnológicas

Uno de los aportes más relevantes del constructivismo al estudio de las Relaciones Internacionales 6.0 consiste en destacar la importancia de las narrativas tecnológicas.

Las potencias contemporáneas no solo compiten por infraestructura o innovación, sino también por imponer interpretaciones legítimas sobre el futuro digital. Estados Unidos, China y la Unión Europea promueven modelos diferenciados de gobernanza tecnológica que reflejan valores políticos e institucionales distintos (Farrell & Newman, 2019).

Por ejemplo:

- Estados Unidos enfatiza la innovación impulsada por el mercado.
- La Unión Europea prioriza los derechos fundamentales y la regulación.
- China promueve un enfoque asociado a la soberanía digital y la estabilidad estatal.

Estas diferencias evidencian que la competencia tecnológica contemporánea también constituye una disputa por normas, valores y modelos de organización social.

Tabla 1.3

Interpretaciones constructivistas de la gobernanza digital

Actor	Narrativa predominante
Estados Unidos	Innovación y libre mercado
Unión Europea	Derechos digitales y regulación
China	Soberanía digital y control estatal
Naciones Unidas	Gobernanza multilateral

Fuente: Elaboración autores

1.2.7. Hacia una síntesis teórica para las Relaciones Internacionales 6.0

Ninguna teoría clásica puede explicar por sí sola la complejidad de la transformación digital. El realismo permite comprender la competencia estratégica por recursos tecnológicos; el liberalismo explica la necesidad de cooperación e instituciones digitales; y el constructivismo aporta herramientas para analizar las disputas normativas y simbólicas asociadas a la revolución tecnológica.

Las Relaciones Internacionales 6.0 proponen una integración de estos enfoques para interpretar un sistema internacional caracterizado simultáneamente por:

- Rivalidad geopolítica.
- Interdependencia tecnológica.
- Producción normativa global.
- Transformaciones culturales digitales.

1.3. Economía política internacional: tecnología, acumulación y relaciones de dependencia

La economía política internacional (EPI) constituye uno de los enfoques más relevantes para comprender la relación entre poder, mercados, producción y distribución de recursos dentro del sistema internacional. Mientras las teorías tradicionales de las Relaciones Internacionales se han concentrado en la seguridad y la diplomacia, la EPI analiza cómo las estructuras económicas globales condicionan las capacidades de los Estados, las empresas y otros actores para ejercer influencia en el escenario internacional (Gilpin, 2001; O'Brien & Williams, 2020).

En el siglo XXI, la transformación digital ha modificado profundamente la arquitectura económica global. La información, los datos, los algoritmos y la inteligencia artificial se han convertido en factores estratégicos de acumulación económica y generación de poder político. En consecuencia, los procesos de industrialización que definieron la economía internacional durante los siglos XIX y XX están siendo complementados por nuevas formas de acumulación basadas en el conocimiento, la capacidad computacional y el control de ecosistemas digitales (Castells, 2010; Zuboff, 2019).

Esta realidad plantea interrogantes fundamentales para las Relaciones Internacionales 6.0: ¿quién controla la economía digital global?, ¿cómo se distribuye el valor generado por las tecnologías emergentes?, ¿qué nuevas formas de dependencia surgen a partir del dominio tecnológico? y ¿de qué manera estas dinámicas transforman la estructura del poder internacional?

1.3.1. La economía política internacional como estudio del poder y la riqueza

La economía política internacional surge como un campo interdisciplinario destinado a explicar la interacción entre política y economía a escala global. Según Gilpin (2001), la principal preocupación de la disciplina consiste en analizar cómo las relaciones de poder influyen en la producción, distribución y consumo de riqueza entre actores internacionales.

Desde esta perspectiva, la economía mundial no constituye un espacio neutral de intercambio, sino una estructura donde diferentes actores compiten por maximizar beneficios y preservar posiciones de influencia. Los mercados internacionales están profundamente condicionados por instituciones, normas, capacidades tecnológicas y relaciones de poder que favorecen a determinados actores sobre otros (Strange, 1996).

1.3.2. Tecnología y transformación de los mecanismos de acumulación

La historia económica internacional puede interpretarse como una sucesión de transformaciones tecnológicas que modifican las principales fuentes de riqueza y poder.

Durante la Revolución Industrial, la acumulación dependía principalmente de:

- Manufactura.
- Producción industrial.
- Capital físico.
- Recursos energéticos.

Sin embargo, en la economía contemporánea, el conocimiento se ha convertido en un activo estratégico fundamental. Drucker (1993) fue uno de los primeros autores en anticipar el surgimiento de una economía basada en el conocimiento, donde la información reemplazaría progresivamente a los factores tradicionales de producción.

Castells (2010) sostiene que la economía informacional se caracteriza por la capacidad para generar, procesar y aplicar conocimiento mediante redes digitales globales. Como resultado, la innovación tecnológica adquiere una importancia comparable a la que tuvo la industrialización durante los siglos XIX y XX.

Tabla 1.4

Evolución histórica de los factores de acumulación

Periodo	Factor dominante de acumulación
Economía agraria	Tierra
Revolución Industrial	Industria
Capitalismo financiero	Capital
Globalización	Información
Economía digital	Datos e inteligencia artificial

Fuente: Elaboración autores

La digitalización ha convertido los datos en uno de los activos más valiosos de la economía mundial. Las organizaciones capaces de recopilar, procesar y explotar grandes volúmenes de información poseen ventajas competitivas extraordinarias frente a otros actores económicos (Mayer-Schönberger & Cukier, 2013).

1.3.3. El surgimiento del capitalismo digital

La expansión de Internet y las plataformas tecnológicas ha impulsado el desarrollo de una nueva fase del capitalismo caracterizada por la centralidad de los datos como fuente de valor económico.

Srnicek (2017) define este modelo como capitalismo de plataformas, un sistema donde las empresas digitales actúan como intermediarias de múltiples interacciones sociales y económicas, capturando información que posteriormente es utilizada para generar nuevos productos, servicios y mercados.

Google, Amazon, Microsoft, Meta, Apple y Alibaba constituyen ejemplos paradigmáticos de esta transformación. Estas organizaciones no solo ofrecen servicios digitales, sino que también poseen la capacidad de recopilar enormes cantidades de datos que fortalecen continuamente sus posiciones competitivas.

Zuboff (2019) denomina este fenómeno capitalismo de vigilancia, enfatizando cómo la extracción masiva de datos personales se ha convertido en una fuente esencial de acumulación económica.

1.3.4. Poder estructural y control de la economía digital

Susan Strange (1996) introdujo el concepto de **poder estructural** para describir la capacidad de ciertos actores para determinar las reglas de funcionamiento de la economía internacional.

Según esta autora, el verdadero poder no consiste únicamente en influir sobre decisiones específicas, sino en moldear las estructuras dentro de las cuales dichas decisiones son tomadas.

En la actualidad, las empresas tecnológicas globales ejercen formas significativas de poder estructural mediante el control de:

- Infraestructuras digitales.
- Servicios de computación en la nube.
- Sistemas operativos.
- Plataformas de comercio electrónico.
- Mercados de aplicaciones.
- Ecosistemas de inteligencia artificial.

Esta realidad ha llevado a algunos autores a señalar que las grandes corporaciones tecnológicas poseen una capacidad de influencia comparable a la de numerosos Estados nacionales (Farrell & Newman, 2019).

Tabla 1.5

Fuentes contemporáneas de poder estructural digital

Recurso	Impacto estratégico
Datos	Ventaja competitiva
Infraestructura cloud	Dependencia tecnológica
Algoritmos	Influencia económica
Plataformas	Control de mercados
IA	Innovación y productividad

Fuente: Elaboración autores

1.3.5. Dependencia tecnológica y nuevas desigualdades internacionales

Uno de los principales desafíos de la economía digital consiste en la creciente concentración de capacidades tecnológicas en un reducido grupo de países.

La teoría de la dependencia desarrollada por Cardoso y Faletto (1979) argumentaba que la estructura económica internacional reproducía relaciones asimétricas entre economías centrales y periféricas. Aunque formulada originalmente para explicar procesos industriales y financieros, esta perspectiva continúa siendo relevante para analizar las nuevas desigualdades tecnológicas.

Actualmente, la mayor parte de las plataformas digitales globales, los centros de investigación avanzada y las empresas líderes en inteligencia artificial se encuentran concentrados en:

- Estados Unidos.
- China.
- Unión Europea.
- Japón.
- Corea del Sur.

Mientras tanto, numerosas economías del Sur Global dependen de tecnologías desarrolladas externamente, lo que limita su capacidad para capturar valor dentro de la economía digital internacional (UNCTAD, 2024).

1.3.6. Geopolítica de la innovación y concentración tecnológica

La distribución desigual de capacidades tecnológicas ha convertido la innovación en un componente central de la competencia geopolítica.

Mazzucato (2018) sostiene que los avances tecnológicos más disruptivos suelen estar vinculados a inversiones públicas estratégicas que posteriormente generan beneficios privados. Esto implica que la innovación constituye también una cuestión de política industrial y poder estatal.

La competencia actual por los semiconductores ilustra esta dinámica. Los chips avanzados representan la infraestructura fundamental de:

- Inteligencia artificial.
- Telecomunicaciones.
- Defensa.
- Computación avanzada.

Miller (2022) demuestra que el control de las cadenas globales de semiconductores se ha convertido en uno de los principales factores de poder geoeconómico del siglo XXI.

Tabla 1.6

Recursos estratégicos en la economía digital

Recurso	Impacto estratégico
Datos	Ventaja competitiva
Infraestructura cloud	Dependencia tecnológica
Algoritmos	Influencia económica
Plataformas	Control de mercados
IA	Innovación y productividad

Fuente: Elaboración autores

La competencia por estos recursos redefine la distribución internacional del poder económico y tecnológico.

1.3.7. Hacia una economía política de las Relaciones Internacionales 6.0

Las Relaciones Internacionales 6.0 incorporan una visión ampliada de la economía política internacional donde el poder económico ya no depende exclusivamente del comercio, las finanzas o la producción industrial.

En el nuevo entorno digital, la capacidad de generar conocimiento, controlar infraestructuras tecnológicas y desarrollar inteligencia artificial se convierte en un factor determinante de la influencia internacional.

1.4. Conceptualización de las Relaciones Internacionales 6.0: alcances, dimensiones y límites analíticos

Las Relaciones Internacionales han evolucionado históricamente en respuesta a profundas transformaciones de carácter político, económico, tecnológico y social. La transición desde el sistema westfaliano hacia una sociedad global interconectada ha impulsado la aparición de nuevos marcos conceptuales destinados a interpretar fenómenos que las teorías tradicionales no explican completamente. La expansión de la inteligencia artificial, el análisis masivo de datos, la computación en la nube, la automatización avanzada, las plataformas digitales y la creciente dependencia de infraestructuras tecnológicas globales han modificado significativamente las estructuras de poder, gobernanza y cooperación internacional (Castells, 2010; Floridi, 2014).

En este contexto emerge el concepto de **Relaciones Internacionales 6.0 (RI 6.0)** como una propuesta teórica orientada a explicar las dinámicas del orden mundial en la era digital. Este enfoque reconoce que las tecnologías digitales han dejado de ser simples instrumentos auxiliares de la política internacional para convertirse en factores estructurales que condicionan la distribución del poder, la competitividad económica, la legitimidad institucional y la influencia global.

Las Relaciones Internacionales 6.0 no pretenden sustituir los paradigmas clásicos de la disciplina, sino integrarlos dentro de un modelo analítico capaz de incorporar las nuevas realidades derivadas de la revolución tecnológica contemporánea. Desde esta perspectiva, comprender la naturaleza del poder internacional exige analizar simultáneamente dimensiones geopolíticas, económicas, tecnológicas, normativas y culturales.

1.4.1. Origen conceptual de las Relaciones Internacionales 6.0

La evolución histórica de las Relaciones Internacionales puede interpretarse como un proceso de adaptación permanente a los cambios estructurales del sistema internacional. Cada revolución tecnológica ha modificado las formas de organización política, producción económica y competencia estratégica.

Las Relaciones Internacionales 6.0 representan una nueva fase caracterizada por la convergencia de múltiples revoluciones simultáneas:

- Revolución digital.
- Revolución de los datos.
- Revolución algorítmica.
- Revolución de la inteligencia artificial.
- Revolución de la conectividad global.

Según Schwab (2016), la Cuarta Revolución Industrial está redefiniendo la interacción entre los sistemas físicos, digitales y biológicos, generando impactos profundos sobre las estructuras estatales y la gobernanza global.

Bajo estas condiciones, el análisis del poder internacional ya no puede limitarse únicamente al estudio del territorio, la militarización o la economía tradicional.

1.4.2. Definición de las Relaciones Internacionales 6.0

Las Relaciones Internacionales 6.0 pueden definirse como:

Un enfoque teórico y analítico que estudia la interacción entre actores internacionales, tecnologías emergentes, datos, inteligencia artificial y sistemas de gobernanza digital, con el propósito de comprender la transformación contemporánea del poder, la cooperación, los conflictos y la configuración del orden mundial.

Esta definición incorpora elementos provenientes de diversas tradiciones teóricas.

Desde el realismo, reconoce la persistencia de la competencia estratégica entre Estados.

Desde el liberalismo, incorpora la importancia de las instituciones y la cooperación internacional.

Desde el constructivismo, considera el papel de las normas, identidades y narrativas digitales.

Desde la economía política internacional, analiza las estructuras de acumulación tecnológica y dependencia digital.

Por tanto, las Relaciones Internacionales 6.0 constituyen un enfoque multidimensional orientado a comprender un sistema internacional donde las capacidades tecnológicas se han convertido en recursos fundamentales de poder.

1.4.3. Principios fundamentales de las Relaciones Internacionales 6.0

El paradigma de las Relaciones Internacionales 6.0 se sustenta en cinco principios fundamentales.

a) Centralidad del poder digital

Los datos, los algoritmos, la inteligencia artificial y las infraestructuras tecnológicas constituyen recursos estratégicos comparables a los recursos militares, energéticos o financieros.

Nye (2024) sostiene que el poder contemporáneo depende crecientemente de la capacidad para procesar información y generar conocimiento estratégico.

b) Interdependencia tecnológica

Los Estados son cada vez más dependientes de redes internacionales de conectividad, servicios digitales y cadenas globales de valor tecnológicas.

Farrell y Newman (2019) demuestran que las redes económicas y tecnológicas generan nuevas formas de vulnerabilidad e influencia internacional.

c) Multiplicidad de actores

Las empresas tecnológicas globales, organismos internacionales, universidades, centros de investigación y plataformas digitales participan activamente en la gobernanza mundial.

d) Gobernanza multinivel

La regulación de los ecosistemas digitales involucra simultáneamente:

- Estados.
- Organismos multilaterales.
- Empresas privadas.
- Sociedad civil.
- Comunidad científica.

e) Transformación permanente

La aceleración tecnológica produce un entorno internacional caracterizado por cambios continuos y elevados niveles de incertidumbre.

Tabla 1.7

Dimensiones de las Relaciones Internacionales 6.0

Recurso	Impacto estratégico
Datos	Ventaja competitiva
Infraestructura cloud	Dependencia tecnológica
Algoritmos	Influencia económica
Plataformas	Control de mercados
IA	Innovación y productividad

Fuente: Elaboración autores

Estas dimensiones permiten superar las limitaciones de enfoques excesivamente centrados en un único nivel de análisis.

1.4.5. El poder digital como núcleo explicativo

La principal innovación conceptual de las Relaciones Internacionales 6.0 es la incorporación del poder digital como categoría analítica central.

Se define como:

La capacidad de producir, controlar, procesar y utilizar información estratégica mediante tecnologías digitales para influir en resultados políticos, económicos, sociales y geopolíticos.

El poder digital se compone de cuatro elementos fundamentales:

Infraestructura

Incluye centros de datos, cables submarinos, satélites, redes 5G, supercomputadoras y servicios en la nube.

Datos

Constituyen el insumo principal de los sistemas de inteligencia artificial.

Capacidad computacional

Permite procesar grandes volúmenes de información y desarrollar modelos avanzados de IA.

Capital humano

Comprende investigadores, científicos de datos, ingenieros y especialistas tecnológicos.

Figura 1.4

Componentes del poder digital



Fuente: Elaboración autores

Esta conceptualización amplía las categorías tradicionales de poder desarrolladas por autores como Morgenthau (2006) y Nye (2011).

1.4.6. Alcances teóricos de las Relaciones Internacionales 6.0

Las Relaciones Internacionales 6.0 poseen importantes capacidades explicativas para analizar fenómenos contemporáneos.

Entre sus principales aportes se encuentran:

Explicar la geopolítica tecnológica

Permite comprender la competencia entre Estados Unidos y China por el liderazgo en inteligencia artificial, semiconductores y computación avanzada (Allison, 2017; Miller, 2022).

Analizar la gobernanza digital

Facilita el estudio de las instituciones y mecanismos regulatorios que intentan gestionar tecnologías emergentes.

Comprender nuevas formas de dependencia

Integra aportes de la economía política internacional para examinar la concentración tecnológica global.

Estudiar conflictos híbridos

Permite analizar fenómenos como:

- Ciberataques.
- Desinformación digital.
- Operaciones de influencia.
- Guerra cognitiva.

Evaluar capacidades estatales

Proporciona indicadores para medir la preparación tecnológica de los Estados en el entorno digital.

1.4.7. Limitaciones analíticas y desafíos conceptuales

Como toda construcción teórica emergente, las Relaciones Internacionales 6.0 presentan diversas limitaciones que deben reconocerse para evitar visiones deterministas.

Riesgo de tecnocentrismo

Una de las principales críticas potenciales consiste en asumir que la tecnología explica por sí sola las dinámicas internacionales.

Cambios tecnológicos acelerados

La velocidad de innovación dificulta la construcción de modelos estables de largo plazo.

Tecnologías emergentes como la computación cuántica o la inteligencia artificial general podrían modificar sustancialmente el entorno internacional en los próximos años.

Desigualdad de capacidades

Las experiencias de los países desarrollados y del Sur Global no son homogéneas.

Por tanto, el modelo debe incorporar perspectivas diferenciadas sobre desarrollo, dependencia tecnológica y asimetrías estructurales.

Problemas de medición

Variables como:

- Influencia algorítmica.
- Capacidad digital.
- Soberanía tecnológica.
- Poder informacional.

aún presentan importantes desafíos metodológicos y estadísticos.

Tabla 1.8

Fortalezas y limitaciones de las RI 6.0

Recurso	Impacto estratégico
Datos	Ventaja competitiva
Infraestructura cloud	Dependencia tecnológica
Algoritmos	Influencia económica
Plataformas	Control de mercados
IA	Innovación y productividad

Fuente: Elaboración autores

1.4.8. Propuesta teórica integradora: Modelo RI 6.0

Como síntesis conceptual, este libro propone que la capacidad de influencia internacional en la era digital depende de la interacción de cuatro variables estratégicas:

Poder Digital (PD)

Capacidad tecnológica e infraestructura.

Gobernanza Inteligente (GI)

Capacidad regulatoria e institucional.

Capacidad Geoeconómica (CG)

Innovación, productividad y competitividad.

Influencia Internacional (II)

Capacidad diplomática y normativa.

De manera conceptual:

$$RI6 = f(PD + GI + CG + II)$$

Donde:

$$PD = Infraestructura + Datos + IA + Talento$$
$$GI = Regulación + Instituciones + Cooperación$$
$$CG = Innovación + Industria + ComercioDigital$$
$$II = Diplomacia + SoftPower + LiderazgoNormativo$$

Esta formulación constituye el núcleo analítico de las Relaciones Internacionales 6.0 y servirá como referencia para los capítulos posteriores del libro.

1.5. Reconfiguración de los actores internacionales: Estados, organismos multilaterales, empresas tecnológicas y redes transnacionales

Uno de los cambios más significativos del sistema internacional contemporáneo radica en la transformación de la estructura de actores que participan en los procesos globales de poder, gobernanza y toma de decisiones. Durante gran parte de la historia moderna, el Estado fue considerado el actor predominante de las relaciones internacionales, concentrando la autoridad política, la capacidad coercitiva y la representación legítima de la soberanía nacional (Waltz, 1979; Morgenthau, 2006). Sin embargo, la intensificación de la globalización y la revolución digital han modificado sustancialmente esta realidad.

La expansión de las tecnologías de información y comunicación, el desarrollo de plataformas digitales globales, el crecimiento de organizaciones multilaterales y la emergencia de redes transnacionales han generado un sistema internacional caracterizado por una mayor complejidad, interdependencia y dispersión del poder (Keohane & Nye, 2012; Castells, 2010). Actualmente, la influencia internacional ya no depende exclusivamente de la capacidad estatal para controlar territorios o recursos físicos. El acceso al conocimiento, la innovación tecnológica, la capacidad regulatoria y el control de infraestructuras digitales se han convertido en fuentes estratégicas de poder compartidas por una diversidad creciente de actores.

En el marco de las Relaciones Internacionales 6.0, esta transformación exige abandonar visiones exclusivamente estatocéntricas y adoptar enfoques más amplios que reconozcan la interacción dinámica entre Estados, organismos multilaterales, corporaciones tecnológicas, comunidades científicas, organizaciones de la sociedad civil y redes globales de información.

1.5.1. Del Estado westfaliano al ecosistema multinivel de actores globales

La teoría clásica de las Relaciones Internacionales asumió durante décadas que los Estados constituían los únicos actores relevantes del sistema internacional. Tanto el realismo como buena parte del liberalismo tradicional construyeron sus marcos analíticos sobre la premisa de que la política mundial estaba determinada principalmente por la interacción entre unidades soberanas (Waltz, 1979; Gilpin, 2001).

Aspectos como el cambio climático, las crisis financieras, las pandemias, la ciberseguridad y la gobernanza de la inteligencia artificial involucran simultáneamente a múltiples actores con capacidades de influencia diferenciadas (Held & McGrew, 2007).

Como resultado, el sistema internacional contemporáneo ha evolucionado hacia una estructura multinivel donde coexistenn actores estatales y no estatales con diferentes recursos de poder.

Figura 1.5

Evolución de la estructura de actores internacionales



Fuente: Elaboración autores

Esta transformación no implica la desaparición del Estado, sino su inserción dentro de una red mucho más compleja de interacciones globales.

1.5.2. El Estado como actor central en la era digital

A pesar de las profundas transformaciones derivadas de la revolución tecnológica, los Estados continúan siendo los principales titulares de soberanía y los actores con mayores capacidades formales de regulación, coerción y representación internacional (Jackson, 2007).

Lejos de perder relevancia, numerosos gobiernos han fortalecido su intervención en sectores estratégicos de la economía digital mediante:

- Políticas industriales tecnológicas.
- Regulación de plataformas digitales.
- Estrategias nacionales de inteligencia artificial.
- Protección de infraestructuras críticas.
- Programas de ciberseguridad.

La competencia tecnológica entre Estados Unidos y China constituye una evidencia clara de esta realidad. Ambos países han desarrollado políticas nacionales orientadas a consolidar liderazgo en áreas como:

- Inteligencia artificial.
- Computación cuántica.
- Semiconductores.
- Telecomunicaciones avanzadas.
- Sistemas de defensa autónomos.

Según Allison (2017), la rivalidad estratégica contemporánea refleja una competencia sistémica por la supremacía tecnológica, económica y geopolítica.

Tabla 1.9

Capacidades tradicionales y digitales del Estado

Recurso	Impacto estratégico
Datos	Ventaja competitiva
Infraestructura cloud	Dependencia tecnológica
Algoritmos	Influencia económica
Plataformas	Control de mercados

Fuente: Elaboración autores

En consecuencia, el Estado continúa siendo un actor fundamental, aunque ahora debe desarrollar nuevas capacidades tecnológicas para preservar su autonomía e influencia internacional.

1.5.3. Organismos multilaterales y gobernanza global

El crecimiento de la interdependencia internacional ha incrementado la importancia de las organizaciones multilaterales como mecanismos de coordinación, regulación y cooperación global.

Autores como Keohane (1984) sostienen que las instituciones internacionales reducen la incertidumbre y facilitan la cooperación entre actores que enfrentan problemas comunes.

En la era digital, organismos como:

- Organización de las Naciones Unidas (ONU).
- Unión Internacional de Telecomunicaciones (UIT).
- Organización para la Cooperación y el Desarrollo Económicos (OCDE).
- Banco Mundial.
- UNESCO.
- Organización Mundial del Comercio (OMC).

participan activamente en la construcción de marcos regulatorios orientados a gestionar desafíos tecnológicos emergentes.

Particularmente relevante ha sido la discusión internacional sobre inteligencia artificial ética, privacidad digital, gobernanza de datos y ciberseguridad. Estas áreas evidencian que ningún Estado posee capacidad suficiente para regular unilateralmente fenómenos tecnológicos que operan a escala global (Floridi, 2014).

Sin embargo, los organismos multilaterales enfrentan desafíos crecientes asociados a la fragmentación geopolítica y a la competencia entre grandes potencias por definir las reglas del orden digital emergente.

1.5.4. Empresas tecnológicas como actores geopolíticos

Una de las transformaciones más profundas de las Relaciones Internacionales contemporáneas es el surgimiento de grandes corporaciones tecnológicas con capacidades de influencia comparables a las de numerosos Estados.

Empresas como:

- Microsoft.
- Google (Alphabet).
- Amazon.
- Meta.
- Apple.
- Alibaba.

controlan infraestructuras esenciales para el funcionamiento de la economía digital global.

Estas organizaciones gestionan:

- Centros de datos.
- Servicios cloud.
- Sistemas operativos.
- Plataformas de comunicación.
- Mercados digitales.
- Herramientas de inteligencia artificial.

Asimismo, poseen recursos financieros que superan el producto interno bruto de numerosos países en desarrollo (Srnicek, 2017; Zuboff, 2019).

Tabla 1.10

Recursos estratégicos de las empresas tecnológicas globales

Recurso	Impacto estratégico
Datos	Ventaja competitiva
Infraestructura cloud	Dependencia tecnológica
Algoritmos	Influencia económica
Plataformas	Control de mercados
IA	Innovación y productividad

Fuente: Elaboración autores

Susan Strange (1996) argumentó que el verdadero poder internacional reside en la capacidad para moldear estructuras y reglas. Bajo esta lógica, las grandes plataformas tecnológicas ejercen formas significativas de poder estructural al controlar nodos esenciales de la economía digital global.

1.5.5. Redes transnacionales y nuevas comunidades de influencia

La globalización también ha favorecido el desarrollo de redes transnacionales integradas por actores que operan más allá de las fronteras estatales.

Keck y Sikkink (1998) fueron pioneras en demostrar cómo las redes transnacionales pueden influir en decisiones políticas internacionales mediante la producción de conocimiento, movilización social y difusión de normas.

Actualmente estas redes incluyen:

- Universidades internacionales.
- Centros de investigación.
- Comunidades científicas.
- Organizaciones no gubernamentales.
- Movimientos sociales digitales.
- Consorcios tecnológicos.

Su influencia resulta particularmente significativa en áreas relacionadas con:

- Cambio climático.
- Derechos digitales.
- Ética de la inteligencia artificial.
- Gobernanza de Internet.
- Protección de datos.

Figura 1.6

Ecosistema de redes transnacionales



Fuente: Elaboración autores

Castells (2010) sostiene que estas estructuras constituyen expresiones de la sociedad red, donde la capacidad de conectarse y coordinar información se convierte en una fuente esencial de influencia.

1.5.6. El surgimiento de las plataformas como espacios de gobernanza

Las plataformas digitales no solo funcionan como empresas privadas, sino también como estructuras de regulación capaces de influir sobre comportamientos sociales, económicos y políticos.

Facebook, X, YouTube, TikTok o LinkedIn establecen permanentemente reglas sobre:

- Acceso a contenidos.
- Moderación de información.
- Protección de usuarios.

- Gestión de datos.
- Publicidad política.

Esta situación ha llevado a algunos autores a describirlas como formas emergentes de gobernanza privada transnacional (Zuboff, 2019).

En muchos casos, las decisiones tomadas por estas plataformas afectan simultáneamente a millones de usuarios distribuidos en múltiples jurisdicciones nacionales.

1.5.7. Relaciones Internacionales 6.0 y la multipolaridad de actores

Las Relaciones Internacionales 6.0 reconocen que el sistema internacional contemporáneo ha evolucionado hacia una estructura donde el poder se encuentra distribuido entre múltiples actores interdependientes.

Desde esta perspectiva, la capacidad de influencia internacional depende cada vez más de la habilidad para coordinar recursos provenientes de diversos actores dentro de ecosistemas digitales complejos.

1.6. Poder material, institucional y simbólico: articulación con las capacidades digitales

La comprensión del poder ha constituido históricamente uno de los principales ejes analíticos de las Relaciones Internacionales. Desde los planteamientos clásicos de Hans Morgenthau (2006) hasta las contribuciones contemporáneas de Joseph Nye (2011, 2024), la capacidad de influir sobre el comportamiento de otros actores ha sido considerada el elemento central para explicar la dinámica del sistema internacional. Sin embargo, la revolución digital está transformando profundamente los mecanismos mediante los cuales el poder es acumulado, proyectado y ejercido.

Tradicionalmente, el poder internacional se asociaba a recursos tangibles como la fuerza militar, la capacidad económica o el control territorial. No obstante, la creciente relevancia de la información, los datos, la inteligencia artificial, las plataformas digitales y las infraestructuras tecnológicas globales ha ampliado considerablemente las fuentes de influencia internacional. En consecuencia, el poder contemporáneo debe entenderse como

una combinación dinámica de recursos materiales, institucionales y simbólicos articulados mediante capacidades digitales avanzadas (Castells, 2010; Nye, 2011).

Desde la perspectiva de las Relaciones Internacionales 6.0, las capacidades digitales no constituyen una nueva forma independiente de poder, sino un factor transversal que potencia, amplifica y reconfigura las dimensiones tradicionales del poder internacional. Esta convergencia está dando origen a nuevas formas de competencia geopolítica, gobernanza global e influencia transnacional que redefinen la arquitectura del orden mundial.

1.6.1. El concepto de poder en las Relaciones Internacionales

El poder ha sido definido de múltiples maneras dentro de la teoría internacional. Una de las conceptualizaciones más influyentes corresponde a Dahl (1957), quien sostiene que un actor ejerce poder cuando logra que otro actor realice acciones que de otro modo no llevaría a cabo.

En el ámbito de las Relaciones Internacionales, Morgenthau (2006) definió el poder como la capacidad de controlar las acciones y decisiones de otros Estados. Desde esta perspectiva, el poder constituye el objetivo principal de la política internacional y el fundamento de la seguridad estatal.

Posteriormente, Nye (2011) amplió esta visión distinguiendo entre diversas formas de poder:

- Poder duro (*hard power*).
- Poder blando (*soft power*).
- Poder inteligente (*smart power*).

Esta clasificación permitió reconocer que la influencia internacional no depende únicamente de la coerción militar o económica, sino también de la capacidad para atraer, La transformación digital obliga a reconsiderar estas aproximaciones, ya que el control de la información, los algoritmos y las plataformas tecnológicas se ha convertido en un componente fundamental de la influencia global.

1.6.2. Poder material en la era digital

El poder material se refiere a los recursos tangibles que permiten a los actores ejercer influencia internacional. Tradicionalmente ha incluido elementos como:

- Fuerza militar.
- Capacidad industrial.
- Recursos energéticos.
- Tamaño económico.
- Infraestructura estratégica.

Desde la perspectiva realista, estas capacidades continúan siendo fundamentales para la competencia internacional (Waltz, 1979; Mearsheimer, 2001). Sin embargo, la revolución digital ha ampliado significativamente la naturaleza de los recursos materiales estratégicos.

Actualmente, la infraestructura tecnológica constituye una dimensión esencial del poder material.

Componentes contemporáneos del poder material digital

- Centros de datos.
- Redes 5G y 6G.
- Satélites de comunicaciones.
- Supercomputadoras.
- Infraestructura cloud.
- Semiconductores avanzados.
- Computación cuántica.

Miller (2022) argumenta que los semiconductores representan el recurso estratégico más importante del siglo XXI debido a que sustentan prácticamente todas las actividades vinculadas a la economía digital, la inteligencia artificial y los sistemas de defensa.

La creciente disputa entre Estados Unidos y China por el control de cadenas de suministro tecnológicas evidencia cómo las capacidades digitales se han convertido en un componente central de la seguridad nacional (Allison, 2017; Miller, 2022).

1.6.3. Poder institucional y gobernanza digital

El poder institucional hace referencia a la capacidad de influir en las reglas, normas y procedimientos que regulan las interacciones internacionales (Keohane, 1984).

A diferencia del poder material, esta forma de influencia no depende directamente de recursos coercitivos, sino de la capacidad para moldear los marcos institucionales dentro de los cuales operan otros actores.

Según Keohane (1984), las instituciones internacionales reducen los costos de cooperación, generan información y establecen expectativas de comportamiento que facilitan la gobernanza global.

En la era digital, el poder institucional se manifiesta crecientemente mediante la capacidad para definir estándares tecnológicos y marcos regulatorios relacionados con:

- Inteligencia artificial.
- Protección de datos.
- Ciberseguridad.
- Comercio digital.
- Gobernanza de Internet.

La Unión Europea constituye uno de los ejemplos más relevantes de esta modalidad de poder. A través del Reglamento General de Protección de Datos (GDPR) y del futuro marco regulatorio de inteligencia artificial, la UE ha logrado proyectar influencia normativa más allá de sus fronteras, fenómeno que Bradford (2020) denomina **Brussels Effect**.

La regulación tecnológica se ha convertido así en una nueva fuente de competencia geopolítica por la definición de las reglas que estructurarán el orden digital internacional.

1.6.4. Poder simbólico e influencia en la sociedad digital

Pierre Bourdieu (1991) desarrolló el concepto de poder simbólico para describir la capacidad de moldear percepciones, valores y significados sociales.

En el ámbito internacional, esta noción se relaciona estrechamente con el concepto de poder blando desarrollado por Nye (2004, 2011), entendido como la capacidad de obtener resultados mediante atracción y legitimidad en lugar de coerción.

La revolución digital ha multiplicado exponencialmente las oportunidades para ejercer influencia simbólica a través de:

- Redes sociales.
- Plataformas digitales.
- Medios de comunicación globales.
- Ecosistemas culturales.
- Producción de contenido digital.

Figura 1.7

Fuentes contemporáneas del poder simbólico



Fuente: Elaboración autores

Castells (2010) sostiene que la comunicación constituye actualmente uno de los espacios centrales donde se disputa el poder. Quienes controlan la producción y circulación de información poseen una capacidad significativa para modelar agendas políticas, preferencias sociales y percepciones colectivas.

1.6.5. La convergencia entre poder material, institucional y simbólico

Una de las principales características de la era digital es la creciente interdependencia entre las distintas formas de poder.

Las fronteras que tradicionalmente separaban el poder económico, político, militar y cultural se vuelven cada vez más difusas debido al carácter transversal de las tecnologías digitales.

Por ejemplo:

- Una plataforma digital posee recursos materiales mediante infraestructura tecnológica.
- Ejerce poder institucional mediante normas de uso y gobernanza algorítmica.
- Produce poder simbólico al influir sobre percepciones y comportamientos sociales.

Esta convergencia explica por qué las grandes empresas tecnológicas se han convertido en actores geopolíticos de relevancia internacional.

1.6.6. Capacidades digitales como multiplicadores de poder

Las capacidades digitales funcionan como multiplicadores que fortalecen simultáneamente las diferentes dimensiones del poder internacional.

Infraestructura digital

Incrementa el poder material.

Datos

Mejoran capacidades de análisis y toma de decisiones.

Inteligencia artificial

Aumenta productividad, innovación y eficiencia estratégica.

Plataformas globales

Amplían la influencia institucional y simbólica.

Capital humano tecnológico

Fortalece la adaptación frente a cambios disruptivos.

Nye (2024) sostiene que la capacidad para combinar recursos tecnológicos con mecanismos tradicionales de influencia determinará el liderazgo internacional durante las próximas décadas.

1.6.7. El surgimiento del poder digital como nueva categoría analítica

Las Relaciones Internacionales 6.0 proponen incorporar el concepto de **poder digital** como una categoría integradora capaz de explicar la articulación entre las diferentes formas de influencia contemporánea.

Definición

El poder digital puede definirse como:

La capacidad de producir, controlar, procesar y utilizar recursos tecnológicos, información estratégica, datos e inteligencia artificial para influir en decisiones, comportamientos y estructuras dentro del sistema internacional.

Componentes fundamentales

Infraestructura digital

Capacidad tecnológica instalada.

Datos estratégicos

Disponibilidad y control de información.

Inteligencia artificial

Capacidad de análisis y automatización.

Gobernanza tecnológica

Capacidad regulatoria e institucional.

Influencia cognitiva

Capacidad para moldear narrativas y percepciones.

Esta propuesta permite comprender de manera más integral las dinámicas de influencia en un entorno internacional caracterizado por la creciente centralidad de la tecnología.

1.6.8. Hacia una teoría integrada del poder en las Relaciones Internacionales 6.0

Las Relaciones Internacionales 6.0 plantean que el poder internacional contemporáneo surge de la interacción entre tres dimensiones clásicas y una dimensión emergente.

Modelo teórico

$$PI = PM + PIN + PS + PD$$

Donde:

- **PM** = Poder Material
- **PIN** = Poder Institucional
- **PS** = Poder Simbólico
- **PD** = Poder Digital

Asimismo:

$$PD = I + D + IA + G$$

Donde:

- **I** = Infraestructura digital
- **D** = Datos
- **IA** = Inteligencia artificial
- **G** = Gobernanza tecnológica

Este modelo reconoce que las capacidades digitales no sustituyen las formas tradicionales de poder, sino que las potencian y reconfiguran.

1.7. Métodos de investigación del poder internacional: análisis comparado, redes y prospectiva estratégica

La comprensión del poder internacional ha constituido uno de los principales desafíos epistemológicos y metodológicos de las Relaciones Internacionales. A medida que el sistema internacional se ha vuelto más complejo, interdependiente y tecnológicamente sofisticado, también han evolucionado las herramientas utilizadas para estudiar los procesos de influencia, cooperación, conflicto y gobernanza global. En la actualidad, fenómenos como la inteligencia artificial, las plataformas digitales, las cadenas globales de valor, los ciberconflictos y la gobernanza multinivel exigen metodologías capaces de capturar dinámicas que trascienden los enfoques tradicionales centrados exclusivamente en los Estados (Keohane & Nye, 2012; Castells, 2010).

Las Relaciones Internacionales 6.0 requieren una renovación metodológica que permita analizar tanto las formas clásicas de poder como las nuevas capacidades digitales que están transformando la estructura del orden mundial. En este contexto, el análisis comparado, el análisis de redes y la prospectiva estratégica emergen como herramientas particularmente relevantes para estudiar la distribución y evolución del poder internacional.

Estos enfoques no son excluyentes. Por el contrario, su integración permite construir marcos analíticos multidimensionales capaces de examinar simultáneamente actores, estructuras, relaciones, escenarios futuros y dinámicas de transformación tecnológica.

1.7.1. El desafío metodológico de estudiar el poder internacional

Desde los trabajos pioneros de Morgenthau (2006), Waltz (1979) y Keohane (1984), la medición del poder ha enfrentado importantes dificultades conceptuales y metodológicas. Aunque existe consenso respecto a la centralidad del poder para explicar la política internacional, no existe una única forma de definirlo ni de medirlo empíricamente.

Tradicionalmente, los estudios internacionales utilizaron variables como:

- Producto Interno Bruto (PIB).

- Gasto militar.
- Tamaño poblacional.
- Extensión territorial.
- Capacidad industrial.

Sin embargo, la revolución digital ha introducido nuevas variables difíciles de cuantificar:

- Capacidad de inteligencia artificial.
- Infraestructura computacional.
- Producción científica.
- Control de datos.
- Influencia algorítmica.
- Soberanía digital.

Según Nye (2011), el poder contemporáneo se caracteriza por una creciente complejidad debido a la coexistencia de recursos materiales e intangibles que interactúan simultáneamente.

- Datos
- IA
- Redes
- Plataformas
- Gobernanza Digital

En consecuencia, las metodologías tradicionales deben complementarse con herramientas capaces de capturar fenómenos complejos y multidimensionales.

1.7.2. El análisis comparado como herramienta para estudiar el poder internacional

El análisis comparado constituye uno de los métodos más utilizados dentro de las ciencias sociales y las Relaciones Internacionales. Su objetivo consiste en identificar similitudes y diferencias entre casos con el fin de explicar variaciones observadas en fenómenos políticos, económicos o institucionales (Lijphart, 1971).

Según Sartori (1991), comparar permite transformar observaciones aisladas en conocimiento sistemático, facilitando la construcción de explicaciones causales.

En el contexto de las Relaciones Internacionales 6.0, el análisis comparado resulta especialmente útil para estudiar:

- Estrategias nacionales de inteligencia artificial.
- Políticas de soberanía digital.
- Modelos de gobernanza tecnológica.
- Capacidades tecnológicas estatales.
- Sistemas de innovación.

Por ejemplo, la comparación entre Estados Unidos, China y la Unión Europea permite identificar diferencias significativas en la forma en que estas potencias abordan la inteligencia artificial y la regulación tecnológica.

Tabla 1.11

Caso comparado: modelos de gobernanza digital

Recurso	Impacto estratégico
Datos	Ventaja competitiva
Infraestructura cloud	Dependencia tecnológica
Algoritmos	Influencia económica
Plataformas	Control de mercados
IA	Innovación y productividad

Fuente: Elaboración autores

Esta metodología permite identificar patrones y construir tipologías que contribuyen a una mejor comprensión de las dinámicas internacionales contemporáneas.

1.7.3. Ventajas y limitaciones del análisis comparado

El análisis comparado presenta importantes ventajas para el estudio del poder internacional.

Ventajas

- Facilita la identificación de patrones comunes.

- Permite evaluar políticas públicas internacionales.
- Mejora la validez de explicaciones causales.
- Favorece la construcción teórica.

Sin embargo, también enfrenta limitaciones relevantes.

Limitaciones

- Dificultades para controlar todas las variables.
- Problemas de equivalencia conceptual entre países.
- Diferencias culturales e históricas.
- Complejidad creciente de los fenómenos digitales.

Mahoney y Thelen (2010) señalan que los procesos de cambio institucional suelen estar influenciados por múltiples factores simultáneos, dificultando el establecimiento de relaciones causales directas.

Por ello, el análisis comparado suele complementarse con otros enfoques metodológicos.

1.7.4. El análisis de redes y la comprensión de la interdependencia global

La creciente conectividad internacional ha impulsado el desarrollo del análisis de redes como una herramienta clave para comprender las estructuras contemporáneas de poder.

Castells (2010) sostiene que la sociedad actual se organiza mediante redes de información, comunicación y conocimiento que atraviesan fronteras nacionales. Como resultado, el poder depende cada vez más de la posición que los actores ocupan dentro de dichas redes.

El análisis de redes permite estudiar:

- Relaciones entre Estados.
- Flujos comerciales.
- Ecosistemas tecnológicos.
- Redes científicas.
- Infraestructuras digitales.
- Cadenas globales de suministro.

En este enfoque, la posición estratégica de un actor puede ser tan importante como los recursos que posee.

1.7.5. Conceptos fundamentales del análisis de redes

La teoría de redes incorpora conceptos específicos que permiten examinar estructuras complejas de interacción.

Nodo

Representa un actor dentro de la red.

Ejemplos:

- Estados.
- Empresas.
- Organizaciones internacionales.
- Universidades.

Vínculo

Representa una relación entre nodos.

Ejemplos:

- Comercio.
- Cooperación científica.
- Intercambio de datos.
- Alianzas tecnológicas.

Centralidad

Mide la importancia de un actor dentro de una red.

Intermediación

Evalúa la capacidad de un actor para controlar flujos de información o recursos.

Borgatti, Everett y Johnson (2018) destacan que los actores con posiciones centrales suelen ejercer mayor influencia sobre el comportamiento del sistema.

En las Relaciones Internacionales 6.0, estas métricas permiten estudiar la distribución global del poder digital.

1.7.6. Redes digitales y poder internacional

Farrell y Newman (2019) desarrollaron el concepto de **interdependencia armada** (*weaponized interdependence*) para explicar cómo ciertos actores pueden utilizar su posición privilegiada dentro de redes globales para ejercer coerción económica y política.

Según estos autores, quienes controlan nodos estratégicos de la economía digital poseen ventajas significativas en términos de:

- Vigilancia.
- Monitoreo.
- Influencia.
- Capacidad coercitiva.

Esta perspectiva resulta especialmente relevante para comprender fenómenos como:

- Dominio de plataformas digitales.
- Infraestructura cloud global.
- Redes financieras internacionales.
- Cadenas de suministro tecnológicas.

Por ello, el análisis de redes constituye una herramienta indispensable para estudiar la geopolítica digital contemporánea.

1.7.7. Prospectiva estratégica y anticipación del cambio internacional

La aceleración tecnológica ha incrementado los niveles de incertidumbre que enfrentan gobiernos, empresas y organizaciones internacionales.

En este contexto, la prospectiva estratégica surge como una metodología orientada a explorar futuros posibles y reducir la incertidumbre asociada a procesos complejos de transformación (Godet, 2006).

A diferencia de la predicción tradicional, la prospectiva no busca anticipar un único futuro, sino identificar múltiples escenarios plausibles.

Según Schwartz (1996), esta metodología permite mejorar la preparación estratégica frente a cambios disruptivos.

Este enfoque resulta particularmente útil en contextos caracterizados por innovaciones tecnológicas aceleradas.

1.7.8. Herramientas de prospectiva aplicadas a las RI 6.0

Las Relaciones Internacionales 6.0 incorporan diversas herramientas prospectivas para analizar la evolución del poder internacional.

Método Delphi

Consiste en consultas sistemáticas a expertos con el fin de identificar tendencias futuras.

Construcción de escenarios

Permite analizar distintos futuros alternativos.

Análisis estructural

Identifica variables clave y relaciones de influencia.

Vigilancia estratégica

Realiza monitoreo continuo de cambios tecnológicos y geopolíticos.

Tabla 1.12

Técnicas de prospectiva estratégica

Recurso	Impacto estratégico
Datos	Ventaja competitiva
Infraestructura cloud	Dependencia tecnológica
Algoritmos	Influencia económica
Plataformas	Control de mercados
IA	Innovación y productividad

Fuente: Elaboración autores

Estas metodologías son ampliamente utilizadas por organismos internacionales, gobiernos y centros de investigación estratégica.

1.7.9. Propuesta metodológica para las Relaciones Internacionales 6.0

Este libro propone una estrategia metodológica integrada para estudiar el poder internacional en la era digital.

- **Fase 1 .** Análisis comparado de capacidades nacionales.
- **Fase 2.** Análisis de redes para identificar estructuras de influencia.
- **Fase 3.** Construcción de escenarios prospectivos.

Este enfoque permite combinar evidencia empírica, análisis estructural y anticipación estratégica en una sola arquitectura metodológica.

EDITORIAL ANDES COGNITIO

CAPÍTULO II

GEOPOLÍTICA INTELIGENTE: DATOS, INTELIGENCIA ARTIFICIAL Y COMPETENCIA ESTRATEGICA



CAPÍTULO II

GEOPOLÍTICA INTELIGENTE: DATOS, INTELIGENCIA ARTIFICIAL Y COMPETENCIA ESTRATÉGICA

Las transformaciones tecnológicas de las primeras décadas del siglo XXI están modificando profundamente las bases sobre las cuales se distribuye el poder internacional. Si durante la Guerra Fría el equilibrio estratégico dependía principalmente de la posesión de capacidades militares, arsenales nucleares y recursos industriales, en la actualidad los datos, los algoritmos, la inteligencia artificial (IA), los semiconductores y las infraestructuras digitales constituyen elementos fundamentales para la competencia entre Estados y otros actores internacionales (Farrell & Newman, 2019; Nye, 2024).

Esta realidad ha impulsado la aparición de un nuevo paradigma analítico que puede denominarse geopolítica inteligente, entendido como el estudio de la interacción entre territorio, tecnología, información y capacidad de decisión estratégica dentro del sistema internacional contemporáneo. A diferencia de la geopolítica clásica, centrada principalmente en variables geográficas y militares, la geopolítica inteligente incorpora recursos digitales que redefinen las fuentes tradicionales de ventaja estratégica (Khanna, 2016).

La creciente rivalidad entre Estados Unidos y China por el liderazgo en inteligencia artificial, computación avanzada y producción de semiconductores evidencia que la competencia internacional ya no se limita al control de espacios físicos. Actualmente, la influencia geopolítica depende también del dominio de infraestructuras digitales, flujos de datos, ecosistemas de innovación y capacidades algorítmicas (Allison, 2017; Miller, 2022).

Este capítulo examina cómo la revolución digital está transformando los fundamentos del poder internacional mediante el análisis de la inteligencia artificial, los datos, las infraestructuras críticas y los mecanismos de anticipación estratégica que caracterizan a las Relaciones Internacionales 6.0.

2.1 Geopolítica inteligente: integración del análisis territorial, tecnológico y de información

2.1.1. De la geopolítica clásica a la geopolítica inteligente

La geopolítica surgió como una disciplina interesada en analizar la relación entre el espacio geográfico y el poder político. Autores clásicos como Friedrich Ratzel (1897), Halford Mackinder (1904) y Nicholas Spykman (1942) sostuvieron que la posición geográfica y el control territorial constituían factores determinantes para la proyección de influencia internacional.

Mackinder (1904), por ejemplo, formuló su conocida teoría del *Heartland*, afirmando que el control de Eurasia determinaba la distribución global del poder. Posteriormente, Spykman (1942) destacó la importancia estratégica del *Rimland*, enfatizando las regiones costeras como espacios clave para la competencia geopolítica.

Durante gran parte del siglo XX, estas perspectivas orientaron el análisis de conflictos, alianzas y estrategias de seguridad internacional. Sin embargo, la revolución digital ha transformado significativamente esta lógica.

Según Bratton (2016), la arquitectura contemporánea del poder ya no se encuentra exclusivamente determinada por la geografía física, sino también por infraestructuras informacionales distribuidas globalmente que operan mediante plataformas, centros de datos, redes satelitales y sistemas algorítmicos.

Como consecuencia, el territorio continúa siendo relevante, pero ahora se encuentra complementado por nuevas capas digitales que configuran una geografía ampliada del poder.

2.1.2. Definición de geopolítica inteligente

La geopolítica inteligente puede definirse como:

El estudio de las relaciones entre espacio geográfico, infraestructura tecnológica, inteligencia artificial, datos y procesos de toma de decisiones estratégicas que determinan la distribución del poder en el sistema internacional contemporáneo.

Esta conceptualización integra tres dimensiones fundamentales:

Dimensión territorial

Comprende:

- Recursos naturales estratégicos.
- Posición geográfica.
- Infraestructura física.
- Corredores logísticos.
- Acceso energético.

Dimensión tecnológica

Incluye:

- Inteligencia artificial.
- Computación avanzada.
- Semiconductores.
- Redes digitales.
- Innovación tecnológica.

Dimensión informacional

Considera:

- Datos.
- Algoritmos.
- Plataformas digitales.
- Sistemas de vigilancia.
- Capacidades analíticas.

2.1.3. Datos como nuevo recurso geopolítico

La economía internacional contemporánea se caracteriza por la creciente importancia de los datos como recurso estratégico. Diversos autores han señalado que los datos constituyen el principal insumo de la inteligencia artificial y uno de los activos más valiosos del siglo XXI (Mayer-Schönberger & Cukier, 2013; Zuboff, 2019).

A diferencia de los recursos naturales tradicionales, los datos presentan características particulares:

- Son reproducibles.
- Pueden ser utilizados simultáneamente por múltiples actores.
- Generan rendimientos crecientes.
- Adquieren valor mediante procesamiento algorítmico.

Consecuentemente, la capacidad para recopilar, almacenar y analizar grandes volúmenes de información se ha convertido en una fuente estratégica de ventaja internacional.

Tabla 2.1

Comparación entre recursos geopolíticos tradicionales y digitales

Recurso	Siglo predominante	Función estratégica
Territorio	XIX	Expansión estatal
Petróleo	XX	Industrialización
Energía nuclear	XX	Disuasión
Datos	XXI	Inteligencia estratégica
IA	XXI	Ventaja competitiva

Fuente: Elaboración autores

2.1.4. Estados Unidos y China: la competencia por la supremacía digital

El principal escenario de la geopolítica inteligente contemporánea está representado por la rivalidad entre Estados Unidos y China.

Según Allison (2017), esta competencia reúne características comparables a las grandes transiciones de poder históricas descritas por la denominada "Trampa de Tucídides".

Actualmente ambos países lideran sectores clave:

Estados Unidos

- Computación avanzada.
- Plataformas digitales globales.

- Servicios cloud.
- Innovación universitaria.
- Capital de riesgo.

China

- Aplicaciones de inteligencia artificial.
- Comercio electrónico.
- Ecosistemas digitales integrados.
- Manufactura tecnológica.
- Datos masivos.

Lee (2018) sostiene que China posee ventajas significativas derivadas de su enorme volumen de usuarios digitales y de su ecosistema de datos, factores fundamentales para el entrenamiento de modelos de IA a gran escala.

2.1.5. Las infraestructuras invisibles del poder

La geopolítica inteligente pone en evidencia que gran parte de la infraestructura estratégica contemporánea permanece oculta para la mayoría de los ciudadanos.

Entre estas infraestructuras destacan:

- Centros de datos.
- Cables submarinos.
- Redes satelitales.
- Sistemas cloud.
- Estaciones terrestres.
- Redes de sensores.

Starosielski (2015) demuestra que aproximadamente el 95 % de las comunicaciones intercontinentales dependen de cables submarinos, convirtiéndolos en puntos críticos para la seguridad global.

La infraestructura digital se transforma así en un componente esencial de la soberanía tecnológica y de la resiliencia nacional.

2.1.6. La inteligencia geopolítica basada en datos

Uno de los principales cambios introducidos por la revolución digital es la posibilidad de integrar cantidades masivas de información en tiempo real para apoyar procesos de decisión estratégica.

La denominada inteligencia geoespacial combina:

- Imágenes satelitales.
- Sensores remotos.
- Datos de telecomunicaciones.
- Inteligencia artificial.
- Aprendizaje automático.

Según Kello (2017), estas tecnologías están modificando tanto los procesos de seguridad nacional como las capacidades de vigilancia económica y militar de los Estados.

El análisis algorítmico permite identificar:

- Patrones de movilidad.
- Despliegues militares.
- Interrupciones logísticas.
- Flujos comerciales.
- Riesgos geopolíticos.

Nunca antes los responsables políticos habían tenido acceso a tal volumen de información estratégica.

2.1.7. Implicaciones para las Relaciones Internacionales 6.0

La geopolítica inteligente representa una evolución de los paradigmas geopolíticos tradicionales. La competencia internacional ya no puede analizarse únicamente desde el control territorial o militar, sino que requiere incorporar capacidades digitales como variables fundamentales de poder.

Desde la perspectiva de las Relaciones Internacionales 6.0, la ventaja estratégica depende de la interacción entre:

$$GI = T + Tec + Inf$$

Donde:

- T = Recursos territoriales
- Tec = Capacidades tecnológicas
- Inf = Capacidad informacional

Esta integración configura nuevas formas de influencia internacional que redefinen la competencia geopolítica del siglo XXI.

2.2 Inteligencia artificial y capacidades estatales para la toma de decisiones estratégicas

La inteligencia artificial (IA) se ha convertido en uno de los principales factores de transformación del poder estatal en el siglo XXI. Si la Revolución Industrial amplió la capacidad de producción y la era nuclear modificó los equilibrios de seguridad global, la inteligencia artificial está redefiniendo la capacidad de los Estados para analizar información, anticipar riesgos, formular políticas públicas y proyectar influencia internacional. En consecuencia, la IA ha dejado de ser una herramienta exclusivamente tecnológica para convertirse en un componente esencial de la capacidad estratégica nacional (Schwab, 2016; Lee, 2018).

La creciente disponibilidad de datos masivos, el aumento exponencial de la capacidad de cómputo y los avances en aprendizaje automático están permitiendo a los gobiernos procesar volúmenes de información que serían imposibles de analizar mediante métodos tradicionales. Esta transformación está modificando la manera en que se desarrollan actividades fundamentales como la inteligencia estratégica, la seguridad nacional, la planificación económica, la gestión de crisis y la diplomacia internacional (Russell & Norvig, 2021).

Desde la perspectiva de las Relaciones Internacionales 6.0, la inteligencia artificial constituye un multiplicador de poder que incrementa la capacidad de los Estados para comprender entornos complejos, reducir incertidumbres y tomar decisiones en escenarios caracterizados por altos niveles de volatilidad e interdependencia tecnológica.

2.2.1. La inteligencia artificial como recurso estratégico de poder

La inteligencia artificial puede definirse como el conjunto de técnicas computacionales que permiten a las máquinas realizar tareas asociadas tradicionalmente a la inteligencia humana, incluyendo aprendizaje, reconocimiento de patrones, procesamiento del lenguaje natural, razonamiento y toma de decisiones (Russell & Norvig, 2021).

Más allá de su dimensión tecnológica, la IA representa una capacidad estratégica debido a que mejora significativamente los procesos de recopilación, procesamiento e interpretación de información. Como señala Kissinger, Schmidt y Huttenlocher (2021), las tecnologías de inteligencia artificial están transformando las bases cognitivas sobre las cuales se construyen las decisiones políticas y estratégicas.

Figura 2.1

La IA como multiplicador estratégico



Fuente: Elaboración autores

En consecuencia, los países que lideran el desarrollo de inteligencia artificial no solo adquieren ventajas económicas, sino también capacidades geopolíticas y militares superiores.

2.2.2. Transformación de la toma de decisiones estatales

Tradicionalmente, la toma de decisiones gubernamentales dependió de estructuras burocráticas encargadas de recopilar información, elaborar informes y asesorar a los responsables políticos. Sin embargo, la velocidad de los procesos contemporáneos ha superado la capacidad humana para procesar grandes cantidades de información en tiempo real.

La inteligencia artificial permite automatizar parcialmente estos procesos mediante:

- Identificación de tendencias.
- Detección temprana de riesgos.
- Simulación de escenarios.
- Evaluación de políticas públicas.
- Modelización predictiva.

Según Davenport y Miller (2022), los sistemas de IA pueden analizar millones de datos en cuestión de segundos, proporcionando información estratégica para apoyar la toma de decisiones complejas.

Tabla 2.2

Funciones de la IA en la gestión estatal

Función	Aplicación gubernamental
Análisis predictivo	Anticipación de riesgos
Procesamiento masivo de datos	Inteligencia estratégica
Modelación de escenarios	Planificación nacional
Automatización	Gestión pública
Reconocimiento de patrones	Seguridad y defensa

Fuente: Elaboración autores

Esta transformación no implica sustituir completamente a los responsables políticos, sino aumentar sus capacidades analíticas mediante sistemas avanzados de asistencia inteligente.

2.2.3. Inteligencia artificial e inteligencia estratégica

La inteligencia estratégica constituye uno de los ámbitos donde la inteligencia artificial está generando mayores impactos.

Tradicionalmente, los organismos de inteligencia procesaban información proveniente de fuentes humanas, imágenes satelitales, comunicaciones y documentos oficiales. Según Clark (2020), actualmente más del 90 % de los datos mundiales han sido generados durante las últimas décadas, lo que exige nuevas herramientas para su procesamiento.

La IA permite:

- Analizar imágenes satelitales automáticamente.
- Detectar movimientos militares.
- Identificar anomalías económicas.
- Monitorear amenazas cibernéticas.
- Procesar redes sociales en tiempo real.

2.2.4. Estados Unidos y la estrategia de liderazgo en inteligencia artificial

Estados Unidos continúa siendo uno de los líderes mundiales en inteligencia artificial gracias a la combinación de universidades de excelencia, empresas tecnológicas innovadoras y una sólida capacidad de investigación y desarrollo.

Organizaciones como:

- OpenAI
- Microsoft
- Google DeepMind
- NVIDIA
- Anthropic

han situado al país en posiciones de liderazgo tecnológico global (Lee, 2018; Miller, 2022).

El Departamento de Defensa estadounidense ha incorporado la IA en programas relacionados con:

- Inteligencia geoespacial.
- Ciberseguridad.
- Sistemas autónomos.
- Logística militar.
- Análisis de amenazas.

La Estrategia Nacional de Inteligencia Artificial de Estados Unidos considera la IA un recurso crítico para preservar la seguridad nacional y la competitividad económica durante las próximas décadas (National Security Commission on Artificial Intelligence [NSCAI], 2021).

Caso de estudio: Proyecto Maven

El Proyecto Maven utiliza algoritmos de aprendizaje automático para analizar imágenes captadas por drones militares, identificando objetivos potenciales con mayor rapidez que los sistemas convencionales (Scharre, 2018).

Este caso ilustra cómo la IA modifica la relación entre información, velocidad y ventaja estratégica.

2.2.5. China y la construcción de una potencia algorítmica

China ha desarrollado una estrategia nacional orientada a convertirse en líder mundial en inteligencia artificial.

El plan **Next Generation Artificial Intelligence Development Plan**, publicado por el Consejo de Estado chino, establece objetivos de liderazgo tecnológico para mediados del siglo XXI (State Council of China, 2017).

Las fortalezas chinas incluyen:

- Gran volumen de datos.
- Amplio mercado digital.
- Inversión pública sostenida.
- Integración entre Estado y empresas tecnológicas.
- Ecosistemas de innovación emergentes.

Lee (2018) sostiene que el principal activo de China es su extraordinaria disponibilidad de datos, condición fundamental para entrenar modelos avanzados de inteligencia artificial.

Tabla 2.3

Factores comparativos Estados Unidos–China en IA

Variable	Estados Unidos	China
Universidades líderes	Muy alta	Alta
Datos disponibles	Alta	Muy alta
Inversión privada	Muy alta	Alta
Apoyo estatal	Alta	Muy alta
Ecosistema empresarial	Muy alta	Alta

Fuente: Elaboración autores

La competencia tecnológica entre ambas potencias constituye uno de los factores geopolíticos más relevantes del sistema internacional contemporáneo.

2.2.6. Inteligencia artificial y seguridad nacional

La relación entre inteligencia artificial y seguridad nacional constituye uno de los temas más debatidos de la actualidad.

Según Scharre (2018), la IA está transformando múltiples dimensiones de la defensa:

Vigilancia

Procesamiento masivo de imágenes y señales.

Guerra electrónica

Identificación automática de amenazas.

Ciberseguridad

Detección de ataques en tiempo real.

Logística militar

Optimización de operaciones complejas.

Sistemas autónomos

Apoyo a operaciones militares avanzadas.

2.2.7. Limitaciones de la inteligencia artificial en la toma de decisiones

A pesar de sus ventajas, la inteligencia artificial presenta importantes limitaciones que deben ser consideradas en el ámbito estratégico.

Sesgos algorítmicos

Los sistemas de IA reflejan los datos utilizados durante su entrenamiento.

Opacidad

Muchos modelos funcionan como "cajas negras", dificultando la comprensión de sus resultados (Floridi, 2019).

Dependencia de datos

La calidad de las decisiones depende de la calidad de la información disponible.

Incertidumbre estratégica

La complejidad del comportamiento humano limita la capacidad predictiva de los algoritmos.

Tabla 2.4

Fortalezas y limitaciones de la IA estratégica

Fortalezas	Limitaciones
Procesamiento masivo	Sesgos
Velocidad analítica	Opacidad
Capacidad predictiva	Dependencia de datos
Automatización	Riesgo de errores
Integración de información	Incertidumbre humana

Fuente: Elaboración autores

En consecuencia, la mayoría de especialistas coinciden en que la IA debe complementar y no sustituir completamente el juicio humano.

2.2.8. Hacia una capacidad estatal aumentada por inteligencia artificial

Las Relaciones Internacionales 6.0 proponen interpretar la inteligencia artificial como una capacidad transversal que fortalece múltiples dimensiones del poder estatal.

Modelo conceptual

$$CE = IA + D + C + I$$

Donde:

- CE = Capacidad Estratégica Estatal
- IA = Inteligencia Artificial
- D = Datos
- C = Capacidad de cómputo
- I = Inteligencia institucional

2.3 2.3. Datos, capacidad de cómputo y talento especializado como recursos de poder

La distribución del poder internacional ha estado históricamente vinculada al control de recursos estratégicos. Durante la era industrial, la posesión de carbón, acero, petróleo y

capacidad manufacturera determinó el ascenso y la consolidación de las grandes potencias. En el siglo XXI, sin embargo, la economía digital ha modificado significativamente esta ecuación. Los datos, la capacidad de cómputo y el talento altamente especializado han emergido como factores decisivos para la innovación tecnológica, la competitividad económica, la seguridad nacional y la influencia geopolítica (Castells, 2010; Brynjolfsson & McAfee, 2014).

La inteligencia artificial contemporánea depende fundamentalmente de la interacción de tres variables estratégicas: grandes volúmenes de datos para entrenar modelos, infraestructura computacional capaz de procesarlos y capital humano altamente cualificado para diseñar, implementar y optimizar algoritmos complejos (Lee, 2018; Russell & Norvig, 2021). La combinación de estos elementos configura una nueva estructura de poder internacional donde la ventaja competitiva no se encuentra únicamente en la posesión de recursos materiales tradicionales, sino en la capacidad para generar conocimiento e innovación tecnológica.

Desde la perspectiva de las Relaciones Internacionales 6.0, estos tres componentes constituyen los pilares del denominado **poder computacional**, entendido como la capacidad de transformar información en inteligencia estratégica, innovación económica y ventaja geopolítica.

2.3.1. Los datos como recurso estratégico del siglo XXI

En las últimas dos décadas, diversos autores han señalado que los datos representan el recurso económico más importante de la economía digital. The Economist (2017) llegó incluso a afirmar que los datos constituyen "el nuevo petróleo", debido a su creciente relevancia para la generación de valor económico.

Sin embargo, esta analogía posee limitaciones importantes. A diferencia del petróleo, los datos:

- Son reproducibles.
- No se agotan con su uso.
- Pueden utilizarse simultáneamente por múltiples actores.
- Incrementan su valor cuando se combinan con otros conjuntos de información.
- Adquieren utilidad mediante procesamiento algorítmico.

Mayer-Schönberger y Cukier (2013) sostienen que la verdadera revolución del Big Data no consiste únicamente en la acumulación masiva de información, sino en la capacidad para identificar patrones, correlaciones y tendencias previamente invisibles.

2.3.2. Big Data y ventaja competitiva internacional

El concepto de Big Data hace referencia a conjuntos de datos caracterizados por su gran volumen, velocidad de generación, variedad de formatos y complejidad analítica (Kitchin, 2021).

Tradicionalmente se identifican cinco características fundamentales:

- **Volumen.** Cantidad masiva de información disponible.
- **Velocidad.** Generación continua y acelerada de datos.
- **Variedad.** Diversidad de formatos estructurados y no estructurados.
- **Veracidad.** Calidad y confiabilidad de la información.
- **Valor.** Capacidad para producir conocimiento útil.

Tabla 2.5

Características estratégicas del Big Data

Característica	Implicación geopolítica
Volumen	Mayor capacidad predictiva
Velocidad	Respuesta rápida
Variedad	Visión multidimensional
Veracidad	Mayor precisión analítica
Valor	Ventaja estratégica

Fuente: Elaboración autores

Los gobiernos y empresas que poseen acceso a grandes volúmenes de datos pueden desarrollar algoritmos más precisos, sistemas predictivos más eficientes y capacidades de inteligencia superiores, generando ventajas competitivas difíciles de replicar (Zuboff, 2019).

2.3.3. Economía de los datos y concentración del poder digital

La economía digital contemporánea presenta fuertes tendencias hacia la concentración. Las principales plataformas tecnológicas globales han construido modelos de negocio basados en la captura, almacenamiento y procesamiento de datos generados por miles de millones de usuarios.

Autores como Srnicek (2017) denominan este fenómeno capitalismo de plataformas, mientras que Zuboff (2019) lo describe como capitalismo de vigilancia, enfatizando la importancia económica de la información personal en la generación de beneficios corporativos.

Las empresas con mayor capacidad de recopilación de datos poseen ventajas significativas para:

- Entrenar modelos de inteligencia artificial.
- Personalizar servicios.
- Generar publicidad dirigida.
- Incrementar productividad.
- Consolidar posiciones dominantes de mercado.

Figura 2.2

Relación entre datos y poder económico



Fuente: Elaboración autores

Este ciclo genera importantes barreras de entrada para nuevos competidores y fortalece la concentración de capacidades digitales en un reducido número de actores.

2.3.4. La capacidad de cómputo como infraestructura estratégica

Los datos, por sí solos, poseen un valor limitado. Para transformarlos en conocimiento útil es necesario contar con capacidades computacionales suficientes para almacenarlos, procesarlos y analizarlos.

La capacidad de cómputo incluye:

- Supercomputadoras.
- Centros de datos.
- Procesadores especializados.
- Infraestructura cloud.
- Chips avanzados para inteligencia artificial.

Amodei y Hernández (2018) demostraron que los requerimientos computacionales de los sistemas de inteligencia artificial más avanzados están creciendo a ritmos extraordinarios, convirtiendo el acceso a recursos computacionales en un factor crítico de competitividad tecnológica.

Figura 2.3

Componentes de la capacidad de cómputo



Fuente: Elaboración autores

En consecuencia, la infraestructura computacional se ha convertido en un activo estratégico comparable a las redes energéticas o los sistemas de transporte de épocas anteriores.

2.3.5. Supercomputación y competencia geopolítica

La posesión de sistemas de supercomputación representa actualmente una ventaja significativa en términos científicos, económicos y militares.

Las supercomputadoras permiten:

- Simular fenómenos complejos.
- Desarrollar nuevos materiales.
- Entrenar modelos avanzados de IA.
- Mejorar sistemas de defensa.
- Modelizar procesos climáticos.

Estados Unidos, China, Japón y la Unión Europea han invertido cantidades significativas de recursos en el desarrollo de capacidades de computación de alto rendimiento (HPC, por sus siglas en inglés).

Tabla 2.6

Aplicaciones estratégicas de la supercomputación

Sector	Aplicación
Defensa	Simulación militar
Medicina	Investigación biomédica
Energía	Modelación compleja
IA	Entrenamiento de modelos
Clima	Pronósticos avanzados

Fuente: Elaboración autores

La competencia por el liderazgo en supercomputación refleja una lucha más amplia por el dominio tecnológico global.

2.3.6. La nube como nueva infraestructura del poder

La computación en la nube ha transformado profundamente la arquitectura digital mundial.

Según Armbrust et al. (2010), los servicios cloud permiten acceder a recursos computacionales de manera flexible, escalable y eficiente.

Actualmente, gran parte de la infraestructura digital global depende de proveedores especializados como:

- Microsoft Azure.
- Amazon Web Services (AWS).
- Google Cloud.
- Alibaba Cloud.

Esta realidad plantea interrogantes sobre soberanía digital y dependencia tecnológica, especialmente para países que carecen de infraestructura propia de gran escala.

2.3.7. Talento especializado: el recurso más escaso

Aunque los datos y la capacidad computacional son fundamentales, el verdadero motor de la innovación digital continúa siendo el capital humano.

Florida (2014) sostiene que la economía global contemporánea depende crecientemente de la denominada "clase creativa", integrada por científicos, ingenieros, investigadores y profesionales altamente especializados.

En el ámbito de la inteligencia artificial, el talento incluye:

- Científicos de datos.
- Ingenieros de aprendizaje automático.
- Matemáticos.
- Especialistas en computación avanzada.
- Investigadores en IA.

La disponibilidad de este talento se ha convertido en un componente crítico de la competitividad nacional.

2.3.8. La guerra global por el talento tecnológico

Numerosas potencias han desarrollado estrategias específicas para atraer y retener profesionales altamente cualificados.

Esta competencia internacional involucra:

- Universidades de excelencia.
- Centros de investigación.
- Incentivos migratorios.
- Programas de becas.
- Financiamiento científico.

Lee (2018) argumenta que el acceso al talento será uno de los factores más importantes para determinar qué países liderarán la próxima generación de innovaciones digitales.

La ausencia de cualquiera de estos tres componentes limita significativamente la capacidad tecnológica de un país.

2.3.9. Datos, cómputo y talento como nueva estructura del poder internacional

Las Relaciones Internacionales 6.0 proponen interpretar estos tres elementos como componentes fundamentales de una nueva arquitectura de poder.

Modelo conceptual

$$PD = D + CC + T$$

Donde:

- **PD** = Poder Digital
- **D** = Datos
- **CC** = Capacidad de Cómputo
- **T** = Talento Especializado

Asimismo:

$$IA = f(D, C, CT)$$

Esto implica que el desarrollo de inteligencia artificial depende directamente de la interacción entre estas tres variables estratégicas.

2.4 Semiconductores, centros de datos y servicios en la nube: dependencias y vulnerabilidades estratégicas

Los semiconductores, los centros de datos y los servicios de computación en la nube constituyen infraestructuras esenciales para el funcionamiento de la economía digital y para el ejercicio del poder en el sistema internacional. Su importancia trasciende el ámbito comercial, pues intervienen en las telecomunicaciones, la inteligencia artificial, los sistemas financieros, la industria de defensa, la automatización industrial y la administración pública. Por ello, el control de estas tecnologías se ha convertido en un componente estratégico de la competencia entre las principales potencias.

Los semiconductores son componentes fundamentales de dispositivos electrónicos y sistemas computacionales. Su producción requiere conocimientos especializados, inversiones elevadas, equipos de fabricación avanzados y cadenas internacionales de suministro altamente interdependientes. La fabricación de los chips más sofisticados se concentra en un número limitado de empresas y territorios, lo que genera vulnerabilidades ante conflictos comerciales, restricciones de exportación, interrupciones logísticas o tensiones militares. Miller (2022) explica que la industria de los semiconductores se caracteriza por una compleja división internacional del trabajo, en la que el diseño, la fabricación, los equipos especializados y los materiales dependen de capacidades distribuidas entre diferentes economías.

Esta estructura convierte a los semiconductores en instrumentos de influencia geopolítica. Las restricciones impuestas por Estados Unidos a determinadas exportaciones de tecnologías avanzadas hacia China ilustran cómo los controles tecnológicos pueden utilizarse para limitar el acceso a capacidades consideradas estratégicas. Estas medidas no solo afectan a las empresas directamente involucradas, sino que también repercuten en proveedores, fabricantes y países que participan en las cadenas globales de valor.

La vulnerabilidad de esta industria se relaciona, además, con su concentración geográfica. Una interrupción importante en los principales centros de fabricación podría afectar la producción de automóviles, equipos médicos, dispositivos electrónicos y sistemas de telecomunicaciones. Por tanto, la seguridad del suministro depende tanto de la capacidad industrial como de la diversificación de proveedores y de la cooperación internacional.

Los centros de datos cumplen una función complementaria. En ellos se concentran servidores, sistemas de almacenamiento y equipos de procesamiento que permiten gestionar grandes volúmenes de información. Su funcionamiento requiere electricidad, refrigeración, conectividad de alta capacidad y mecanismos de seguridad física y digital. La expansión de la inteligencia artificial ha incrementado la importancia de estas instalaciones, especialmente aquellas capaces de soportar cargas de trabajo computacional intensivas.

Por su parte, los servicios en la nube permiten utilizar recursos informáticos sin que las organizaciones deban adquirir y mantener toda la infraestructura necesaria. Esta modalidad reduce determinadas barreras de entrada y facilita la innovación; sin embargo,

también puede generar dependencia de proveedores que controlan plataformas, herramientas y servicios difíciles de sustituir. La concentración empresarial puede limitar la capacidad de negociación de los clientes y aumentar los riesgos asociados con interrupciones, cambios contractuales o restricciones jurisdiccionales.

Desde una perspectiva geopolítica, la soberanía tecnológica no exige que cada país produzca todos sus semiconductores o disponga de una infraestructura digital completamente autónoma. Requiere identificar las dependencias críticas, desarrollar alternativas viables y asegurar que las tecnologías esenciales puedan mantenerse operativas en situaciones de crisis. La diversificación de proveedores, la interoperabilidad y la formación de especialistas son, en este sentido, componentes de una política de resiliencia.

2.5 Cables submarinos, satélites y redes de telecomunicaciones en la disputa por la conectividad

La conectividad constituye una infraestructura esencial del poder contemporáneo, porque permite la circulación de información, capitales, conocimientos y comunicaciones estratégicas. Los cables submarinos, los satélites y las redes terrestres conforman una arquitectura interdependiente que sostiene el comercio digital, los servicios financieros, las operaciones gubernamentales y la cooperación internacional. En consecuencia, el control, la protección y la disponibilidad de estas infraestructuras han adquirido una creciente relevancia geopolítica.

Los cables submarinos de fibra óptica transportan más del 99 % del tráfico internacional de datos, según la Unión Internacional de Telecomunicaciones (UIT, s. f.). Su importancia radica en la capacidad de transmitir grandes volúmenes de información entre continentes con elevada velocidad y eficiencia. Sin embargo, su distribución geográfica es desigual y su funcionamiento puede verse afectado por terremotos, deslizamientos submarinos, actividades pesqueras, anclas y posibles acciones deliberadas contra infraestructuras críticas.

Desde una perspectiva estratégica, estas vulnerabilidades adquieren importancia porque una interrupción puede afectar simultáneamente múltiples servicios. La conectividad de un país depende no solo de la cantidad de cables disponibles, sino también de la existencia

de rutas alternativas, puntos de conexión diversificados y mecanismos de reparación oportunos. Cuando un territorio depende de pocos enlaces internacionales, una avería puede incrementar los costos de comunicación y reducir temporalmente la disponibilidad de determinados servicios digitales.

La competencia geopolítica también se manifiesta en la construcción, propiedad y gestión de estas infraestructuras. Las inversiones en cables submarinos pueden ampliar la conectividad, facilitar el comercio y atraer actividades tecnológicas, pero también generan relaciones de dependencia respecto de operadores, financiadores y proveedores especializados. Runde et al. (2024) destacan que los cables submarinos han adquirido una importancia creciente en la competencia entre grandes potencias, debido a su función en la transmisión de datos comerciales, financieros y gubernamentales.

Los satélites complementan esta infraestructura al proporcionar comunicaciones en zonas remotas, marítimas y rurales, así como servicios de navegación, observación terrestre y respuesta ante emergencias. Su utilidad estratégica se manifiesta especialmente cuando las redes terrestres son insuficientes o quedan interrumpidas. No obstante, los sistemas satelitales también presentan vulnerabilidades relacionadas con interferencias, ciberataques, congestión orbital y dependencia de operadores específicos.

La expansión de las constelaciones de satélites de órbita baja ha incrementado las posibilidades de ofrecer internet en zonas de difícil acceso. Sin embargo, la capacidad efectiva de estos servicios depende de la cobertura, el costo, los terminales disponibles y las condiciones regulatorias. Por tanto, no sustituyen universalmente a los cables de fibra óptica, sino que cumplen funciones complementarias.

Las redes móviles y terrestres, incluidas las tecnologías 5G y las futuras generaciones de telecomunicaciones, completan esta arquitectura. Su despliegue está relacionado con la competencia industrial, los estándares técnicos y la seguridad de los equipos utilizados. Las decisiones de los gobiernos sobre proveedores, certificaciones y requisitos de seguridad pueden responder a consideraciones económicas, pero también a preocupaciones sobre espionaje, continuidad operativa y autonomía tecnológica.

En este contexto, la conectividad se convierte en un espacio de competencia por la influencia internacional. Los Estados buscan atraer inversiones, proteger sus

infraestructuras y evitar dependencias excesivas, mientras que las empresas compiten por establecer redes, ofrecer servicios y consolidar posiciones en mercados estratégicos.

Para Ecuador y América Latina, el desafío consiste en fortalecer la resiliencia de las comunicaciones internacionales mediante la diversificación de rutas, la cooperación regional, la protección de infraestructuras críticas y la ampliación del acceso en territorios rurales. La conectividad debe entenderse como un componente de la seguridad económica y del desarrollo, no únicamente como un servicio comercial.

En síntesis, los cables submarinos, los satélites y las redes de telecomunicaciones constituyen una infraestructura material del poder digital. La capacidad de mantenerlos operativos, diversificar sus conexiones y garantizar un acceso confiable influye directamente en la autonomía tecnológica y en la participación de los países en la economía mundial.

2.6 Minerales críticos, energía y condiciones materiales de la transformación digital

La transformación digital suele asociarse con información, software e inteligencia artificial, pero su funcionamiento depende de una base material compuesta por minerales, energía, agua e infraestructura industrial. Los dispositivos electrónicos, los semiconductores, las baterías, los centros de datos y los sistemas de telecomunicaciones requieren recursos naturales cuya extracción y procesamiento están distribuidos de manera desigual entre países.

Los minerales críticos son aquellos cuya disponibilidad resulta estratégica para determinadas actividades económicas y tecnológicas y cuya cadena de suministro presenta riesgos relevantes. Su importancia varía según la tecnología considerada y puede cambiar con las innovaciones, la aparición de sustitutos y las transformaciones de los mercados. Entre los materiales relevantes para distintas aplicaciones digitales y energéticas se encuentran el cobre, el litio, el níquel, el cobalto, el grafito, el galio y las tierras raras.

La Agencia Internacional de la Energía (AIE, 2025) advierte que la concentración de la extracción y, especialmente, del procesamiento de determinados minerales puede generar vulnerabilidades frente a restricciones comerciales, interrupciones productivas y tensiones geopolíticas. Su análisis también destaca que la expansión de tecnologías

digitales y energéticas incrementa la importancia estratégica de las cadenas de suministro de materiales especializados.

La dependencia de estos recursos introduce una dimensión geopolítica en la transición digital. Los países productores pueden adquirir influencia por su capacidad para suministrar materiales esenciales, mientras que las economías importadoras buscan diversificar proveedores, desarrollar procesos de reciclaje y promover inversiones en nuevas fuentes de abastecimiento. Sin embargo, disponer de reservas minerales no garantiza automáticamente un mayor desarrollo industrial. La distribución de los beneficios depende de la capacidad de procesamiento, la tecnología disponible, la formación profesional, las condiciones contractuales y las políticas públicas.

La energía constituye otra condición material fundamental. Los centros de datos y las instalaciones que procesan grandes volúmenes de información requieren electricidad continua, sistemas de refrigeración y redes de transmisión confiables. La expansión de la inteligencia artificial puede incrementar estas necesidades, aunque el consumo efectivo depende de la eficiencia de los equipos, la arquitectura de los sistemas y las fuentes energéticas utilizadas.

Esta situación vincula la geopolítica digital con la seguridad energética. Los países que disponen de electricidad competitiva, infraestructura estable y fuentes diversificadas pueden presentar ventajas para atraer inversiones tecnológicas. Por el contrario, las limitaciones de generación y transmisión pueden elevar los costos operativos y restringir la expansión de servicios digitales intensivos en computación.

La dimensión ambiental también resulta decisiva. La extracción de minerales puede generar impactos sobre ecosistemas, disponibilidad de agua y medios de vida locales. A su vez, los equipos electrónicos requieren procesos de fabricación y generan residuos al finalizar su vida útil. La UNCTAD (2024) subraya que una economía digital sostenible debe considerar los impactos ambientales a lo largo del ciclo de vida de los productos, desde la extracción de materias primas hasta la reutilización y el reciclaje.

Para América Latina, esta situación representa tanto una oportunidad como un desafío. La disponibilidad de recursos minerales y energéticos puede favorecer la participación en las cadenas globales de suministro, pero existe el riesgo de mantener una especialización

concentrada en la exportación de materias primas, mientras las actividades de mayor valor agregado se desarrollan en otras economías.

En Ecuador, una estrategia de desarrollo tecnológico vinculada con los recursos naturales debería combinar la gestión ambiental, la investigación científica, la formación de especialistas y el fortalecimiento de las capacidades industriales. La evaluación de proyectos extractivos debe considerar no solo su rentabilidad, sino también sus efectos territoriales, el uso del agua, la conservación de la biodiversidad y la distribución de los beneficios económicos.

La transición digital, por tanto, no es inmaterial ni ambientalmente neutra. Su sostenibilidad depende de cómo se obtienen los recursos, cómo se produce la energía y cómo se distribuyen los costos y beneficios de las cadenas de suministro. La autonomía estratégica requiere no solo acceso a tecnologías, sino también capacidad para gestionar de manera sostenible las condiciones materiales que las hacen posibles.

2.7 Inteligencia estratégica y anticipación de conflictos: utilidad, incertidumbre y límites de los modelos predictivos

La inteligencia estratégica constituye un proceso sistemático de recopilación, evaluación e interpretación de información para apoyar decisiones relacionadas con la seguridad, la política exterior y la gestión de riesgos. En un entorno internacional caracterizado por la competencia tecnológica, las crisis económicas y la incertidumbre geopolítica, anticipar posibles conflictos permite identificar señales de alerta, evaluar escenarios y preparar respuestas institucionales.

La transformación digital ha ampliado las fuentes de información disponibles para este propósito. Los datos satelitales, los indicadores económicos, las comunicaciones públicas, las noticias, los registros comerciales y las bases de datos sobre violencia política pueden utilizarse para identificar patrones asociados con situaciones de inestabilidad. Las técnicas estadísticas y los algoritmos de aprendizaje automático permiten procesar grandes volúmenes de información y estimar probabilidades de determinados acontecimientos.

No obstante, es necesario distinguir entre inteligencia estratégica, análisis de riesgos y predicción. La inteligencia estratégica integra información y juicio especializado para

apoyar decisiones; el análisis de riesgos identifica amenazas, vulnerabilidades y consecuencias potenciales; los modelos predictivos estiman la probabilidad de resultados a partir de datos y supuestos específicos. Estas actividades se complementan, pero ninguna garantiza que los acontecimientos futuros puedan conocerse con certeza.

Rød et al. (2024), en su revisión de sistemas de alerta temprana de conflictos, identifican diferencias entre modelos en cuanto a transparencia, accesibilidad de los datos, parámetros y resultados de las predicciones. Los autores destacan la importancia de mejorar la transparencia y la cooperación entre sistemas para fortalecer la evaluación de riesgos y la prevención de la violencia.

Una aplicación relevante de estos métodos consiste en identificar condiciones que históricamente han estado asociadas con el aumento de la violencia. Entre ellas pueden encontrarse la intensificación de enfrentamientos previos, la inestabilidad política, las protestas, las dificultades económicas y determinadas tensiones territoriales. Sin embargo, la presencia de estos factores no implica necesariamente que se produzca un conflicto: su influencia depende del contexto y de la interacción con otras variables.

Los modelos predictivos pueden aportar valor al detectar cambios que resultarían difíciles de identificar mediante la revisión manual de grandes conjuntos de datos. También permiten comparar escenarios y actualizar estimaciones a medida que se incorpora nueva información. Su utilidad aumenta cuando las predicciones se acompañan de indicadores comprensibles, evaluación estadística y procedimientos claros para revisar los resultados.

Sin embargo, existen límites importantes. En primer lugar, los datos históricos pueden ser incompletos, inconsistentes o poco representativos. En segundo lugar, los conflictos son procesos dinámicos en los que intervienen decisiones políticas, percepciones, estrategias y acontecimientos inesperados. En tercer lugar, las relaciones identificadas en los datos no demuestran necesariamente causalidad. Un modelo puede reconocer patrones asociados con la violencia sin explicar de manera suficiente los mecanismos que la originan.

Chadefaux (2017) distingue entre explicar un fenómeno y predecirlo: una teoría puede contribuir a comprender las causas de un conflicto sin ofrecer predicciones precisas sobre su momento de aparición, mientras que un modelo predictivo puede identificar patrones

útiles sin proporcionar una explicación causal completa. Esta diferencia es esencial para evitar que las estimaciones algorítmicas se interpreten como certezas.

Otro problema es la falsa precisión. Una probabilidad calculada con numerosos decimales no es necesariamente más confiable que una estimación expresada de manera sencilla. La calidad de una predicción depende de los datos, de los supuestos, de la validación y de su capacidad para funcionar en contextos diferentes de aquellos utilizados para entrenar el modelo.

Además, los modelos pueden reproducir sesgos presentes en las fuentes de información. Si determinados territorios están mejor documentados que otros, las estimaciones pueden ser menos confiables en regiones con registros limitados. La automatización también puede generar errores cuando se interpretan noticias, publicaciones digitales o indicadores sociales sin considerar sus contextos políticos y culturales.

La anticipación de conflictos exige, por tanto, combinar métodos cuantitativos con conocimiento histórico, análisis cualitativo y evaluación experta. Los sistemas de alerta temprana deben comunicar tanto los riesgos identificados como los niveles de incertidumbre, evitando que una estimación estadística se convierta automáticamente en una decisión política o de seguridad.

Desde la perspectiva de las Relaciones Internacionales 6.0, la inteligencia estratégica representa una herramienta para mejorar la preparación institucional, no un mecanismo infalible para controlar el futuro. Su aplicación responsable requiere transparencia metodológica, protección de la información, supervisión humana y evaluación continua de los errores.

Para Ecuador y América Latina, estas herramientas pueden contribuir a analizar riesgos de conflictividad social, tensiones fronterizas, interrupciones de infraestructuras críticas y amenazas asociadas con eventos climáticos. Sin embargo, deben utilizarse respetando los derechos fundamentales y evitando que las correlaciones estadísticas se conviertan en mecanismos de estigmatización de comunidades o grupos sociales.

EDITORIAL ANDES COGNITIO

CAPÍTULO III

TRANSFORMACIÓN DEL PODER Y GEOECONOMÍA EN LA ERA DIGITAL



CAPÍTULO III

TRANSFORMACIÓN DEL PODER Y GEOECONOMÍA EN LA ERA DIGITAL

3.1 Poder estructural y capacidad de influencia en la economía digital internacional

La transformación digital ha modificado las bases tradicionales del poder en las relaciones internacionales. Si durante buena parte del siglo XX la influencia de los Estados se vinculaba principalmente con su capacidad militar, territorial, industrial y financiera, en el siglo XXI adquieren creciente relevancia el control de los datos, las infraestructuras digitales, los semiconductores, los sistemas de inteligencia artificial y las redes de comunicación. En este contexto, el poder no consiste únicamente en imponer decisiones de manera directa, sino también en configurar las condiciones bajo las cuales otros actores pueden participar en la economía global.

Susan Strange (1988) definió el poder estructural como la capacidad de configurar las estructuras dentro de las cuales operan los Estados, las empresas y otros actores internacionales. Esta perspectiva resulta especialmente útil para comprender la economía digital, puesto que determinados países y corporaciones pueden influir en las reglas de acceso a tecnologías, mercados, información y recursos estratégicos. Quien controla infraestructuras fundamentales o establece estándares tecnológicos dispone de ventajas que trascienden las relaciones comerciales convencionales.

Por ejemplo, los países que concentran capacidades avanzadas de diseño de semiconductores, fabricación de chips, computación en la nube y desarrollo de inteligencia artificial pueden condicionar las posibilidades tecnológicas de otros Estados. Estas ventajas generan relaciones de interdependencia asimétrica: aunque varios países participan en una misma cadena de producción, no todos poseen la misma capacidad para sustituir proveedores, desarrollar alternativas o resistir una interrupción del suministro. Farrell y Newman (2019) explican que las redes económicas internacionales pueden convertirse en instrumentos de coerción cuando determinados actores ocupan posiciones centrales desde las cuales pueden observar, restringir o interrumpir flujos de información y recursos.

La influencia digital también se manifiesta mediante la definición de estándares técnicos, protocolos de interoperabilidad, normas de ciberseguridad y condiciones de acceso a los mercados. Las decisiones sobre qué tecnologías se adoptan, qué sistemas son compatibles y qué requisitos deben cumplir los proveedores pueden favorecer a determinados actores y elevar los costos de entrada para sus competidores. Por tanto, el poder estructural no se limita a la propiedad de los recursos tecnológicos, sino que comprende la capacidad de establecer las reglas que organizan su utilización.

En el plano geopolítico, Estados Unidos, China y la Unión Europea representan modelos diferentes, aunque parcialmente superpuestos, de influencia digital. Estados Unidos mantiene una posición relevante en servicios digitales, plataformas, computación en la nube y diseño de tecnologías avanzadas; China ha fortalecido sus capacidades industriales y tecnológicas, así como su presencia en mercados internacionales; mientras que la Unión Europea ha desarrollado un enfoque centrado en la regulación, la protección de datos, la competencia y la gobernanza de las tecnologías emergentes. Estas estrategias muestran que el poder digital puede ejercerse mediante la innovación, la capacidad productiva, el control de infraestructuras o la definición de normas.

La economía digital también introduce nuevas desigualdades entre países desarrollados y economías en desarrollo. Los Estados que carecen de infraestructura de conectividad, capacidades científicas, financiamiento y personal especializado suelen depender de tecnologías desarrolladas en el exterior. Esta dependencia puede limitar su margen de negociación y dificultar la construcción de industrias digitales propias. De acuerdo con la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD, 2024), la expansión de la economía digital debe analizarse considerando tanto sus oportunidades económicas como sus efectos ambientales y distributivos.

Para América Latina, el desafío consiste en transformar la participación en los mercados digitales en una fuente efectiva de capacidad estratégica. Esto implica fortalecer la investigación científica, mejorar la infraestructura de telecomunicaciones, desarrollar talento especializado y promover marcos de cooperación regional. En el caso de Ecuador, una estrategia de inserción digital sostenible requiere aprovechar las tecnologías para modernizar la producción, la educación y la gestión pública, sin profundizar una dependencia absoluta de proveedores externos.

En consecuencia, el poder estructural en la economía digital internacional debe entenderse como la capacidad de influir sobre las infraestructuras, los flujos de información, los estándares y las reglas que organizan la actividad económica. Su distribución determinará, en buena medida, qué países pueden orientar la transformación tecnológica y cuáles deberán adaptarse a decisiones adoptadas fuera de sus fronteras.

3.2 Plataformas tecnológicas y relaciones de autoridad entre Estados y corporaciones

Las plataformas tecnológicas se han convertido en actores centrales de las relaciones internacionales porque administran espacios fundamentales de comunicación, intercambio comercial, publicidad, almacenamiento de información y prestación de servicios digitales. Empresas como Google, Microsoft, Amazon, Apple, Meta y otras corporaciones con presencia global no son Estados ni sustituyen formalmente sus competencias soberanas; sin embargo, sus decisiones pueden producir efectos económicos, sociales y políticos que atraviesan las fronteras nacionales.

La relevancia de estas empresas se explica, en parte, por los efectos de red: una plataforma puede adquirir mayor valor a medida que aumenta el número de usuarios, proveedores y organizaciones que dependen de ella. Esta dinámica favorece la concentración del mercado y puede dificultar la entrada de nuevos competidores. Parker, Van Alstyne y Choudary (2016) señalan que las plataformas organizan interacciones entre distintos grupos de participantes, estableciendo reglas de acceso, mecanismos de intercambio y condiciones de participación. Por ello, su poder no deriva únicamente de la tecnología que poseen, sino también de su capacidad para organizar ecosistemas económicos completos.

Las plataformas ejercen autoridad mediante decisiones aparentemente operativas: determinar qué contenidos se muestran, suspender cuentas, modificar algoritmos, cambiar las condiciones comerciales o restringir el acceso a determinados servicios. Estas decisiones pueden afectar a empresas, medios de comunicación, instituciones públicas y ciudadanos. Aunque no constituyen actos de gobierno en sentido jurídico, pueden influir en el debate público, la visibilidad de determinados discursos y las oportunidades económicas de millones de usuarios.

Esta situación genera una relación compleja entre los Estados y las corporaciones tecnológicas. Por un lado, los gobiernos necesitan sus servicios para modernizar la administración pública, mejorar la conectividad y desarrollar capacidades de inteligencia artificial. Por otro, deben garantizar la protección de los derechos, la competencia, la seguridad nacional y el cumplimiento de las leyes. La dificultad radica en que las plataformas operan internacionalmente, mientras que muchas competencias regulatorias continúan organizadas dentro de jurisdicciones nacionales.

La gobernanza de datos constituye uno de los principales escenarios de esta disputa. La información recopilada por plataformas digitales puede generar ventajas comerciales, mejorar sistemas predictivos y alimentar modelos de inteligencia artificial. Sin embargo, también plantea interrogantes sobre privacidad, vigilancia, transferencia internacional de datos y distribución de beneficios. La Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2022) destaca la importancia de construir políticas de gobernanza de datos que faciliten su utilización legítima y, al mismo tiempo, consideren la confianza, la seguridad y los derechos de las personas.

Otro ámbito de tensión es la regulación de los mercados digitales. Las autoridades públicas buscan limitar prácticas anticompetitivas, promover la interoperabilidad y reducir las barreras de entrada, mientras que las empresas defienden la protección de sus innovaciones y modelos de negocio. La regulación europea de los mercados digitales y de los servicios digitales ilustra el intento de establecer obligaciones específicas para las grandes plataformas y aumentar su rendición de cuentas. No obstante, la eficacia de estas medidas depende de la capacidad institucional para supervisar operaciones tecnológicas complejas y hacer cumplir las normas frente a empresas transnacionales.

La relación entre Estados y corporaciones también adquiere una dimensión geopolítica cuando las plataformas proporcionan servicios esenciales para infraestructuras críticas, comunicaciones oficiales, almacenamiento de información gubernamental o sistemas de inteligencia artificial. La concentración de estos servicios en pocos proveedores puede generar vulnerabilidades estratégicas, especialmente si las decisiones empresariales, las restricciones legales de otros países o las tensiones diplomáticas afectan su disponibilidad.

Para los países en desarrollo, la cuestión central no consiste necesariamente en excluir a las grandes corporaciones, sino en establecer condiciones que permitan aprovechar sus capacidades sin perder margen de decisión. Entre las medidas posibles se encuentran la contratación pública transparente, la evaluación de riesgos tecnológicos, la protección de datos, la diversificación de proveedores, la formación especializada y el fortalecimiento de las capacidades regulatorias. En Ecuador, estas acciones pueden contribuir a que la digitalización de los servicios públicos y de las actividades productivas se realice con criterios de seguridad, eficiencia e interés nacional.

En definitiva, las plataformas tecnológicas han configurado una forma de autoridad privada que coexiste y, en ocasiones, entra en tensión con la autoridad estatal. La gobernanza de la economía digital exige, por tanto, mecanismos de cooperación y regulación capaces de equilibrar innovación, competencia, derechos fundamentales y soberanía. El objetivo no es reemplazar la iniciativa empresarial por el control estatal absoluto, sino impedir que la concentración de capacidades tecnológicas reduzca la autonomía de las sociedades y limite la rendición de cuentas.

3.3 Cadenas globales de valor: concentración tecnológica, relocalización y autonomía estratégica

Las cadenas globales de valor constituyen uno de los principales mecanismos de organización de la economía internacional contemporánea. A través de ellas, las actividades de investigación, diseño, producción, ensamblaje, distribución y comercialización se desarrollan en distintos países, de acuerdo con sus capacidades tecnológicas, costos, recursos naturales y condiciones institucionales. La digitalización ha intensificado esta fragmentación productiva, pero también ha evidenciado que la eficiencia económica puede generar vulnerabilidades cuando las actividades esenciales se concentran en un número reducido de territorios o empresas.

Gereffi, Humphrey y Sturgeon (2005) explican que la gobernanza de las cadenas globales de valor depende de las relaciones de coordinación y poder entre las empresas participantes. Estas relaciones no son necesariamente equilibradas: las compañías que controlan el diseño, las tecnologías fundamentales, las marcas o el acceso a los mercados suelen capturar una proporción significativa del valor generado. En la economía digital, esta asimetría resulta especialmente visible en industrias como los semiconductores, los

equipos de telecomunicaciones, los dispositivos electrónicos y los servicios de computación en la nube.

La industria de semiconductores ejemplifica esta interdependencia. El diseño de chips, la fabricación de equipos especializados, la producción de obleas, el ensamblaje y las pruebas requieren conocimientos, inversiones e infraestructuras altamente especializadas. Ningún territorio concentra necesariamente todas las capacidades de la cadena en condiciones equivalentes. Como analiza Miller (2022), esta distribución internacional de competencias ha convertido a los semiconductores en un recurso estratégico, debido a su importancia para las telecomunicaciones, la inteligencia artificial, la industria automotriz y los sistemas de defensa.

La concentración tecnológica presenta ventajas económicas, pues permite aprovechar economías de escala, conocimiento especializado y redes de proveedores. Sin embargo, también expone a las economías a interrupciones provocadas por conflictos geopolíticos, restricciones comerciales, desastres naturales, crisis sanitarias o decisiones empresariales. Cuando un componente indispensable depende de pocos fabricantes, sustituirlo puede resultar costoso y requerir largos períodos de adaptación. La interdependencia, por tanto, no garantiza estabilidad: también puede convertirse en un mecanismo de presión política.

Frente a estas vulnerabilidades, diversos gobiernos y empresas han impulsado estrategias de relocalización productiva, diversificación y autonomía estratégica. La relocalización consiste en trasladar determinadas actividades hacia el territorio nacional o hacia países considerados más próximos o confiables. El nearshoring busca acercar la producción a los mercados de consumo, mientras que el friend-shoring procura fortalecer los vínculos productivos con socios considerados estratégicamente confiables. Estas estrategias responden al interés de reducir riesgos de suministro, aunque pueden incrementar los costos de producción y reproducir nuevas concentraciones regionales.

La disputa tecnológica entre Estados Unidos y China refleja estas transformaciones. Las restricciones a la exportación de determinadas tecnologías avanzadas, los incentivos para establecer instalaciones de fabricación y las políticas de fortalecimiento industrial muestran que las cadenas globales de valor se han convertido en instrumentos de competencia geopolítica. Farrell y Newman (2019) advierten que la posición de un actor dentro de las redes económicas internacionales puede proporcionarle capacidad para

ejercer presión sobre otros. En consecuencia, las decisiones de localización productiva ya no responden exclusivamente a criterios de rentabilidad, sino también a consideraciones de seguridad económica y política exterior.

Para América Latina, esta reconfiguración representa una oportunidad de inserción en nuevas cadenas de suministro, pero también un desafío relacionado con la calidad de esa participación. La disponibilidad de minerales críticos, energía, biodiversidad y recursos humanos constituye una ventaja potencial; sin embargo, la exportación de materias primas sin desarrollar capacidades de procesamiento, investigación e innovación puede mantener estructuras de dependencia. La autonomía estratégica requiere avanzar hacia actividades que generen mayor valor agregado, promuevan transferencia de conocimientos y fortalezcan los vínculos entre universidades, centros de investigación, empresas y organismos públicos.

En el caso de Ecuador, la participación en cadenas globales de valor digitales puede apoyarse en la formación de talento especializado, el desarrollo de servicios basados en conocimiento, la modernización de la infraestructura digital y la investigación aplicada. También resulta relevante analizar las oportunidades relacionadas con la gestión de recursos naturales, la observación de ecosistemas, el procesamiento de datos ambientales y la aplicación de inteligencia artificial a la agricultura y la planificación territorial. Estas capacidades no sustituyen la necesidad de acceder a tecnologías internacionales, pero pueden mejorar la posición negociadora del país y reducir su dependencia de actividades de escaso valor agregado.

La política pública debe procurar que la atracción de inversiones tecnológicas se traduzca en beneficios duraderos. Para ello, es necesario evaluar la creación de empleo especializado, la transferencia efectiva de conocimientos, la participación de proveedores nacionales, la sostenibilidad ambiental y la capacidad de las empresas locales para incorporarse a redes internacionales de innovación. De igual forma, la cooperación regional puede facilitar la construcción de infraestructura compartida, el intercambio de capacidades científicas y la coordinación de estrategias de abastecimiento.

3.4 La economía y la tecnología como instrumentos del poder geopolítico

En el sistema internacional contemporáneo, el poder de los Estados no se expresa exclusivamente mediante la capacidad militar, la extensión territorial o la influencia diplomática. También se manifiesta a través del control de los mercados, la regulación de los flujos financieros, el acceso a materias primas estratégicas, la administración de infraestructuras digitales y la capacidad de limitar o facilitar la circulación internacional del conocimiento científico y tecnológico. Esta transformación adquiere especial relevancia en un escenario caracterizado por la interdependencia económica, la digitalización de las actividades productivas y la creciente competencia por el dominio de tecnologías de uso civil y militar.

Las sanciones económicas, los controles de exportación y las restricciones a la transferencia tecnológica constituyen instrumentos fundamentales de lo que la literatura especializada denomina poder económico del Estado o coerción económica. A través de ellos, los gobiernos buscan modificar los incentivos de otros actores internacionales, elevar el costo de determinadas decisiones políticas, restringir capacidades consideradas estratégicamente sensibles o preservar ventajas competitivas en sectores esenciales para la seguridad nacional. Estas medidas pueden aplicarse de manera unilateral, coordinarse entre varios Estados o establecerse mediante decisiones de organismos internacionales, dependiendo de su fundamento jurídico, sus objetivos y los actores que participan en su implementación.

La importancia de estos mecanismos radica en que permiten ejercer presión sin recurrir necesariamente al empleo directo de la fuerza armada. Sin embargo, su naturaleza no es exclusivamente económica: sus efectos pueden alcanzar la estructura industrial, las relaciones diplomáticas, la estabilidad financiera, la autonomía científica y las posibilidades de desarrollo de los países afectados. En consecuencia, su análisis exige integrar las perspectivas de las relaciones internacionales, la economía política internacional, los estudios estratégicos y la gobernanza tecnológica.

Desde una perspectiva clásica, las sanciones pueden interpretarse como instrumentos de coerción destinados a modificar el comportamiento de un adversario. No obstante, la interdependencia contemporánea ha ampliado las posibilidades de ejercer presión mediante redes comerciales y financieras que conectan a empresas, instituciones, Estados

y organismos multilaterales. Farrell y Newman (2019) explican que la estructura de estas redes genera asimetrías de poder: los actores que controlan nodos centrales pueden aprovechar su posición para obtener información estratégica o restringir el acceso de terceros a recursos y servicios esenciales.

Esta interpretación permite comprender un aspecto fundamental de las relaciones internacionales del siglo XXI: la interdependencia no elimina las relaciones de poder; también puede convertirse en una fuente de vulnerabilidad y coerción. La integración en los mercados globales genera beneficios económicos, pero puede producir dependencias asimétricas cuando un país necesita acceder a tecnologías, sistemas de pagos, componentes industriales o plataformas digitales controladas por actores externos.

En este contexto, el concepto de Relaciones Internacionales 6.0 puede utilizarse como una perspectiva analítica para estudiar la interacción entre geopolítica, datos, infraestructura digital, inteligencia artificial y soberanía tecnológica. No constituye una categoría teórica universalmente consolidada, sino un marco interpretativo propuesto para examinar cómo las capacidades digitales transforman los instrumentos tradicionales del poder internacional.

Desde esta perspectiva, las sanciones económicas y las restricciones tecnológicas deben analizarse no solo por las pérdidas comerciales que ocasionan, sino también por su capacidad para reorganizar las redes de dependencia, alterar las trayectorias de innovación y redefinir las condiciones de participación de los Estados en la economía mundial.

3.4.1. Fundamentos conceptuales de las sanciones económicas

Las sanciones económicas pueden definirse como medidas restrictivas adoptadas por uno o varios actores políticos para incrementar los costos económicos de determinadas conductas y promover un cambio de comportamiento, impedir el acceso a recursos estratégicos o expresar una respuesta institucional frente a acciones consideradas incompatibles con determinados objetivos internacionales. Su aplicación puede afectar a gobiernos, entidades financieras, empresas, organizaciones o personas específicas.

Hufbauer et al. (2007), en uno de los estudios de referencia sobre el tema, examinan las sanciones como instrumentos de política exterior cuyo alcance y resultados dependen de

factores como los objetivos perseguidos, las relaciones económicas entre los países, la capacidad de resistencia del Estado destinatario y la cooperación internacional. Su análisis evidencia que la imposición de costos económicos no garantiza automáticamente la modificación de una conducta política. La eficacia depende de la relación entre los objetivos establecidos, los mecanismos de presión y las condiciones internas y externas del país afectado.

Esta distinción es esencial para evitar una interpretación simplificada de las sanciones. Un deterioro económico puede demostrar que las restricciones producen efectos materiales, pero no necesariamente que han alcanzado su finalidad política. Un gobierno puede experimentar pérdidas comerciales, dificultades financieras y problemas de abastecimiento sin modificar la decisión que originó las medidas. De igual manera, una sanción que no genera una transformación política inmediata puede producir efectos acumulativos sobre la capacidad industrial, el acceso a financiamiento o las posibilidades de modernización tecnológica.

Drezner (1999) analiza las sanciones desde la perspectiva de la coerción económica y de las relaciones estratégicas entre los Estados. Su planteamiento permite comprender que las sanciones no se aplican en un vacío político: los vínculos previos, las expectativas de cooperación y las posibles represalias influyen en la decisión de imponerlas y en la respuesta del destinatario. La interdependencia comercial puede aumentar la capacidad de presión, pero también eleva los costos que debe asumir quien decide interrumpir los intercambios.

Por ello, las sanciones deben entenderse como parte de una relación estratégica en la que intervienen, al menos, tres dimensiones. La primera corresponde a la capacidad material del actor que impone la medida para restringir flujos comerciales, financieros o tecnológicos. La segunda se relaciona con la vulnerabilidad y las posibilidades de adaptación del destinatario. La tercera comprende la legitimidad política y jurídica de la medida, así como el grado de cooperación internacional necesario para sostenerla.

Desde el punto de vista institucional, es importante diferenciar las sanciones adoptadas por el Consejo de Seguridad de las Naciones Unidas de aquellas establecidas unilateralmente por los Estados o mediante mecanismos regionales. El artículo 41 de la Carta de las Naciones Unidas contempla medidas que no implican el uso de la fuerza

armada y que pueden incluir la interrupción total o parcial de relaciones económicas y de comunicaciones, así como la ruptura de relaciones diplomáticas. El Consejo de Seguridad utiliza este marco para establecer medidas que pueden abarcar embargos de armas, restricciones financieras, prohibiciones de viaje y otras limitaciones específicas.

Esta base jurídica no significa que todas las medidas denominadas sanciones posean idéntico fundamento legal, alcance o legitimidad. Las sanciones unilaterales, las restricciones coordinadas entre aliados y las medidas obligatorias adoptadas por el Consejo de Seguridad deben examinarse de acuerdo con sus respectivos marcos normativos, las obligaciones internacionales aplicables y las circunstancias particulares de cada caso.

La distinción también resulta relevante para la gobernanza global. Cuando las restricciones se adoptan mediante mecanismos multilaterales, pueden contar con procedimientos institucionales de deliberación, seguimiento y revisión. Cuando se establecen unilateralmente, su alcance internacional puede depender en mayor medida del peso económico del Estado emisor, de la posición de sus empresas en las redes globales y de la disposición de terceros países a cumplirlas.

En consecuencia, la capacidad de imponer sanciones no deriva únicamente del tamaño de una economía. También depende de su centralidad en las redes financieras, de su influencia sobre los mercados, de la jurisdicción aplicable a determinadas transacciones y de la disponibilidad de instrumentos administrativos para supervisar el cumplimiento.

3.4.2. Evolución de las sanciones: de la presión comercial a la coerción mediante redes globales

Históricamente, las restricciones económicas han acompañado los conflictos entre Estados mediante bloqueos comerciales, embargos, prohibiciones de importación y limitaciones al acceso a recursos esenciales. Durante buena parte del siglo XX, estos instrumentos se vincularon con estrategias de aislamiento económico, presión diplomática y contención de capacidades militares o industriales.

La expansión de la globalización modificó sus condiciones de aplicación. La internacionalización de las cadenas de suministro, el crecimiento de los mercados financieros y la concentración de determinados servicios en redes transnacionales

generaron nuevas oportunidades para ejercer presión. El poder dejó de depender exclusivamente de la capacidad de bloquear físicamente una ruta comercial o controlar un recurso natural y comenzó a incluir la posibilidad de interrumpir transacciones financieras, restringir servicios especializados y limitar el acceso a infraestructuras digitales.

Farrell y Newman (2019) conceptualizan esta transformación mediante la noción de interdependencia instrumentalizada (weaponized interdependence). Su argumento identifica dos mecanismos principales. El primero, denominado efecto de vigilancia o panopticon effect, aparece cuando la centralidad de un actor en una red le permite acceder a información relevante sobre las transacciones y actividades de otros participantes. El segundo, denominado efecto de estrangulamiento o chokepoint effect, se produce cuando esa posición central permite interrumpir o dificultar el acceso de terceros a una red esencial.

Ambos mecanismos tienen implicaciones para la política internacional. Un Estado que posee una influencia considerable sobre determinados canales financieros puede dificultar las operaciones de instituciones sujetas a restricciones. De manera semejante, un país que controla tecnologías, componentes o servicios indispensables para una industria puede limitar el acceso de otros actores a esos recursos. La capacidad de ejercer presión surge, en estos casos, de la posición estructural que se ocupa dentro de la red, no solamente del volumen total de la economía.

Esta perspectiva explica por qué las sanciones contemporáneas pueden producir efectos más amplios que una prohibición comercial tradicional. Cuando una entidad financiera teme perder acceso a mercados, sistemas de compensación o corresponsales internacionales, puede interrumpir operaciones incluso cuando la transacción concreta requiere una evaluación jurídica más detallada. De manera análoga, una empresa tecnológica puede suspender suministros, licencias o servicios de mantenimiento para reducir riesgos regulatorios.

La centralidad de las redes también introduce una contradicción estratégica. El control de infraestructuras globales proporciona ventajas a corto plazo, pero su utilización reiterada con fines coercitivos puede incentivar a otros Estados a diversificar proveedores, desarrollar sistemas alternativos o reducir su exposición a los centros de poder existentes.

Farrell y Newman (2019) permiten interpretar esta reacción como una consecuencia de las asimetrías de la interdependencia y de los incentivos para disminuir la vulnerabilidad frente a posibles restricciones.

Así, las sanciones dejan de ser únicamente mecanismos destinados a castigar conductas específicas y pueden convertirse en factores que impulsan la reorganización de la economía mundial. Su impacto se extiende a las decisiones de inversión, las estrategias de innovación, la localización de infraestructuras, las alianzas internacionales y la formulación de políticas de autonomía estratégica.

Desde la perspectiva de las Relaciones Internacionales 6.0, esta evolución representa un cambio en la geografía del poder. La influencia internacional depende cada vez más de quién controla los puntos críticos de las redes globales, quién establece las condiciones de acceso y quién posee la capacidad científica e industrial para sustituir los recursos restringidos.

3.4.3. Tipología de las sanciones económicas y sus mecanismos de aplicación

La diversidad de sanciones económicas exige distinguir entre los instrumentos utilizados, los destinatarios de las medidas y los objetivos estratégicos que se persiguen. Aunque en la práctica pueden combinarse varias modalidades, su diferenciación permite comprender los canales mediante los cuales se ejerce presión y los efectos que pueden producir sobre las economías nacionales y las relaciones internacionales.

Sanciones comerciales

Las sanciones comerciales comprenden restricciones a las importaciones y exportaciones, prohibiciones de comercialización de determinados productos, embargos sectoriales y limitaciones a la prestación de servicios relacionados con las actividades restringidas. Su finalidad puede consistir en reducir los ingresos de un Estado, impedir el abastecimiento de bienes estratégicos o limitar su capacidad para sostener determinadas actividades industriales y militares.

El impacto de estas medidas depende de la estructura productiva del país destinatario. Una economía que depende de la exportación de un reducido número de productos puede experimentar una reducción significativa de sus ingresos cuando pierde acceso a

mercados importantes. Por el contrario, un país con mercados alternativos, reservas suficientes y capacidad productiva interna puede amortiguar parte de las consecuencias.

No obstante, la sustitución de mercados no siempre resulta inmediata. Los contratos comerciales, las características técnicas de los productos, los costos logísticos y las exigencias regulatorias pueden dificultar la búsqueda de compradores o proveedores alternativos. Por consiguiente, el efecto de una sanción comercial debe analizarse considerando tanto la pérdida inicial de intercambios como los costos de adaptación que enfrenta el sistema económico.

Sanciones financieras

Las sanciones financieras restringen el acceso a determinados activos, servicios bancarios, operaciones de crédito, mecanismos de pago o transacciones internacionales. Entre sus modalidades se encuentran la congelación de activos de personas y entidades designadas, las restricciones a la financiación de determinados sectores y las prohibiciones de realizar operaciones con instituciones específicas.

Estas medidas adquieren especial relevancia porque las economías contemporáneas dependen de sistemas financieros que facilitan el comercio, la inversión y la circulación internacional del capital. La restricción de una operación financiera puede repercutir en otras actividades, como la adquisición de maquinaria, la contratación de seguros, el pago de servicios o la financiación de proyectos industriales.

Drezner (1999) destaca la importancia de las relaciones estratégicas y de los costos de las sanciones para comprender su aplicación. En el entorno financiero actual, esta cuestión se amplía debido a la posición que determinadas monedas, instituciones y redes de pago ocupan en las transacciones internacionales. La posibilidad de perder acceso a estos canales puede inducir a empresas y bancos a modificar su comportamiento incluso antes de que se materialicen todas las consecuencias económicas de una medida.

Sin embargo, los efectos financieros no se distribuyen de manera uniforme. Las grandes empresas pueden disponer de asesoría jurídica, equipos de cumplimiento normativo y recursos para reorganizar sus operaciones, mientras que las pequeñas y medianas empresas pueden enfrentar dificultades para interpretar las restricciones y encontrar

alternativas. Asimismo, las interrupciones de pagos pueden afectar a terceros que no constituyen el objetivo principal de las medidas.

Sanciones sectoriales y restricciones a la inversión

Las sanciones sectoriales se dirigen a actividades económicas consideradas estratégicamente sensibles, como la energía, la defensa, la minería, las telecomunicaciones o determinados servicios tecnológicos. Pueden incluir prohibiciones de inversión, limitaciones a la financiación de proyectos, restricciones a la venta de equipos y controles sobre la prestación de asistencia técnica.

Su lógica consiste en reducir las capacidades de un sector sin necesariamente interrumpir todas las relaciones económicas con el Estado destinatario. Esta orientación permite concentrar la presión en actividades vinculadas con objetivos de seguridad o política exterior.

Sin embargo, los límites entre sectores civiles y estratégicos pueden resultar difusos. Los sistemas de navegación por satélite, la inteligencia artificial, los sensores, las telecomunicaciones y los componentes electrónicos pueden utilizarse en actividades comerciales, científicas, industriales o militares. Por esta razón, la identificación de los productos y destinatarios sujetos a restricciones constituye una de las principales dificultades de la regulación contemporánea.

Sanciones selectivas y sanciones de alcance general

Las sanciones selectivas, también denominadas sanciones dirigidas, buscan afectar a personas, organizaciones, empresas o actividades específicas. Entre sus instrumentos se encuentran las congelaciones de activos, las prohibiciones de viaje, los embargos de armas y determinadas restricciones comerciales o financieras.

La selección de destinatarios puede reducir la exposición de la población a los efectos de una medida, aunque no garantiza que sus consecuencias indirectas sean limitadas. Las empresas relacionadas con las entidades designadas, los trabajadores de sectores afectados y los consumidores pueden experimentar efectos derivados de la reducción de las operaciones o de la incertidumbre regulatoria.

Las sanciones de alcance general, por su parte, restringen una proporción más amplia de los intercambios económicos. Su aplicación puede afectar la disponibilidad de bienes, los ingresos fiscales y el funcionamiento de las cadenas productivas. La experiencia histórica ha contribuido a reforzar el interés por medidas más focalizadas, sin eliminar el debate sobre su eficacia, proporcionalidad y consecuencias humanitarias.

En el marco de las Naciones Unidas, el Consejo de Seguridad ha utilizado tanto medidas económicas y comerciales generales como sanciones dirigidas contra actores determinados. Esta diversidad demuestra que las sanciones no constituyen una herramienta única, sino un conjunto de instrumentos cuya configuración depende de los objetivos y las circunstancias de cada situación (Naciones Unidas, s. f.).

Sanciones secundarias y efectos extraterritoriales

Las sanciones secundarias buscan influir en la conducta de actores de terceros países que mantienen determinadas relaciones económicas con las entidades o sectores objeto de restricciones. Su aplicación puede generar un dilema para empresas y bancos internacionales: continuar una operación comercial puede implicar riesgos regulatorios en una jurisdicción, mientras que interrumpirla puede ocasionar pérdidas en otra.

Esta modalidad adquiere relevancia cuando un Estado utiliza su posición en los mercados financieros o tecnológicos para extender los efectos de sus decisiones más allá de sus fronteras. Farrell y Newman (2019) ofrecen un marco útil para interpretar esta capacidad, al mostrar cómo el control de nodos centrales de las redes globales puede transformarse en una fuente de influencia sobre actores que no dependen directamente del Estado emisor en todas sus actividades.

No obstante, las sanciones secundarias también pueden generar tensiones diplomáticas y conflictos de jurisdicción. Los Estados afectados pueden considerar que estas medidas interfieren con sus políticas comerciales o con sus decisiones soberanas. Por ello, su análisis requiere distinguir entre la existencia de una norma interna, su alcance jurídico, sus efectos prácticos y las controversias que suscita en el plano internacional.

3.4.4. Controles de exportación: seguridad nacional, competitividad y poder industrial

Los controles de exportación constituyen instrumentos regulatorios mediante los cuales los Estados determinan qué bienes, tecnologías, programas informáticos, conocimientos técnicos o servicios pueden transferirse a determinados destinos, usuarios finales o aplicaciones. A diferencia de una sanción económica general, un control de exportación puede aplicarse de manera preventiva, sin que exista necesariamente un conflicto diplomático abierto o una sanción formal contra el país receptor.

Su fundamento suele encontrarse en la necesidad de evitar la proliferación de armas, proteger tecnologías sensibles, impedir determinados usos militares o preservar capacidades consideradas esenciales para la seguridad nacional. Sin embargo, el alcance de estos controles también puede influir en la competencia industrial y en la distribución internacional de las capacidades tecnológicas.

Los productos de doble uso ocupan una posición central en este ámbito. Se trata de bienes, programas o tecnologías que pueden emplearse tanto con fines civiles como militares. Un componente electrónico, un equipo de fabricación de precisión, un sensor avanzado o determinado software de simulación pueden utilizarse en actividades científicas y productivas, pero también integrarse en sistemas de defensa o vigilancia.

Esta dualidad dificulta la separación entre cooperación económica legítima y riesgos de seguridad. La evaluación de una exportación no depende exclusivamente de las características físicas del producto, sino también de su rendimiento técnico, el usuario final, la aplicación prevista, el destino y las normas aplicables.

En consecuencia, los controles contemporáneos requieren sistemas de clasificación de productos, licencias, verificación de usuarios finales, auditorías de cumplimiento y mecanismos de coordinación entre autoridades y empresas. En sectores de rápida evolución, como la computación avanzada, la actualización normativa constituye un desafío permanente porque las características de los productos pueden cambiar con mayor rapidez que los procedimientos administrativos.

El caso de los semiconductores y la computación avanzada

Los semiconductores constituyen un ejemplo especialmente ilustrativo de la convergencia entre política industrial, seguridad nacional y competencia geopolítica. Estos componentes son esenciales para los centros de datos, los teléfonos inteligentes, los vehículos, los sistemas de comunicación, la automatización industrial y las aplicaciones de inteligencia artificial. También desempeñan funciones relevantes en sistemas militares y tecnologías de uso estratégico.

La capacidad de fabricar semiconductores avanzados depende de una cadena internacional especializada que incluye diseño electrónico, propiedad intelectual, equipos de litografía, materiales de alta pureza, software de diseño y procesos de fabricación de elevada precisión. Ningún análisis de la competencia tecnológica puede comprenderse adecuadamente sin considerar las interdependencias que existen entre estos componentes.

En octubre de 2022, el Departamento de Comercio de Estados Unidos, mediante su Bureau of Industry and Security (BIS), anunció controles sobre determinados circuitos integrados de computación avanzada, equipos para fabricar semiconductores y actividades relacionadas con la producción tecnológica en China. Las disposiciones fueron actualizadas en octubre de 2023 para ajustar los criterios técnicos, ampliar determinados requisitos de licencia y abordar posibles mecanismos de elusión (Bureau of Industry and Security [BIS], 2022, 2023).

Estas medidas permiten observar cómo el control de exportaciones puede actuar sobre diferentes eslabones de una misma cadena de valor. La restricción no se limita necesariamente a impedir la venta de un producto terminado; también puede afectar los equipos utilizados para producirlo, determinados componentes de alto rendimiento y la asistencia técnica vinculada con su fabricación.

Desde el punto de vista estratégico, la finalidad declarada de estas disposiciones se relaciona con la protección de intereses de seguridad nacional y la limitación de ciertas capacidades tecnológicas sensibles. Su efecto económico, sin embargo, debe analizarse por separado de su justificación oficial. Los controles pueden aumentar las dificultades de acceso a tecnologías específicas, modificar las decisiones de inversión y alterar la organización de las cadenas internacionales de suministro.

La evaluación de sus resultados requiere distinguir entre la reducción inmediata del acceso a determinados productos, la capacidad del país destinatario para sustituirlos, los costos que enfrentan las empresas proveedoras y las transformaciones de largo plazo en la innovación. Las restricciones pueden dificultar el desarrollo de determinadas capacidades, pero también pueden incentivar inversiones en investigación, formación de especialistas y producción nacional de componentes alternativos.

Por ello, el caso de los semiconductores ilustra una característica esencial de la geopolítica tecnológica: restringir el acceso a una tecnología no equivale necesariamente a eliminar la capacidad de desarrollarla. El resultado depende de la complejidad del conocimiento requerido, de la disponibilidad de recursos financieros y humanos, de las redes de cooperación científica y de la posibilidad de acceder a equipos, materiales y mercados alternativos.

La interdependencia de las cadenas tecnológicas

La industria de los semiconductores también demuestra que el poder tecnológico no debe medirse exclusivamente por la capacidad de fabricar un producto final. Una empresa puede dominar el diseño de un circuito, otra desarrollar el software especializado, una tercera producir los equipos de fabricación y una cuarta disponer de instalaciones capaces de manufacturar los componentes con el nivel de precisión requerido.

Esta distribución internacional de capacidades genera una red de especialización que puede aumentar la eficiencia productiva, pero también produce dependencias críticas. Cuando una jurisdicción controla una tecnología difícil de sustituir, sus decisiones regulatorias pueden repercutir sobre empresas de numerosos países.

La consecuencia geopolítica es que la ventaja estratégica puede concentrarse en determinados puntos de la cadena de valor. No obstante, esa concentración también puede representar una vulnerabilidad para el país que controla el punto crítico, pues sus empresas dependen de clientes, materiales, mercados y conocimientos desarrollados en otras jurisdicciones. La instrumentalización de la interdependencia puede provocar, por tanto, respuestas de diversificación y estrategias de reducción de dependencias por parte de todos los actores involucrados (Farrell & Newman, 2019).

En este contexto, los controles de exportación plantean una cuestión fundamental para la gobernanza global: ¿cómo proteger tecnologías sensibles sin fragmentar innecesariamente los sistemas de cooperación científica y productiva de los que depende la innovación mundial?

Una respuesta institucional requiere definir criterios claros sobre las tecnologías restringidas, mantener procedimientos de revisión, distinguir entre usos civiles y aplicaciones sensibles cuando sea posible y establecer mecanismos de coordinación internacional. La ausencia de criterios transparentes puede incrementar la incertidumbre empresarial y dificultar la cooperación científica, mientras que una regulación demasiado limitada puede no responder adecuadamente a los riesgos de seguridad que pretende atender.

3.4.5. Restricciones a la transferencia tecnológica y disputa por la soberanía del conocimiento

La transferencia tecnológica comprende los procesos mediante los cuales conocimientos científicos, capacidades técnicas, procedimientos productivos, licencias, diseños, software y otros activos tecnológicos pasan de una organización o jurisdicción a otra. Puede realizarse mediante inversión extranjera, contratos de licencia, cooperación universitaria, investigación conjunta, movilidad de especialistas, adquisición de empresas o suministro de equipos acompañados de asistencia técnica.

Estas transferencias contribuyen a la innovación porque permiten que las organizaciones receptoras incorporen conocimientos que, de otro modo, requerirían largos periodos de investigación y desarrollo. También facilitan la formación de capital humano, la creación de capacidades industriales y la integración en cadenas internacionales de valor.

Sin embargo, el conocimiento tecnológico puede tener implicaciones estratégicas. Algunas capacidades son indispensables para la fabricación de productos militares, sistemas de vigilancia, infraestructuras críticas o herramientas avanzadas de procesamiento de información. Por esta razón, los Estados pueden imponer restricciones a determinadas transferencias, especialmente cuando consideran que el conocimiento podría utilizarse para fines contrarios a sus intereses de seguridad.

Es necesario distinguir, en este punto, entre las restricciones justificadas por objetivos de seguridad y las medidas que responden principalmente a consideraciones de competencia económica. Aunque ambas pueden coincidir en una misma política, sus fundamentos y consecuencias no son idénticos. Una restricción dirigida a impedir la transferencia de conocimientos vinculados con armas de destrucción masiva presenta características diferentes de una política que limita inversiones o adquisiciones empresariales en un sector considerado estratégicamente importante.

La distinción resulta relevante porque la seguridad tecnológica puede convertirse en un argumento amplio que abarque actividades científicas, comerciales y empresariales. Cuando las categorías regulatorias no se definen con precisión, aumenta el riesgo de que la incertidumbre afecte intercambios legítimos, inversiones productivas y proyectos de investigación internacional.

Propiedad intelectual y control del conocimiento

La propiedad intelectual constituye uno de los mecanismos mediante los cuales se regula la explotación y circulación de determinados conocimientos tecnológicos. Las patentes, los derechos de autor, los secretos empresariales y las licencias contractuales pueden determinar quién utiliza una tecnología, en qué condiciones y con qué limitaciones.

No obstante, propiedad intelectual y control de exportaciones son categorías diferentes. La primera regula derechos sobre determinados activos intangibles; el segundo establece restricciones públicas sobre operaciones o transferencias que pueden involucrar bienes, software, conocimientos o servicios. Una tecnología puede estar protegida mediante una patente y, al mismo tiempo, quedar sometida a controles de exportación. Del mismo modo, la existencia de derechos de propiedad intelectual no implica automáticamente que una transferencia esté prohibida por razones de seguridad nacional.

En términos geopolíticos, la capacidad de desarrollar tecnologías propias puede incrementar el margen de autonomía de un Estado. Cuando un país depende de licencias extranjeras, proveedores exclusivos o servicios tecnológicos sujetos a decisiones regulatorias externas, su capacidad de planificación puede verse condicionada por factores que escapan a su control directo.

Sin embargo, la autonomía tecnológica no significa necesariamente autosuficiencia absoluta. La producción de tecnologías avanzadas suele requerir cooperación internacional, mercados amplios, cadenas de suministro especializadas y acceso a conocimientos científicos distribuidos entre múltiples países. Una estrategia de soberanía tecnológica puede orientarse, por tanto, a diversificar proveedores, fortalecer capacidades nacionales en áreas críticas y conservar alternativas de acceso, en lugar de intentar reproducir internamente todos los componentes de una industria.

Restricciones a la cooperación científica y la movilidad del conocimiento

La transferencia tecnológica no se produce únicamente mediante mercancías o contratos comerciales. También tiene lugar a través de la colaboración entre universidades, centros de investigación, empresas y especialistas. La movilidad de investigadores, el intercambio de datos, el acceso a laboratorios y el desarrollo de proyectos conjuntos pueden contribuir a la formación de capacidades tecnológicas.

Las restricciones que afectan estas actividades pueden generar consecuencias que van más allá de una transacción económica. La limitación del acceso a determinados equipos o programas especializados puede retrasar proyectos científicos, reducir la disponibilidad de herramientas de análisis y dificultar la formación de personal altamente cualificado.

Este aspecto adquiere especial importancia en el ámbito de la inteligencia artificial, la biotecnología, la computación de alto rendimiento, la robótica y las tecnologías aeroespaciales. En estos sectores, las capacidades de innovación dependen tanto de la infraestructura material como de la circulación del conocimiento y de la colaboración entre especialistas.

No obstante, tampoco sería adecuado considerar toda cooperación científica como exenta de riesgos. Los proyectos internacionales pueden involucrar tecnologías de doble uso, datos sensibles o conocimientos sujetos a obligaciones regulatorias. La cuestión central consiste en establecer mecanismos de evaluación proporcionales que permitan proteger intereses legítimos de seguridad sin convertir las restricciones en obstáculos indiscriminados para la investigación y la cooperación académica.

Desde el enfoque de las Relaciones Internacionales 6.0, la disputa por la tecnología es también una disputa por las condiciones de producción, validación y circulación del

conocimiento. La capacidad de innovar, formar especialistas y mantener infraestructuras científicas confiables constituye una fuente de influencia internacional que complementa las formas tradicionales de poder económico y militar.

3.4.6. La competencia tecnológica entre Estados Unidos y China: una expresión de la geopolítica digital

La competencia tecnológica entre Estados Unidos y China constituye uno de los escenarios más representativos de la transformación de las relaciones de poder en la economía internacional. Esta rivalidad no se limita al intercambio comercial ni a las diferencias sobre políticas industriales. Comprende también la capacidad de diseñar semiconductores, desarrollar inteligencia artificial, controlar infraestructuras de telecomunicaciones, producir equipos industriales avanzados y establecer estándares tecnológicos con alcance internacional.

Desde una perspectiva geopolítica, la tecnología representa simultáneamente un recurso económico, un instrumento de seguridad y una fuente de influencia normativa. Los Estados que desarrollan capacidades tecnológicas avanzadas pueden mejorar su productividad, fortalecer determinadas capacidades militares y ejercer influencia sobre los estándares que utilizan empresas y gobiernos de otros países.

Farrell y Newman (2019) permiten interpretar esta competencia mediante el concepto de interdependencia instrumentalizada. La posición que ocupa un Estado en las redes internacionales de producción, financiación y circulación de información puede convertirse en una fuente de poder coercitivo. En el ámbito tecnológico, esta capacidad se manifiesta cuando el acceso a determinados componentes, equipos, programas o servicios depende de proveedores sometidos a jurisdicciones específicas.

Las restricciones estadounidenses sobre determinados semiconductores avanzados destinados a China ilustran esta dinámica. Las disposiciones anunciadas en 2022 y actualizadas en 2023 incluyeron requisitos de licencia para ciertos productos de computación avanzada y equipos de fabricación de semiconductores, así como medidas orientadas a reducir posibles vías de elusión (BIS, 2022, 2023).

Estas medidas deben analizarse en dos niveles. En el primero, se encuentra la justificación oficial relacionada con la seguridad nacional y el control de capacidades consideradas

sensibles. En el segundo, aparecen sus consecuencias sobre la estructura de la competencia industrial, la planificación empresarial y la distribución internacional de las capacidades tecnológicas. La existencia de una justificación de seguridad no elimina la necesidad de estudiar los efectos económicos de las medidas; de igual forma, sus consecuencias comerciales no demuestran por sí solas que su finalidad sea exclusivamente económica.

La respuesta de un país sometido a restricciones puede adoptar diferentes formas: diversificar sus proveedores, invertir en investigación nacional, fortalecer la formación de especialistas, sustituir componentes importados o establecer nuevas alianzas internacionales. Estas estrategias requieren recursos financieros, tiempo y acceso a conocimientos especializados. Su viabilidad depende de las capacidades existentes y del grado de dificultad para reproducir las tecnologías restringidas.

La competencia tecnológica también puede modificar las decisiones de las empresas multinacionales. Cuando el cumplimiento de las normas de exportación implica costos crecientes o incertidumbre jurídica, algunas compañías pueden reorganizar sus cadenas de suministro, modificar sus inversiones o separar determinadas actividades productivas. Estas decisiones pueden contribuir a la fragmentación de redes que anteriormente operaban bajo criterios predominantemente comerciales.

Sin embargo, la fragmentación no es necesariamente completa. Las economías continúan vinculadas por mercados, inversiones, proveedores y capacidades productivas que resultan difíciles de sustituir de manera inmediata. La rivalidad estratégica coexiste, por tanto, con formas de interdependencia económica que pueden limitar los costos de una separación absoluta.

El resultado es una configuración internacional en la que la cooperación y la competencia tecnológica se desarrollan simultáneamente. Los Estados buscan proteger sus capacidades críticas, pero también necesitan acceder a conocimientos, mercados y recursos que se encuentran fuera de sus fronteras. La gestión de esta tensión constituye uno de los principales desafíos de la gobernanza global.

3.4.7. Efectos económicos, sociales y geopolíticos de las restricciones

El análisis de las sanciones y los controles tecnológicos no debe limitarse a identificar sus objetivos declarados. También es necesario examinar los efectos que producen sobre los países destinatarios, las economías que aplican las medidas y los terceros actores que participan en las cadenas internacionales de valor.

En el país destinatario, las restricciones pueden aumentar los costos de importación, reducir la disponibilidad de determinados productos y dificultar la modernización de sectores industriales. Cuando afectan tecnologías esenciales para la producción, sus consecuencias pueden extenderse a actividades que no constituyen el objetivo directo de la política restrictiva.

Los efectos también pueden manifestarse en la inversión y la innovación. La incertidumbre sobre el acceso futuro a componentes, programas o equipos especializados puede inducir a las empresas a aplazar proyectos, modificar sus proveedores o destinar recursos a la búsqueda de alternativas. En determinadas circunstancias, estas decisiones reducen la eficiencia productiva y elevan los costos de adaptación.

Sin embargo, las restricciones también pueden estimular inversiones nacionales orientadas a sustituir importaciones y desarrollar capacidades propias. Este resultado no es automático: requiere financiación, infraestructura, capital humano, acceso a materiales y un entorno institucional que permita sostener procesos de investigación y desarrollo. La sustitución tecnológica puede resultar viable en algunos sectores y considerablemente más difícil en otros.

Los Estados que imponen las restricciones también pueden asumir costos. Sus empresas exportadoras pueden perder mercados, enfrentar represalias comerciales o reducir ingresos provenientes de la venta de productos y servicios especializados. Además, los incentivos para desarrollar proveedores alternativos pueden modificar las relaciones de dependencia que anteriormente favorecían a las compañías del país emisor.

En el ámbito internacional, la adopción reiterada de restricciones puede promover la diversificación de sistemas de pago, la creación de nuevas asociaciones tecnológicas y el desarrollo de cadenas de suministro menos dependientes de determinados países. Farrell y Newman (2019) ayudan a comprender esta dinámica: cuando los actores perciben que

una red puede utilizarse como mecanismo de coerción, aumenta el incentivo para reducir su exposición a los puntos de control dominantes.

La distribución social de los costos merece una consideración particular. Las restricciones que afectan sectores productivos pueden repercutir en el empleo, los precios y los ingresos de los hogares. Los problemas de cumplimiento normativo pueden generar también efectos indirectos cuando instituciones financieras o empresas interrumpen operaciones por precaución. Por esta razón, el análisis de las consecuencias humanitarias debe distinguir entre los efectos directamente establecidos por las normas y aquellos que aparecen como consecuencia de las respuestas de los intermediarios económicos.

La evaluación rigurosa requiere indicadores que permitan distinguir entre la eficacia económica y la eficacia política. La reducción de exportaciones, la caída de la inversión o el encarecimiento de componentes son indicadores de impacto material; no demuestran, por sí mismos, que se haya alcanzado el objetivo diplomático o estratégico de la medida.

En consecuencia, las sanciones y los controles tecnológicos deben evaluarse mediante una perspectiva multidimensional que considere sus objetivos, su fundamento jurídico, los costos para los diferentes actores, las posibilidades de adaptación y los efectos sobre la estabilidad de las relaciones internacionales.

3.4.8. Gobernanza global, derecho internacional y desafíos regulatorios

La expansión de las restricciones económicas y tecnológicas plantea interrogantes sobre la capacidad de las instituciones internacionales para coordinar las decisiones de los Estados y establecer condiciones previsibles para las relaciones comerciales. La dificultad radica en que estos instrumentos se sitúan en la intersección entre seguridad nacional, política exterior, comercio, derechos humanos y regulación de la innovación.

La Carta de las Naciones Unidas establece, en su artículo 41, el marco para que el Consejo de Seguridad adopte medidas que no impliquen el uso de la fuerza armada en el ejercicio de sus responsabilidades relacionadas con la paz y la seguridad internacionales. Entre las medidas contempladas figuran las interrupciones de relaciones económicas y otras restricciones no militares (Naciones Unidas, s. f.).

Este marco institucional debe distinguirse de los regímenes nacionales de control de exportaciones y de las sanciones adoptadas por Estados o agrupaciones regionales. Aunque estos instrumentos pueden perseguir objetivos relacionados, no poseen necesariamente la misma base jurídica ni los mismos procedimientos de adopción y supervisión.

La gobernanza de las restricciones tecnológicas plantea, además, un desafío de coordinación. Las cadenas de suministro atraviesan múltiples jurisdicciones, mientras que las decisiones regulatorias se adoptan principalmente en ámbitos nacionales o regionales. Una empresa puede diseñar un producto en un país, fabricarlo en otro, incorporar componentes procedentes de varias economías y comercializarlo internacionalmente. En estas condiciones, determinar las obligaciones aplicables requiere examinar las normas pertinentes, el origen de los componentes, los destinos, los usuarios finales y las actividades concretas.

La ausencia de coordinación puede generar interpretaciones divergentes, duplicación de procedimientos y costos de cumplimiento. Al mismo tiempo, una coordinación insuficiente puede facilitar el desvío de productos hacia usuarios o aplicaciones restringidos. El desafío consiste en establecer mecanismos que permitan proteger intereses legítimos de seguridad y mantener condiciones previsibles para el comercio y la cooperación científica.

Otro aspecto importante es la transparencia de los procedimientos. La definición de las categorías de productos restringidos, los requisitos de licencia y los mecanismos de revisión puede contribuir a reducir la incertidumbre para las empresas y los centros de investigación. Asimismo, la existencia de procedimientos claros para solicitar autorizaciones, revisar decisiones y resolver controversias ayuda a diferenciar las restricciones específicas de las prohibiciones generales.

La gobernanza global también debe considerar los efectos sobre terceros países. Las economías que no participan directamente en una disputa pueden experimentar dificultades para adquirir equipos, mantener operaciones comerciales o acceder a tecnologías de las que dependen sus procesos de desarrollo. Esta situación es particularmente relevante para los países con menor capacidad de negociación internacional y limitada disponibilidad de proveedores alternativos.

Desde esta perspectiva, la coordinación multilateral, el intercambio de información y la definición de criterios técnicos transparentes pueden contribuir a reducir los efectos no previstos de las restricciones. No eliminan las diferencias estratégicas entre los Estados, pero permiten establecer procedimientos para administrar sus consecuencias sobre la cooperación internacional.

Implicaciones para América Latina y Ecuador: autonomía estratégica y desarrollo tecnológico

Para América Latina, las sanciones económicas y los controles tecnológicos plantean un problema que trasciende la rivalidad entre las grandes potencias. La región participa en cadenas internacionales de valor y depende, en distintos grados, de tecnologías, maquinaria, infraestructura digital, equipos científicos y bienes industriales importados. En consecuencia, las decisiones regulatorias adoptadas por economías tecnológicamente avanzadas pueden influir en sus posibilidades de modernización productiva.

En el caso de Ecuador, el análisis debe partir de la necesidad de fortalecer las capacidades nacionales para identificar dependencias tecnológicas críticas, diversificar proveedores y evaluar los riesgos asociados con la interrupción del suministro de bienes esenciales. No se trata de asumir que todas las restricciones internacionales afectan directamente al país, sino de reconocer que la posición de una economía en las redes globales puede generar vulnerabilidades incluso cuando no es destinataria de una medida.

Un primer ámbito de atención corresponde a la infraestructura digital. Los servicios de computación en la nube, los sistemas de almacenamiento de datos, los programas especializados y los equipos de telecomunicaciones pueden depender de proveedores externos. Una estrategia de resiliencia requiere evaluar las condiciones contractuales, las alternativas de sustitución, la seguridad de la información y la continuidad operativa de los servicios.

Un segundo ámbito corresponde a la investigación científica y la educación superior. Las universidades y los centros de investigación utilizan equipos de laboratorio, software, bases de datos y servicios digitales procedentes de diferentes países. Por ello, las restricciones que afecten productos especializados pueden repercutir en proyectos de investigación, programas de formación y actividades de innovación. La cooperación

científica internacional y la diversificación de proveedores pueden contribuir a reducir determinados riesgos, siempre dentro de los marcos jurídicos aplicables.

Un tercer ámbito corresponde a la transformación productiva. La capacidad de incorporar tecnologías a la agricultura, la gestión del agua, la conservación ambiental, la minería responsable y la industria depende de la disponibilidad de conocimientos, infraestructura y equipamiento. El fortalecimiento de las capacidades nacionales de investigación, adaptación y mantenimiento puede mejorar la resiliencia frente a interrupciones externas.

Un cuarto ámbito corresponde a la diplomacia económica. Los países de menor tamaño relativo pueden beneficiarse de una política exterior que combine el respeto al derecho internacional, la participación en organismos multilaterales, la diversificación de relaciones comerciales y el desarrollo de capacidades nacionales para evaluar las consecuencias de las restricciones.

La autonomía estratégica no debe confundirse con el aislamiento. La cooperación internacional continúa siendo importante para acceder a conocimientos, financiar proyectos y participar en redes de innovación. La cuestión central consiste en evitar dependencias excesivas en ámbitos críticos y desarrollar alternativas que permitan mantener la continuidad de las actividades esenciales.

Para Ecuador, este enfoque puede traducirse en una agenda de trabajo que incluya la identificación de tecnologías críticas, el fortalecimiento de la formación científica, la promoción de acuerdos de cooperación tecnológica, el desarrollo de capacidades de ciberseguridad y la evaluación periódica de los riesgos asociados con proveedores concentrados en una sola jurisdicción.

En términos geopolíticos, la capacidad de un país para participar en las negociaciones tecnológicas depende no solamente de su tamaño económico, sino también de la calidad de sus instituciones, la formación de su capital humano, la articulación entre universidades y empresas y su capacidad para formular políticas públicas basadas en evidencia.

Perspectivas estratégicas para las Relaciones Internacionales 6.0

El análisis de las sanciones económicas, los controles de exportación y las restricciones a la transferencia tecnológica permite identificar varias transformaciones en la naturaleza del poder internacional.

En primer lugar, el poder se relaciona cada vez más con el control de infraestructuras y redes críticas. Las capacidades financieras, logísticas, digitales e industriales pueden proporcionar instrumentos de presión que complementan los mecanismos diplomáticos y militares tradicionales. La centralidad de una red puede otorgar ventajas estratégicas, pero también genera incentivos para que otros actores desarrollen alternativas.

En segundo lugar, la seguridad económica se ha convertido en una dimensión importante de la planificación estatal. Los gobiernos no evalúan únicamente la rentabilidad de los intercambios, sino también la continuidad del suministro, la concentración de proveedores y la disponibilidad de capacidades nacionales para sustituir tecnologías críticas.

En tercer lugar, la innovación tecnológica se encuentra estrechamente vinculada con la competencia internacional. La investigación científica, la propiedad intelectual, la fabricación de componentes avanzados y la formación de especialistas influyen en las posibilidades de desarrollo económico y en la capacidad de los Estados para preservar sus intereses estratégicos.

En cuarto lugar, la interdependencia produce resultados contradictorios. Puede favorecer el crecimiento, la cooperación y la difusión del conocimiento, pero también puede convertirse en una fuente de vulnerabilidad cuando determinados actores controlan puntos de acceso difíciles de sustituir. La interpretación de Farrell y Newman (2019) resulta especialmente útil para comprender esta dualidad.

En quinto lugar, la legitimidad y la previsibilidad de las restricciones adquieren importancia para la gobernanza global. Las medidas destinadas a proteger la seguridad deben analizarse considerando sus fundamentos jurídicos, sus objetivos explícitos, sus efectos económicos y sus consecuencias para terceros actores. La claridad normativa y la cooperación internacional pueden contribuir a reducir la incertidumbre, aunque no eliminen las diferencias estratégicas entre los Estados.

Finalmente, las restricciones tecnológicas plantean una cuestión de largo plazo: la relación entre el poder de controlar tecnologías existentes y la capacidad de crear nuevas alternativas. Un Estado puede utilizar sus ventajas actuales para limitar el acceso de otros actores, pero las respuestas de adaptación, sustitución e innovación pueden modificar las relaciones de dependencia. Por ello, el poder tecnológico no es estático; se encuentra sujeto a procesos de aprendizaje, inversión, competencia y reorganización industrial.

3.5 Comercio digital y flujos transfronterizos de datos: apertura, regulación y soberanía

3.5.1. El comercio digital como dimensión estructural de las relaciones internacionales

La transformación digital de la economía mundial ha modificado profundamente las condiciones en las que se producen, intercambian y consumen bienes y servicios. El comercio internacional ya no depende exclusivamente del desplazamiento físico de mercancías, la prestación presencial de servicios o la circulación de capital financiero. Una proporción creciente de las actividades económicas se organiza mediante plataformas digitales, servicios de computación en la nube, sistemas automatizados de gestión, redes de telecomunicaciones y mecanismos de intercambio de datos que conectan a empresas, gobiernos y consumidores situados en diferentes jurisdicciones.

Esta transformación ha convertido a los datos en un recurso estratégico para la producción de valor, la innovación y la competencia internacional. La información generada por las transacciones comerciales, las operaciones logísticas, las actividades industriales y el comportamiento de los consumidores permite optimizar procesos, anticipar demandas, identificar patrones y desarrollar nuevos productos. En consecuencia, el control de los datos y de las infraestructuras que permiten procesarlos constituye una dimensión relevante del poder económico contemporáneo.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2019) señala que los flujos internacionales de datos facilitan el comercio de bienes y servicios, la coordinación de las cadenas globales de valor, la investigación y el desarrollo, y la prestación de servicios digitales. Su importancia no se limita a las empresas tecnológicas:

las actividades manufactureras, agrícolas, financieras, educativas y sanitarias dependen cada vez más de la circulación de información entre organizaciones y territorios.

Desde la perspectiva de las relaciones internacionales, el comercio digital puede entenderse como un espacio en el que convergen la liberalización económica, la competencia empresarial, la protección de derechos, la seguridad nacional y la soberanía regulatoria. Los Estados deben decidir cómo facilitar los intercambios digitales y, al mismo tiempo, cómo proteger la privacidad, la seguridad de sus infraestructuras y los intereses de sus ciudadanos.

Esta tensión adquiere especial importancia porque los datos pueden circular a través de redes distribuidas, mientras que las leyes se aplican dentro de jurisdicciones concretas. Una empresa puede tener su sede en un país, almacenar información en servidores ubicados en otro y prestar servicios a usuarios de múltiples regiones. En tales circunstancias, determinar qué legislación se aplica, quién puede acceder a los datos y qué autoridad tiene competencia para supervisarlos se convierte en un problema jurídico y geopolítico.

Lynn (2010), desde una perspectiva crítica sobre la globalización económica, advierte que la organización internacional de las cadenas productivas puede generar relaciones de dependencia que no se explican únicamente por el volumen del comercio. Esta perspectiva resulta pertinente para el entorno digital: la participación de un país en los intercambios internacionales no garantiza que controle las plataformas, los estándares, la infraestructura o los conocimientos que permiten capturar la mayor parte del valor generado.

Por consiguiente, el comercio digital no debe interpretarse simplemente como una extensión electrónica del comercio tradicional. Representa una reorganización de las relaciones económicas internacionales en la que la infraestructura digital, los datos, los algoritmos y las capacidades de procesamiento se convierten en factores de competitividad y fuentes de poder.

3.5.2. Los flujos transfronterizos de datos y la economía basada en información

Los flujos transfronterizos de datos comprenden la transferencia, el acceso, el procesamiento y el almacenamiento de información a través de fronteras nacionales.

Estos movimientos permiten que una organización administre operaciones internacionales, que una plataforma digital preste servicios a usuarios ubicados en distintos países y que una institución científica participe en proyectos de investigación colaborativa.

Su importancia se explica por la posibilidad de separar geográficamente las distintas etapas de una actividad económica. El diseño de un producto puede realizarse en un país, el procesamiento de datos en otro y la atención al cliente desde una tercera jurisdicción. Esta distribución permite aprovechar diferencias de costos, capacidades profesionales, infraestructura y especialización productiva.

Goldfarb y Tucker (2019) explican que la digitalización reduce determinados costos asociados con la búsqueda de información, la replicación de contenidos, el transporte de datos y la verificación de transacciones. Estas reducciones modifican los incentivos económicos y permiten desarrollar nuevos modelos de negocio. No obstante, la digitalización también plantea desafíos relacionados con la privacidad, el poder de mercado y la distribución de los beneficios generados por las tecnologías.

En el comercio internacional, los datos cumplen varias funciones simultáneas. En primer lugar, constituyen un insumo para producir bienes y servicios digitales. En segundo lugar, permiten coordinar actividades productivas distribuidas entre diferentes países. En tercer lugar, facilitan la personalización de productos, la gestión de riesgos y la automatización de decisiones. Finalmente, pueden convertirse en activos económicos cuando se integran con capacidades analíticas, algoritmos y conocimiento especializado.

Sin embargo, los datos no generan valor de manera automática. Su aprovechamiento depende de la calidad de la información, de la disponibilidad de infraestructura, de las capacidades humanas para interpretarla y de la posibilidad de incorporarla a procesos productivos. La acumulación de grandes volúmenes de datos sin mecanismos adecuados de organización, seguridad y análisis no garantiza ventajas competitivas.

La diferencia entre generar información y controlar los medios para transformarla en valor constituye una de las principales asimetrías de la economía digital. Una sociedad puede producir enormes cantidades de datos mediante sus actividades comerciales, científicas y cotidianas, mientras que las plataformas que los procesan, clasifican y

monetizan pueden estar domiciliadas en otras jurisdicciones. De esta manera, la creación de información y la apropiación de sus beneficios económicos pueden producirse en territorios diferentes.

La OCDE (2019) destaca la importancia de los flujos internacionales de datos para la productividad y la participación en las cadenas globales de valor. No obstante, también reconoce que la regulación de estos flujos debe considerar objetivos legítimos de política pública, incluidos la protección de datos personales, la seguridad y la confianza en los servicios digitales.

En consecuencia, el desafío de la gobernanza digital no consiste en maximizar indiscriminadamente la circulación de información, sino en establecer condiciones que permitan aprovechar sus beneficios económicos sin ignorar los derechos, los riesgos y las diferencias de capacidad entre los actores participantes.

3.5.3. Apertura digital y liberalización del comercio electrónico

La apertura digital se refiere a las condiciones que permiten la circulación internacional de información y la prestación transfronteriza de servicios mediante redes digitales. En el ámbito comercial, comprende cuestiones como la no discriminación en las transacciones electrónicas, la facilitación del comercio sin papel, la validez de documentos electrónicos, la interoperabilidad de sistemas y el tratamiento regulatorio de los datos.

La liberalización del comercio digital puede reducir barreras de entrada para empresas que antes necesitaban establecer una presencia física en mercados extranjeros. Una empresa pequeña puede ofrecer servicios de diseño, programación, asesoría, educación o análisis de datos a clientes internacionales sin disponer de oficinas en cada país. Esta posibilidad amplía los mercados potenciales y facilita la participación de determinados emprendimientos en la economía mundial.

Sin embargo, las oportunidades no se distribuyen de forma uniforme. Las empresas requieren conectividad confiable, medios de pago accesibles, capacidades lingüísticas, conocimientos regulatorios y mecanismos de protección frente al fraude. La ausencia de estas condiciones puede limitar la participación de organizaciones de menor tamaño y reforzar las ventajas de las compañías que ya disponen de infraestructura y redes internacionales.

La Organización Mundial del Comercio (OMC) ha incorporado el comercio electrónico a las negociaciones comerciales internacionales mediante debates sobre la circulación de información, la protección de los consumidores, la autenticación electrónica y otras cuestiones relacionadas con el comercio digital. Estas negociaciones reflejan las diferencias entre los países respecto del grado de apertura deseable y de la capacidad de los gobiernos para regular los mercados digitales.

Burri (2017) sostiene que la regulación internacional del comercio electrónico plantea dificultades porque las normas comerciales tradicionales no fueron diseñadas para abordar todas las características de la economía digital. Las diferencias entre los sistemas jurídicos, las preocupaciones sobre privacidad y las políticas industriales generan tensiones entre la liberalización comercial y el margen de actuación regulatoria de los Estados.

Por ello, la apertura digital no debe considerarse un objetivo aislado de las demás políticas públicas. La eliminación de barreras puede facilitar el comercio, pero sus resultados dependen de la capacidad de las empresas nacionales para competir y de la existencia de instituciones que protejan a los consumidores y promuevan condiciones de competencia.

Desde la perspectiva geopolítica, los acuerdos internacionales sobre comercio digital también influyen en la definición de estándares. Los países y bloques económicos que participan activamente en la elaboración de reglas pueden favorecer determinadas prácticas de interoperabilidad, protección de datos y contratación electrónica. Las economías que carecen de capacidad negociadora pueden terminar adoptando normas desarrolladas en otros contextos, incluso cuando sus condiciones productivas e institucionales son diferentes.

La apertura digital, por tanto, combina oportunidades de integración económica con una disputa sobre quién define las reglas de participación en los mercados digitales.

3.5.4. Soberanía digital y territorialidad de los datos

La soberanía digital se refiere a la capacidad de un Estado, una sociedad o una organización para establecer condiciones sobre el uso de las tecnologías digitales, la gestión de la información, la protección de los datos y el funcionamiento de las infraestructuras de las que depende. Aunque el concepto admite diferentes

interpretaciones, en las relaciones internacionales se vincula con la autonomía regulatoria, la seguridad de la información y la capacidad de participar en la economía digital sin depender completamente de decisiones adoptadas por actores externos.

La soberanía digital no debe confundirse con la propiedad exclusiva de todos los datos generados dentro de un territorio. Tampoco supone necesariamente que toda la información deba almacenarse en servidores nacionales. Su alcance comprende cuestiones más amplias: quién puede acceder a los datos, bajo qué condiciones pueden transferirse, qué autoridades pueden solicitar información, qué mecanismos protegen a los titulares y qué capacidad posee el país para mantener sus servicios esenciales cuando se producen interrupciones externas.

La territorialidad de los datos constituye uno de los principales puntos de tensión. Los Estados aplican sus leyes dentro de determinados marcos jurisdiccionales, pero los servicios digitales operan mediante redes que atraviesan fronteras. Por consiguiente, la ubicación física de un servidor, el domicilio de la empresa responsable, la residencia de los usuarios y el lugar donde se procesa la información pueden corresponder a jurisdicciones diferentes.

Este fenómeno introduce desafíos para la protección de datos personales y para la cooperación entre autoridades. Una transferencia internacional puede facilitar una operación comercial legítima, pero también puede generar riesgos cuando el país receptor no ofrece garantías suficientes o cuando existen diferencias entre los mecanismos de supervisión y reparación.

La OCDE y la Organización Mundial del Comercio (2025) examinan precisamente la tensión entre apertura y regulación de los flujos internacionales de datos. Su estudio identifica los desafíos que plantean la privacidad, la ciberseguridad, la seguridad nacional y la fragmentación regulatoria, y analiza las consecuencias económicas de las restricciones y de los requisitos de localización de datos.

La localización de datos consiste en exigir que determinadas categorías de información se almacenen o procesen dentro de un territorio nacional. Esta política puede responder a objetivos legítimos, como facilitar la supervisión, proteger información sensible o garantizar la continuidad de determinados servicios. Sin embargo, sus efectos dependen

de su diseño y alcance. Si se aplica indiscriminadamente, puede elevar los costos empresariales, reducir las posibilidades de utilizar infraestructura especializada y dificultar la participación de empresas pequeñas en mercados internacionales.

La soberanía digital, por tanto, exige encontrar un equilibrio entre autonomía y cooperación. Un Estado necesita proteger la información y mantener capacidad de decisión sobre sus infraestructuras, pero también requiere participar en redes internacionales que facilitan la innovación, el comercio y la investigación científica.

El modelo europeo de protección de datos

La Unión Europea ofrece un ejemplo relevante de cómo la protección de los derechos fundamentales puede convertirse en una dimensión de la regulación económica internacional. El Reglamento General de Protección de Datos (RGPD), adoptado en 2016 y aplicable desde el 25 de mayo de 2018, establece obligaciones para el tratamiento de datos personales y condiciones específicas para determinadas transferencias hacia terceros países (Parlamento Europeo y Consejo de la Unión Europea, 2016).

El modelo europeo muestra que la circulación internacional de información no depende únicamente de la infraestructura técnica disponible. También está condicionada por garantías jurídicas, responsabilidades empresariales y mecanismos institucionales de protección.

Las reglas europeas pueden influir en empresas extranjeras que ofrecen servicios a personas dentro de la Unión Europea o que procesan información personal en circunstancias comprendidas por el reglamento. De este modo, una norma regional puede adquirir efectos económicos extraterritoriales en la práctica, al incentivar a las empresas internacionales a adaptar sus sistemas de cumplimiento para operar en ese mercado.

Bradford (2020) utiliza el concepto de efecto Bruselas para explicar cómo la dimensión del mercado europeo y su capacidad regulatoria pueden favorecer la difusión internacional de determinadas normas. Esta influencia no significa que todos los países adopten automáticamente las mismas disposiciones, sino que las empresas con presencia global pueden encontrar conveniente armonizar algunos procedimientos con los requisitos de una jurisdicción importante.

Desde la geopolítica digital, el ejemplo europeo permite identificar una forma de poder distinta del control directo de recursos naturales o de infraestructuras. La capacidad de establecer estándares regulatorios también puede generar influencia internacional, especialmente cuando las empresas consideran que adaptar sus sistemas a una norma facilita el acceso a mercados relevantes.

3.5.5. Fragmentación digital y competencia entre modelos regulatorios

La fragmentación digital se produce cuando las diferencias entre marcos regulatorios, estándares técnicos, infraestructuras y políticas de seguridad dificultan la interoperabilidad de los sistemas internacionales. Puede manifestarse mediante restricciones a la circulación de datos, requisitos divergentes de localización, incompatibilidades técnicas o limitaciones al acceso a determinadas plataformas.

La fragmentación no es necesariamente absoluta. Los países pueden compartir algunos estándares y mantener diferencias en otros ámbitos. Sin embargo, cuando las divergencias regulatorias se acumulan, las empresas deben asumir costos adicionales para adaptar sus sistemas a distintos mercados y cumplir obligaciones potencialmente contradictorias.

La OCDE y la OMC (2025) advierten que la fragmentación de los regímenes de regulación de datos puede tener consecuencias económicas importantes. Su análisis presenta escenarios en los que la fragmentación completa se asocia con pérdidas considerables de producción mundial, mientras que los regímenes abiertos acompañados de salvaguardas pueden generar beneficios económicos. Estas estimaciones son resultados de escenarios modelizados y no deben interpretarse como pronósticos inevitables.

La fragmentación también puede adquirir una dimensión geopolítica cuando los Estados consideran que la dependencia de plataformas, redes o proveedores extranjeros representa un riesgo para su seguridad. En tales circunstancias, las políticas de diversificación, sustitución tecnológica o control de infraestructuras pueden responder a preocupaciones estratégicas, además de objetivos comerciales.

No obstante, la creación de ecosistemas digitales separados puede reducir las oportunidades de cooperación científica y aumentar los costos de acceso a tecnologías avanzadas. Para las economías pequeñas, mantener sistemas completamente autónomos

puede resultar especialmente costoso, porque limita la posibilidad de aprovechar economías de escala y servicios especializados disponibles internacionalmente.

La gobernanza global necesita, por ello, mecanismos que faciliten la interoperabilidad jurídica y técnica. Entre ellos se encuentran los acuerdos sobre protección de datos, los estándares de seguridad, los procedimientos contractuales para transferencias internacionales y la cooperación entre autoridades regulatorias.

El objetivo no consiste en eliminar las diferencias nacionales, sino en permitir que los sistemas puedan relacionarse bajo condiciones transparentes, previsibles y compatibles con la protección de derechos.

3.5.6. Perspectivas estratégicas para América Latina y Ecuador

América Latina participa en la economía digital mediante el comercio electrónico, los servicios profesionales, la administración pública digital, la investigación científica y el uso de plataformas internacionales. Sin embargo, la capacidad de aprovechar estas oportunidades depende de la infraestructura de conectividad, la formación profesional, la seguridad digital y el desarrollo de empresas capaces de crear soluciones tecnológicas propias.

Para Ecuador, la cuestión de la soberanía digital puede abordarse desde tres dimensiones complementarias.

La primera es la protección jurídica de la información. La existencia de normas nacionales sobre protección de datos debe acompañarse de capacidades institucionales para supervisar su cumplimiento, orientar a las organizaciones y facilitar transferencias internacionales bajo condiciones apropiadas.

La segunda es la resiliencia de las infraestructuras. La continuidad de los servicios públicos, educativos, financieros y productivos requiere evaluar las dependencias de proveedores externos, establecer mecanismos de respaldo y desarrollar procedimientos para responder ante incidentes tecnológicos.

La tercera es la creación de valor mediante el conocimiento. La participación en el comercio digital no debería limitarse a consumir plataformas extranjeras. También puede incluir el desarrollo de software, servicios de análisis de datos, soluciones para la gestión

ambiental, aplicaciones agrícolas y herramientas digitales adaptadas a las necesidades nacionales.

En este último ámbito, las universidades pueden desempeñar un papel relevante mediante proyectos de investigación, transferencia de conocimientos y cooperación con empresas e instituciones públicas. La soberanía digital no depende únicamente de adquirir infraestructura: también requiere profesionales capaces de diseñar, mantener, evaluar y mejorar los sistemas utilizados.

En conclusión, el comercio digital plantea una relación compleja entre apertura y autonomía. Una política exclusivamente orientada a la apertura puede ignorar las vulnerabilidades derivadas de la concentración tecnológica; una estrategia centrada únicamente en el control territorial puede elevar costos y limitar la cooperación. El desafío consiste en construir una gobernanza digital que combine la circulación confiable de datos, la protección de derechos, la competencia económica y el desarrollo de capacidades nacionales.

3.6 Infraestructuras de pago, monedas digitales y competencia monetaria internacional

3.6.1. La infraestructura de pagos como fuente de poder geopolítico

El sistema monetario internacional constituye una de las estructuras fundamentales de las relaciones económicas entre los Estados. Mediante él se realizan pagos comerciales, transferencias financieras, inversiones, operaciones de crédito y movimientos de capital. Su funcionamiento depende de monedas utilizadas internacionalmente, bancos corresponsales, sistemas de compensación y liquidación, redes de mensajería financiera y mecanismos de supervisión regulatoria.

Durante décadas, la centralidad del dólar estadounidense ha otorgado a Estados Unidos una posición destacada en los mercados financieros internacionales. Esta centralidad no se explica exclusivamente por la dimensión de su economía, sino también por la profundidad de sus mercados financieros, la disponibilidad de activos denominados en dólares, la confianza institucional, la liquidez y la utilización de la moneda en contratos y transacciones internacionales.

Eichengreen (2011) muestra que la evolución de las monedas internacionales está vinculada con la historia del sistema financiero, las transformaciones económicas y las decisiones de los actores públicos y privados. La posición internacional de una moneda no depende de una única característica, sino de la interacción entre mercados, instituciones, redes comerciales y expectativas de los participantes.

Desde una perspectiva geopolítica, las infraestructuras de pago son relevantes porque determinan cómo se transmite una orden de pago, qué instituciones participan en la operación, qué reglas se aplican y qué mecanismos permiten liquidar las obligaciones. En consecuencia, el control o la influencia sobre determinados componentes de estas infraestructuras puede proporcionar capacidad de supervisión y, bajo ciertas condiciones, de presión económica.

Es importante distinguir, sin embargo, entre los sistemas de mensajería financiera, los sistemas de pago y las infraestructuras de compensación y liquidación. No son equivalentes. Una red de mensajería transmite información sobre las operaciones, pero no necesariamente mantiene cuentas ni liquida por sí misma los pagos. Los sistemas de pago y liquidación cumplen funciones diferentes, aunque pueden interactuar con las redes de mensajería y con los bancos participantes.

Esta distinción es esencial para analizar las sanciones financieras. La exclusión de una institución de una red de mensajería puede dificultar sus operaciones internacionales, pero sus efectos dependen de las relaciones bancarias, las alternativas disponibles y las demás restricciones que se apliquen. No implica automáticamente que toda transacción vinculada con el país afectado quede imposibilitada.

Farrell y Newman (2019) permiten interpretar estas infraestructuras como redes en las que la centralidad puede transformarse en poder estratégico. Los actores que ocupan posiciones importantes pueden disponer de ventajas informativas y regulatorias, mientras que los participantes periféricos pueden depender de canales que no controlan directamente.

La infraestructura de pagos, por tanto, no es solamente un componente técnico de la economía. También forma parte de la arquitectura institucional y estratégica que sostiene las relaciones monetarias internacionales.

3.6.2. El dólar y la estructura monetaria internacional

La posición internacional del dólar se ha construido mediante procesos históricos que incluyen la expansión de los mercados financieros estadounidenses, la utilización de la moneda en el comercio internacional, la profundidad de los mercados de deuda y la presencia de activos líquidos considerados importantes para la gestión de reservas.

El uso de una moneda internacional genera efectos de red. Cuanto mayor es el número de empresas, bancos y gobiernos que la utilizan, más sencillo puede resultar encontrar contrapartes, realizar operaciones y acceder a instrumentos financieros denominados en esa moneda. Estos efectos contribuyen a la persistencia de su utilización, incluso cuando otros Estados intentan promover alternativas.

La centralidad del dólar también influye en la transmisión internacional de las decisiones monetarias estadounidenses. Los cambios en las tasas de interés, las condiciones de liquidez y las expectativas de los mercados financieros pueden afectar los costos de financiación, los flujos de capital y las condiciones de endeudamiento de otras economías.

No obstante, la influencia monetaria internacional no debe confundirse con un control absoluto sobre todas las transacciones. Las empresas y los gobiernos utilizan diferentes monedas según sus necesidades comerciales, las condiciones de los mercados y la disponibilidad de instrumentos financieros.

La posición del dólar puede generar ventajas para Estados Unidos, pero también implica responsabilidades y costos relacionados con la estabilidad de los mercados, la confianza de los participantes y las consecuencias internacionales de las decisiones de política monetaria.

En términos geopolíticos, la infraestructura financiera asociada al dólar puede adquirir relevancia cuando determinadas operaciones quedan sujetas a restricciones legales. Las instituciones financieras internacionales deben evaluar las obligaciones que les corresponden en virtud de las jurisdicciones aplicables, sus relaciones bancarias y las normas de cumplimiento pertinentes.

Esta situación explica por qué las decisiones regulatorias de una economía central pueden repercutir sobre empresas situadas en terceros países. Sin embargo, el alcance concreto

de tales efectos debe establecerse a partir de las disposiciones aplicables a cada operación y no únicamente de la moneda utilizada.

3.6.3. Diversificación monetaria y búsqueda de alternativas

La diversificación monetaria comprende las iniciativas destinadas a reducir la dependencia de una sola moneda o de determinadas infraestructuras de pago. Puede incluir el uso de monedas nacionales en el comercio bilateral, acuerdos de compensación, mecanismos regionales de pago y la exploración de nuevas tecnologías para transferencias internacionales.

Estas iniciativas responden a diferentes motivaciones. Algunos países buscan reducir costos de transacción; otros desean mejorar la eficiencia de los pagos transfronterizos; otros consideran importante disminuir la exposición a riesgos asociados con determinadas jurisdicciones o ampliar su autonomía financiera.

La diversificación, sin embargo, enfrenta obstáculos estructurales. Para que una moneda sea ampliamente utilizada en operaciones internacionales, los participantes necesitan mercados suficientemente líquidos, instrumentos de cobertura, mecanismos confiables de conversión y confianza en las instituciones responsables de su emisión. La mera creación de un canal alternativo no garantiza que empresas y bancos lo adopten de manera generalizada.

Eichengreen (2011) ayuda a comprender que las posiciones monetarias internacionales se mantienen mediante una combinación de condiciones económicas e institucionales. Por ello, el desarrollo de alternativas requiere algo más que decisiones diplomáticas: exige mercados, infraestructura, estabilidad y una demanda sostenida por parte de los usuarios.

La diversificación monetaria puede aumentar la capacidad de elección de los actores internacionales, pero también puede introducir costos de conversión, riesgos cambiarios y nuevas exigencias de coordinación. Sus beneficios dependen de las características de las operaciones y de la capacidad de los sistemas alternativos para garantizar eficiencia y seguridad.

En consecuencia, la competencia monetaria internacional no debe interpretarse como un proceso en el que la aparición de nuevas infraestructuras conduce necesariamente a la

sustitución inmediata de las existentes. Es posible que coexistan distintos sistemas, monedas y mecanismos de pago, con grados variables de interoperabilidad y alcance geográfico.

3.6.4. Monedas digitales de bancos centrales: innovación monetaria y soberanía financiera

Las monedas digitales de bancos centrales, conocidas internacionalmente como CBDC por su denominación en inglés (central bank digital currencies), son formas digitales de dinero emitidas como pasivo directo de un banco central. Se diferencian de los depósitos bancarios comerciales, de los criptoactivos descentralizados y de las monedas estables privadas.

Las CBDC pueden diseñarse para el uso del público general, modalidad denominada minorista, o para operaciones entre instituciones financieras, modalidad mayorista. Sus objetivos potenciales incluyen mejorar determinados mecanismos de pago, facilitar la liquidación de operaciones financieras, promover la innovación y preservar el papel del dinero de banco central en un entorno cada vez más digitalizado.

El Banco de Pagos Internacionales (BIS) ha documentado el creciente interés de los bancos centrales por explorar estas tecnologías. En su encuesta sobre 2024, publicada en 2025, informó que 85 de los 93 bancos centrales encuestados estaban explorando una CBDC minorista, mayorista o ambas. La encuesta también identificó una actividad relativamente avanzada en el estudio de aplicaciones mayoristas y una atención creciente a los posibles efectos de las monedas estables y otros criptoactivos (Illes et al., 2025).

Estos resultados deben interpretarse como evidencia de investigación y experimentación, no como prueba de que todos los países estén preparados para emitir una moneda digital ni de que exista consenso internacional sobre su diseño.

Desde la perspectiva de la soberanía monetaria, las CBDC pueden ofrecer una alternativa pública en determinados segmentos del sistema de pagos. No obstante, su utilidad depende de cuestiones como la interoperabilidad, la privacidad, la seguridad informática, la accesibilidad, la protección frente al fraude y el efecto sobre la intermediación bancaria.

Una CBDC no garantiza por sí misma la independencia financiera de un país. Si su infraestructura depende de proveedores externos, si carece de aceptación internacional o si no dispone de mecanismos adecuados de conversión y liquidación, sus beneficios pueden ser limitados. Del mismo modo, su adopción no elimina automáticamente la dependencia de otras monedas en el comercio internacional.

Por ello, las monedas digitales de bancos centrales deben evaluarse como componentes potenciales de una arquitectura de pagos más amplia, y no como soluciones automáticas a los problemas estructurales del sistema monetario internacional.

3.6.5. Monedas estables, criptoactivos y nuevos intermediarios financieros

Las monedas estables, conocidas como stablecoins, son criptoactivos diseñados para mantener un valor relativamente estable respecto de una referencia, como una moneda fiduciaria o una cesta de activos. Su funcionamiento depende del diseño del instrumento, de los mecanismos de respaldo, de los derechos de los titulares y de la confianza en la entidad o protocolo responsable.

Estas monedas pueden facilitar determinadas operaciones digitales, especialmente dentro de plataformas que integran servicios financieros y tecnologías de registro distribuido. Algunas también se utilizan en transferencias internacionales, aunque su grado de adopción y sus riesgos varían según el mercado y el marco regulatorio.

A diferencia de una CBDC, una moneda estable privada no constituye necesariamente un pasivo del banco central. Su estabilidad depende de la calidad de sus reservas, la posibilidad de reembolso, la supervisión aplicable y la capacidad del emisor para gestionar riesgos operativos y financieros.

La expansión de las monedas estables denominadas en monedas internacionales puede tener implicaciones para la soberanía monetaria de determinados países. Si hogares y empresas utilizan de manera creciente instrumentos privados vinculados a una moneda extranjera, pueden modificarse los patrones de demanda de dinero y la relación entre los sistemas de pago nacionales y las infraestructuras privadas globales.

Sin embargo, no todos los criptoactivos tienen las mismas características ni cumplen las mismas funciones. Los activos de precio fluctuante, las monedas estables y las monedas

digitales de bancos centrales deben analizarse por separado, atendiendo a sus mecanismos de emisión, respaldo, gobernanza y utilización.

La regulación de estos instrumentos requiere considerar la protección de los usuarios, la integridad financiera, los riesgos de liquidez, la prevención del lavado de activos y la interoperabilidad con los sistemas existentes. Un marco demasiado fragmentado puede dificultar la innovación legítima; una supervisión insuficiente puede exponer a los participantes a pérdidas y riesgos sistémicos.

Desde el punto de vista geopolítico, la aparición de nuevos intermediarios digitales amplía el número de actores que pueden influir en la circulación del dinero. Además de los bancos centrales y los bancos comerciales, adquieren importancia las empresas tecnológicas, los proveedores de infraestructura digital y las organizaciones que administran determinados activos o protocolos.

Esta transformación exige que la gobernanza monetaria incorpore capacidades técnicas y regulatorias capaces de evaluar tanto las innovaciones como sus implicaciones para la estabilidad y la autonomía financiera.

3.6.6. Pagos transfronterizos e interoperabilidad internacional

Los pagos transfronterizos permiten transferir fondos entre personas, empresas e instituciones situadas en distintas jurisdicciones. Son esenciales para el comercio internacional, las remesas, las inversiones y la prestación de servicios.

Sin embargo, estas operaciones pueden involucrar múltiples intermediarios, conversiones de moneda, procedimientos de cumplimiento y sistemas tecnológicos que no siempre están integrados. Como resultado, las transferencias pueden presentar costos, demoras y dificultades de seguimiento que afectan especialmente a usuarios y empresas con recursos limitados.

La interoperabilidad busca que sistemas diferentes puedan intercambiar instrucciones y completar operaciones de manera compatible. Puede desarrollarse mediante estándares técnicos comunes, acuerdos entre instituciones financieras, conexiones entre sistemas de pago o experimentos con infraestructuras digitales compartidas.

El BIS ha estudiado las relaciones entre las monedas digitales de bancos centrales y los sistemas de pago rápido, así como las posibilidades de cooperación y competencia entre ambos mecanismos (Aurazo et al., 2024). Estas investigaciones reflejan que la modernización de los pagos no depende de una tecnología única, sino de las decisiones de diseño, la coordinación institucional y las necesidades de los usuarios.

En términos internacionales, una infraestructura interoperable puede facilitar las transacciones entre países y reducir determinados costos operativos. No obstante, su implementación exige acuerdos sobre gobernanza, protección de datos, responsabilidad jurídica, estándares de seguridad y mecanismos de resolución de controversias.

La interoperabilidad tampoco elimina las diferencias entre las políticas monetarias ni los riesgos cambiarios. Una operación puede realizarse con mayor rapidez y continuar expuesta a fluctuaciones de las monedas utilizadas, a restricciones regulatorias o a problemas de liquidez.

En consecuencia, la modernización de los pagos debe evaluarse mediante una combinación de indicadores técnicos, económicos e institucionales. La rapidez de una transferencia es importante, pero también lo son su costo total, su seguridad, su trazabilidad, la protección de los usuarios y la capacidad de las autoridades para supervisar las operaciones conforme al marco jurídico aplicable.

3.6.7. Implicaciones para Ecuador y las economías de América Latina

La relación entre infraestructuras de pago, monedas digitales y competencia monetaria presenta particularidades en América Latina, donde los países poseen regímenes monetarios, estructuras financieras y niveles de desarrollo digital diferentes.

En el caso de Ecuador, la dolarización constituye un elemento central del contexto monetario. El dólar estadounidense cumple funciones fundamentales como unidad de cuenta, medio de pago y reserva de valor en la economía nacional. Esta característica condiciona las alternativas de política monetaria y hace especialmente importante la continuidad de los sistemas de pagos, la liquidez del sistema financiero y el acceso a canales internacionales confiables.

La adopción de nuevas tecnologías de pago no debe confundirse con la creación de una moneda nacional soberana ni con la posibilidad de alterar unilateralmente la naturaleza del régimen monetario. Las decisiones sobre instrumentos digitales deben analizarse de acuerdo con el marco jurídico ecuatoriano, las competencias de las autoridades y los efectos sobre la estabilidad financiera.

Para Ecuador, las oportunidades pueden encontrarse en la modernización de los pagos electrónicos, la interoperabilidad de sistemas, la mejora de las remesas y el fortalecimiento de la seguridad de las transacciones. También es importante evaluar las condiciones bajo las cuales se utilizan plataformas privadas, activos digitales y servicios financieros internacionales.

Una estrategia prudente requiere examinar los costos para los usuarios, la protección frente al fraude, la disponibilidad de mecanismos de reclamación y los riesgos de dependencia de proveedores concentrados. La innovación financiera puede facilitar el acceso a servicios, pero su utilidad depende de la capacidad institucional para supervisar los riesgos y garantizar que los usuarios comprendan las condiciones de los productos.

En el ámbito regional, la cooperación entre autoridades financieras puede contribuir a mejorar los pagos transfronterizos y facilitar operaciones comerciales. Sin embargo, la creación de infraestructuras compartidas requiere acuerdos sobre responsabilidades, estándares, supervisión y tratamiento de controversias.

Desde la perspectiva de las Relaciones Internacionales 6.0, el desafío consiste en reconocer que la infraestructura financiera forma parte de la autonomía económica de un país. La capacidad de realizar pagos seguros y eficientes, mantener acceso a mercados y proteger a los usuarios es una dimensión importante de la resiliencia nacional, aunque no

Para las economías latinoamericanas, la prioridad consiste en mejorar la eficiencia y seguridad de sus sistemas de pago, fortalecer la cooperación internacional y evaluar las innovaciones de acuerdo con sus condiciones institucionales. En Ecuador, estas decisiones deben considerar expresamente el régimen de dolarización y la necesidad de preservar la estabilidad del sistema financiero.

EDITORIAL ANDES COGNITIO

CAPÍTULO IV

GOBERNANZA GLOBAL Y SOBERANÍA DIGITAL: INSTITUCIONES, NORMAS Y RESPONSABILIDADES



CAPÍTULO IV

GOBERNANZA GLOBAL Y SOBERANÍA DIGITAL: INSTITUCIONES, NORMAS Y RESPONSABILIDADES

4.1 Gobernanza de la transformación digital: legitimidad, representación y coordinación internacional

La transformación digital constituye uno de los procesos de cambio estructural más importantes desde la Revolución Industrial. La expansión de Internet, la inteligencia artificial, la computación en la nube, las plataformas digitales y los sistemas algorítmicos está modificando simultáneamente la economía, la política, la seguridad internacional y la vida cotidiana de miles de millones de personas. No obstante, la velocidad de innovación tecnológica ha superado en muchos casos la capacidad de las instituciones nacionales e internacionales para desarrollar marcos regulatorios adecuados, generando importantes desafíos para la gobernanza global (Floridi, 2014; Schwab, 2016).

La cuestión central ya no consiste únicamente en desarrollar nuevas tecnologías, sino en determinar quién establece las reglas bajo las cuales operan, qué principios orientan su utilización y qué mecanismos garantizan su compatibilidad con los derechos humanos, la democracia y el desarrollo sostenible. Como señalan Brousseau, Marzouki y Méadel (2012), el espacio digital ha evolucionado hacia un entorno global donde múltiples actores compiten por influir en la configuración de normas, estándares e instituciones.

Desde la perspectiva de las Relaciones Internacionales 6.0, la gobernanza digital representa una dimensión fundamental del poder contemporáneo. Quienes participan en la definición de las reglas que regulan los datos, las plataformas, la inteligencia artificial y las infraestructuras digitales poseen una capacidad significativa para influir en la configuración futura del orden internacional.

4.1.1. De la regulación tecnológica a la gobernanza digital global

Durante gran parte del siglo XX, la regulación de los medios de comunicación, las telecomunicaciones y los sistemas de información estuvo asociada a marcos jurídicos nacionales. Los Estados podían ejercer control relativamente efectivo sobre los canales

de comunicación que operaban dentro de sus fronteras. Sin embargo, la arquitectura descentralizada de Internet alteró profundamente esta situación.

La expansión de redes digitales transnacionales provocó una creciente desconexión entre la territorialidad de la autoridad política y la naturaleza global de los flujos informacionales. Como resultado, numerosas decisiones relevantes para la sociedad contemporánea comenzaron a depender de actores ubicados fuera de las jurisdicciones nacionales tradicionales (Mueller, 2010).

Keohane y Nye (2012) sostienen que la creciente interdependencia global ha generado problemas cuya solución requiere mecanismos cooperativos capaces de trascender las capacidades individuales de los Estados. La gestión de los flujos de datos, la protección de la privacidad, la ciberseguridad o la inteligencia artificial constituyen ejemplos paradigmáticos de este fenómeno.

4.1.2. Legitimidad y poder en la gobernanza digital

Uno de los problemas más debatidos en la literatura contemporánea sobre gobernanza digital se relaciona con la legitimidad de los actores que participan en la formulación de reglas internacionales.

En los sistemas democráticos tradicionales, la legitimidad política deriva de mecanismos de representación, participación y rendición de cuentas. Sin embargo, gran parte de la infraestructura digital global es controlada por organizaciones privadas que ejercen funciones regulatorias de enorme impacto social sin estar sujetas necesariamente a procesos equiparables de control democrático (Suzor, 2019).

Las plataformas tecnológicas establecen normas que afectan la libertad de expresión, la circulación de información, la privacidad y la interacción social a escala global. Aunque estas reglas son formuladas por actores privados, sus efectos alcanzan dimensiones comparables a las de numerosas políticas públicas estatales.

Este escenario ha llevado a diversos autores a plantear la existencia de una crisis de legitimidad regulatoria. El problema no consiste únicamente en quién posee capacidad para regular el entorno digital, sino también en quién posee la autoridad moral y política para hacerlo.

Desde una perspectiva constructivista, la legitimidad no depende exclusivamente del poder material, sino también de la aceptación social de las normas y de las instituciones que las promueven (Wendt, 1999). Por esta razón, la gobernanza digital requiere mecanismos transparentes de participación y supervisión que fortalezcan la confianza pública en las decisiones tecnológicas.

4.1.3. Representación internacional y desigualdades estructurales

La gobernanza digital global también enfrenta importantes problemas de representación. La economía digital contemporánea presenta elevados niveles de concentración tecnológica, financiera y científica. Estados Unidos, China y, en menor medida, la Unión Europea concentran gran parte de las capacidades relacionadas con inteligencia artificial, plataformas digitales, infraestructura cloud y desarrollo de estándares tecnológicos internacionales (Castells, 2010; Lee, 2018).

Como consecuencia, numerosos países en desarrollo participan de manera limitada en los procesos donde se definen reglas fundamentales para el funcionamiento del ecosistema digital global.

Esta situación plantea interrogantes relevantes sobre la equidad del orden digital emergente. Si las normas internacionales son formuladas principalmente por actores que representan intereses particulares de determinadas regiones o potencias tecnológicas, existe el riesgo de reproducir asimetrías históricas dentro de los nuevos espacios digitales.

Autores vinculados a la economía política internacional han señalado que la gobernanza tecnológica podría convertirse en una nueva dimensión de dependencia estructural si los países periféricos continúan desempeñando exclusivamente funciones de consumo tecnológico mientras los centros de innovación concentran la capacidad normativa y productiva (Strange, 1996; Castells, 2010).

Por esta razón, diversos organismos multilaterales han enfatizado la necesidad de fortalecer la participación del Sur Global en la construcción de estándares relacionados con la inteligencia artificial, la protección de datos y la gobernanza de Internet.

4.1.4. Coordinación internacional en un mundo tecnológicamente fragmentado

La revolución digital ha generado un conjunto de desafíos que trascienden las fronteras nacionales. Los ciberataques pueden originarse en un país y afectar simultáneamente a organizaciones ubicadas en distintos continentes. Los algoritmos entrenados con datos globales producen efectos internacionales. Las plataformas operan sobre infraestructuras distribuidas en múltiples jurisdicciones.

En consecuencia, la cooperación internacional se ha convertido en una condición indispensable para gestionar de forma efectiva los riesgos asociados a la digitalización.

Sin embargo, esta necesidad de cooperación coexiste con un contexto de creciente competencia geopolítica. Farrell y Newman (2019) argumentan que las redes digitales globales se han transformado en instrumentos de poder geopolítico. Los Estados ya no buscan únicamente beneficiarse de la interdependencia tecnológica, sino también utilizarla como mecanismo de influencia y coerción internacional.

Esta tendencia ha favorecido la aparición de procesos de fragmentación digital. Estados Unidos, China, la Unión Europea, India y otras potencias emergentes impulsan marcos regulatorios diferenciados que reflejan prioridades políticas, económicas y estratégicas distintas.

Como resultado, la construcción de consensos globales se vuelve cada vez más difícil, generando tensiones permanentes entre cooperación e interés nacional.

4.1.5. Hacia una gobernanza digital sostenible

La construcción de una gobernanza digital legítima requiere equilibrar múltiples objetivos simultáneamente: innovación tecnológica, protección de derechos fundamentales, seguridad internacional, desarrollo económico e inclusión social.

Desde la perspectiva de las Relaciones Internacionales 6.0, la sostenibilidad del orden digital dependerá de la capacidad de las instituciones internacionales para generar mecanismos de coordinación que incorporen diversidad geográfica, transparencia decisional y responsabilidad compartida.

La gobernanza digital del futuro no podrá basarse exclusivamente en el liderazgo de Estados o corporaciones individuales. Su estabilidad dependerá de modelos cooperativos capaces de integrar diferentes intereses, culturas políticas y niveles de desarrollo tecnológico dentro de una arquitectura institucional legítima y adaptativa.

4.2 Soberanía digital y jurisdicción: tensiones entre autoridad estatal y redes transfronterizas

La soberanía constituye uno de los pilares fundamentales del sistema internacional moderno. Desde la Paz de Westfalia, el principio de autoridad territorial ha servido como base normativa para organizar las relaciones entre los Estados. Sin embargo, la revolución digital ha introducido desafíos sin precedentes para esta concepción tradicional.

La globalización de los flujos de información, la expansión de las plataformas digitales y la creciente dependencia de infraestructuras tecnológicas transnacionales han reducido la capacidad de los gobiernos para controlar plenamente actividades que ocurren dentro de sus fronteras. Como resultado, la noción clásica de soberanía está experimentando un proceso de reinterpretación que ha dado origen al concepto de soberanía digital.

4.2.1. La evolución del concepto de soberanía en la era digital

La soberanía moderna fue concebida como la autoridad suprema que un Estado ejerce sobre una población y un territorio determinados (Krasner, 1999). Durante siglos, este principio proporcionó un marco relativamente claro para delimitar competencias políticas y jurisdiccionales.

No obstante, la digitalización ha introducido dinámicas que desafían los fundamentos territoriales de dicha concepción. Los datos se almacenan simultáneamente en múltiples países, las plataformas operan a escala planetaria y las comunicaciones digitales atraviesan fronteras de manera instantánea.

En este contexto, la soberanía ya no puede interpretarse exclusivamente como control territorial. Cada vez más gobiernos consideran necesario desarrollar capacidades que les permitan ejercer cierto grado de control sobre los recursos digitales estratégicos que afectan a sus sociedades.

4.2.2. Datos, jurisdicción y conflictos normativos

Uno de los aspectos más complejos de la soberanía digital se relaciona con la jurisdicción sobre los datos.

Las actividades digitales suelen involucrar simultáneamente múltiples territorios. Un usuario puede residir en un país, utilizar una plataforma registrada en otro Estado y almacenar su información en servidores ubicados en varias regiones del mundo.

Esta situación genera conflictos legales significativos respecto a:

- Protección de datos.
- Fiscalidad digital.
- Responsabilidad civil.
- Delitos informáticos.
- Acceso gubernamental a información estratégica.

La extraterritorialidad regulatoria se ha convertido en una característica cada vez más frecuente de la gobernanza digital. Normativas como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea producen efectos más allá de las fronteras europeas, influyendo sobre empresas y usuarios ubicados en diferentes regiones del mundo (Bradford, 2020).

4.2.3. Competencia entre modelos de soberanía digital

La gobernanza contemporánea del entorno digital está marcada por la coexistencia de diferentes modelos regulatorios.

El enfoque estadounidense ha privilegiado históricamente la innovación liderada por el mercado y la libre circulación de información. Por el contrario, la Unión Europea ha enfatizado la protección de los derechos fundamentales mediante una regulación más robusta de plataformas y datos personales.

China, por su parte, ha desarrollado un modelo que combina innovación tecnológica con un fuerte control estatal sobre el ecosistema digital nacional.

Estas diferencias reflejan distintas concepciones sobre la relación entre tecnología, mercado, seguridad y autoridad política. La competencia entre dichos modelos constituye una de las principales dimensiones de la geopolítica digital contemporánea.

4.2.4. Autonomía tecnológica y resiliencia estratégica

La creciente dependencia de infraestructuras digitales extranjeras ha impulsado el desarrollo de estrategias orientadas a fortalecer la autonomía tecnológica nacional.

Estas iniciativas incluyen:

- Construcción de capacidades nacionales de computación.
- Desarrollo de ecosistemas propios de innovación.
- Impulso a industrias estratégicas.
- Protección de infraestructuras críticas.
- Formación de talento especializado.

La pandemia de COVID-19 y las tensiones geopolíticas recientes demostraron la vulnerabilidad de las cadenas globales de suministro tecnológico, reforzando la percepción de que la soberanía digital constituye también una cuestión de seguridad nacional (Farrell & Newman, 2019).

4.3 Gobernanza internacional de la inteligencia artificial: seguridad, transparencia y rendición de cuentas

La inteligencia artificial constituye posiblemente la tecnología con mayor potencial transformador de las próximas décadas. Su capacidad para automatizar procesos, generar conocimiento, optimizar decisiones y crear nuevos modelos económicos está modificando profundamente las estructuras productivas, políticas y sociales.

Sin embargo, su expansión también plantea interrogantes éticos, jurídicos y geopolíticos que trascienden las capacidades regulatorias de los Estados individuales. Por esta razón, la gobernanza internacional de la inteligencia artificial se ha convertido en una prioridad creciente para gobiernos, organismos multilaterales y centros de investigación.

4.3.1. La dimensión global de la inteligencia artificial

La inteligencia artificial posee una naturaleza inherentemente transnacional. Los algoritmos se desarrollan mediante colaboración internacional, utilizan datos provenientes de múltiples jurisdicciones y producen impactos que trascienden las fronteras estatales.

En consecuencia, los desafíos asociados con esta tecnología no pueden abordarse exclusivamente desde perspectivas nacionales.

Floridi et al. (2018) argumentan que la gobernanza de la inteligencia artificial requiere marcos internacionales capaces de promover simultáneamente innovación, protección de derechos y responsabilidad institucional.

La dificultad radica en que los Estados poseen intereses divergentes respecto de la velocidad, intensidad y alcance de la regulación tecnológica.

4.3.2. Seguridad internacional y riesgos sistémicos

Uno de los principales debates contemporáneos se relaciona con el impacto de la inteligencia artificial sobre la seguridad internacional.

La incorporación de sistemas algorítmicos en ámbitos militares, cibernéticos y de inteligencia genera oportunidades significativas para mejorar capacidades defensivas. Sin embargo, también aumenta riesgos asociados a errores automatizados, sesgos algorítmicos y escaladas involuntarias de conflictos.

Scharre (2018) advierte que el uso de sistemas autónomos en contextos militares plantea interrogantes fundamentales respecto al control humano significativo sobre decisiones críticas relacionadas con el uso de la fuerza.

Asimismo, los avances en inteligencia artificial generativa han incrementado preocupaciones relacionadas con la desinformación, los contenidos sintéticos y la manipulación cognitiva de sociedades enteras mediante campañas digitales sofisticadas.

4.3.3. Transparencia y explicabilidad algorítmica

La confianza pública en los sistemas de inteligencia artificial depende en gran medida de su capacidad para ser comprendidos, auditados y supervisados.

La transparencia algorítmica se refiere a la posibilidad de conocer cómo funcionan los modelos utilizados para producir decisiones automatizadas. Sin embargo, muchos de los sistemas más avanzados operan mediante arquitecturas complejas que dificultan la interpretación de sus resultados.

Este problema plantea desafíos particularmente relevantes cuando la inteligencia artificial se utiliza en ámbitos sensibles como:

- Administración pública.
- Justicia.
- Seguridad.
- Salud.
- Educación.

La gobernanza internacional de la IA debe abordar esta cuestión mediante mecanismos de auditoría, trazabilidad y supervisión independientes que permitan garantizar la legitimidad de los sistemas automatizados.

4.3.4. Rendición de cuentas y responsabilidad institucional

La expansión de la inteligencia artificial también obliga a reconsiderar las nociones tradicionales de responsabilidad.

Cuando una decisión automatizada produce daños, resulta necesario determinar quién debe responder jurídica y políticamente: el desarrollador, el proveedor tecnológico, la institución que utiliza el sistema o alguna combinación de estos actores.

La rendición de cuentas constituye un componente central de cualquier arquitectura de gobernanza legítima. Sin mecanismos claros de responsabilidad, las ventajas asociadas a la automatización pueden verse acompañadas por riesgos significativos para la protección de derechos y libertades fundamentales.

4.3.5. Hacia una gobernanza global de la inteligencia artificial

Diversas iniciativas internacionales reflejan el creciente reconocimiento de la necesidad de establecer principios comunes para la inteligencia artificial.

Las recomendaciones de la UNESCO, los principios de la OCDE, los debates desarrollados en Naciones Unidas y los esfuerzos regulatorios de la Unión Europea representan pasos importantes hacia la construcción de un régimen global de gobernanza tecnológica (UNESCO, 2021).

Desde la perspectiva de las Relaciones Internacionales 6.0, el futuro de la inteligencia artificial dependerá no solo de avances técnicos, sino también de la capacidad de la comunidad internacional para construir instituciones legítimas, transparentes y adaptativas que orienten su desarrollo hacia objetivos compatibles con el bienestar humano y la estabilidad global.

4.4 Protección de datos, privacidad y derechos humanos en el entorno digital

La expansión de las tecnologías digitales ha transformado profundamente la manera en que las personas interactúan, trabajan, consumen información y participan en la vida pública. Sin embargo, esta transformación también ha incrementado exponencialmente la cantidad de datos personales que son recopilados, procesados, almacenados y comercializados por gobiernos, empresas tecnológicas y múltiples organizaciones. Como consecuencia, la protección de datos y la privacidad han dejado de constituir cuestiones exclusivamente técnicas para convertirse en temas centrales de gobernanza, derechos humanos y seguridad internacional.

En el contexto de las Relaciones Internacionales 6.0, los datos representan simultáneamente un activo económico, un recurso estratégico de poder y una dimensión fundamental de la autonomía individual. Esta triple naturaleza genera tensiones permanentes entre innovación tecnológica, crecimiento económico, seguridad nacional y protección de derechos fundamentales. El desafío contemporáneo consiste en construir marcos normativos que permitan aprovechar los beneficios de la digitalización sin debilitar las libertades individuales que constituyen la base de las sociedades democráticas.

4.4.1. La transformación de la privacidad en la sociedad digital

Tradicionalmente, la privacidad fue concebida como el derecho de las personas a mantener un ámbito de vida libre de interferencias externas. Warren y Brandeis (1890) la definieron como el "derecho a ser dejado solo", formulación que influyó profundamente en el desarrollo posterior de la teoría jurídica contemporánea.

Sin embargo, la digitalización ha modificado radicalmente este concepto. Actualmente, gran parte de las actividades cotidianas generan rastros digitales que permiten reconstruir patrones de comportamiento, preferencias personales, relaciones sociales, hábitos de consumo y opiniones políticas. La utilización de dispositivos móviles, plataformas digitales, sistemas de geolocalización y redes sociales produce cantidades masivas de información que pueden ser analizadas mediante algoritmos avanzados.

Como señala Zuboff (2019), la economía digital contemporánea se caracteriza por una creciente capacidad de convertir experiencias humanas en datos susceptibles de ser procesados, comercializados y utilizados para predecir comportamientos futuros. En consecuencia, la protección de la privacidad ya no depende exclusivamente del control físico sobre la información personal, sino también de la capacidad para gobernar complejos ecosistemas digitales desarrollados a escala global.

4.4.2. Los datos personales como objeto de protección jurídica

La creciente centralidad de los datos en la economía digital ha impulsado el desarrollo de marcos regulatorios específicos orientados a proteger la información personal de los ciudadanos. Esta evolución refleja una transformación conceptual importante: los datos ya no son considerados únicamente información técnica, sino una extensión de la personalidad y de la dignidad humana.

Desde esta perspectiva, la protección de datos busca garantizar principios fundamentales como:

- Consentimiento informado.
- Transparencia en el tratamiento de información.
- Finalidad legítima del procesamiento.
- Minimización de datos.

- Seguridad de la información.
- Derecho de acceso, rectificación y eliminación.

La Unión Europea ha desempeñado un papel particularmente relevante en esta materia mediante el Reglamento General de Protección de Datos (GDPR), que se ha convertido en uno de los principales referentes normativos internacionales. Su influencia trasciende el territorio europeo y ha impulsado reformas regulatorias en múltiples regiones del mundo, demostrando que el poder normativo constituye una forma significativa de influencia internacional (Bradford, 2020).

4.4.3. Derechos humanos en el entorno digital

La transformación digital ha generado un intenso debate sobre la adaptación de los derechos humanos al entorno tecnológico contemporáneo. Aunque los principios fundamentales reconocidos por el derecho internacional continúan siendo aplicables, las tecnologías digitales han creado nuevos escenarios donde dichos derechos pueden verse fortalecidos o vulnerados.

Entre los derechos más directamente afectados destacan:

- Derecho a la privacidad.
- Libertad de expresión.
- Libertad de asociación.
- Derecho a la información.
- No discriminación.
- Debido proceso.
- Protección frente a la vigilancia arbitraria.

La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha sostenido que los mismos derechos que las personas poseen fuera de Internet deben ser protegidos igualmente en el entorno digital. Esta premisa ha adquirido particular relevancia frente a la expansión de sistemas de vigilancia masiva, reconocimiento facial, inteligencia artificial y análisis predictivo.

El desafío consiste en evitar que los avances tecnológicos generen nuevas modalidades de exclusión, discriminación o control que resulten incompatibles con los principios fundamentales del sistema internacional de derechos humanos.

4.4.4. Vigilancia, seguridad y libertades fundamentales

Uno de los principales dilemas contemporáneos surge de la tensión entre seguridad y privacidad. Los gobiernos poseen responsabilidades legítimas relacionadas con la protección de la seguridad nacional, la prevención del terrorismo, la lucha contra el crimen organizado y la defensa de infraestructuras críticas. Sin embargo, el desarrollo de tecnologías digitales amplía considerablemente las capacidades de vigilancia estatal.

Herramientas como el reconocimiento biométrico, la monitorización de comunicaciones, la inteligencia artificial aplicada al análisis de comportamiento o los sistemas de vigilancia predictiva permiten recopilar información a escalas antes inimaginables.

Diversos autores advierten que la expansión de estas capacidades puede producir efectos negativos sobre derechos fundamentales si no existen controles institucionales adecuados (Lyon, 2018). Por esta razón, la gobernanza democrática de las tecnologías de vigilancia exige incorporar principios de necesidad, proporcionalidad, transparencia y supervisión independiente.

La cuestión central no consiste en determinar si la vigilancia tecnológica debe existir, sino en establecer límites legítimos para su utilización dentro de sociedades democráticas.

4.4.5. Hacia una ciudadanía digital basada en derechos

La consolidación de la sociedad digital exige fortalecer un enfoque de ciudadanía centrado en la protección integral de derechos. Esta perspectiva reconoce que la inclusión digital no depende únicamente del acceso a tecnologías, sino también de la capacidad de las personas para ejercer derechos, comprender riesgos y participar activamente en entornos digitales cada vez más complejos.

Desde la perspectiva de las Relaciones Internacionales 6.0, la protección de datos y la privacidad no deben interpretarse únicamente como cuestiones regulatorias. Constituyen elementos esenciales para preservar la autonomía individual, la confianza institucional y la legitimidad de la transformación digital.

4.5 Regulación de plataformas: competencia económica, responsabilidad y supervisión pública

Las plataformas digitales se han convertido en algunos de los actores más influyentes de la economía y la política global. Empresas como Google, Microsoft, Amazon, Meta, Apple, Alibaba o Tencent controlan infraestructuras críticas, servicios digitales esenciales y ecosistemas que conectan a miles de millones de usuarios alrededor del mundo. Esta concentración de capacidades tecnológicas ha transformado profundamente las dinámicas tradicionales de competencia económica y autoridad regulatoria.

La creciente relevancia de estas plataformas plantea interrogantes fundamentales sobre su responsabilidad social, su influencia política y el papel que deben desempeñar los Estados en su supervisión. La cuestión central ya no es únicamente económica; se relaciona con la distribución del poder en la sociedad digital.

4.5.1. El surgimiento del poder de las plataformas digitales

La expansión de las plataformas digitales se encuentra asociada a características económicas particulares. Los efectos de red, las economías de escala y la acumulación masiva de datos favorecen dinámicas de concentración que permiten a determinadas empresas alcanzar posiciones dominantes dentro de los mercados digitales.

Srnicek (2017) sostiene que las plataformas no deben entenderse únicamente como empresas tecnológicas, sino como infraestructuras que organizan flujos de información, interacciones económicas y dinámicas sociales. Su importancia deriva precisamente de esta capacidad para intermediar relaciones entre usuarios, empresas, gobiernos y organizaciones.

A diferencia de sectores tradicionales, las plataformas digitales pueden expandir rápidamente su influencia global debido al carácter escalable de sus modelos de negocio. Como resultado, algunas de ellas poseen recursos financieros, capacidades tecnológicas e influencia social comparables a los de numerosos Estados.

4.5.2. Competencia económica y concentración de mercados

Uno de los principales desafíos regulatorios asociados con las plataformas digitales es la creciente concentración del poder económico.

Los mercados digitales suelen presentar fuertes tendencias hacia estructuras oligopólicas debido a:

- Efectos de red.
- Acumulación de datos.
- Integración vertical.
- Ventajas tecnológicas.
- Altos costos de entrada para competidores.

Estas características generan preocupaciones respecto a la posibilidad de que determinadas empresas ejerzan posiciones dominantes que limiten la innovación y reduzcan la competencia.

Diversas autoridades regulatorias han comenzado a replantear los instrumentos tradicionales de defensa de la competencia para adaptarlos a los nuevos desafíos planteados por la economía digital. El debate contemporáneo no se centra únicamente en precios o cuotas de mercado, sino también en el control de datos, infraestructura digital y ecosistemas tecnológicos.

4.5.3. La responsabilidad de las plataformas en el espacio público digital

Las plataformas han asumido funciones que históricamente estaban asociadas a instituciones públicas o medios de comunicación tradicionales. A través de algoritmos de recomendación, políticas de moderación y sistemas de publicidad digital, estas organizaciones influyen significativamente en la circulación de información y en la formación de opinión pública.

Esta realidad plantea interrogantes complejos respecto a la responsabilidad de las plataformas frente a fenómenos como:

- Desinformación.
- Discursos de odio.
- Manipulación electoral.
- Contenidos ilícitos.
- Violencia digital.

La dificultad radica en encontrar mecanismos de regulación que permitan reducir estos riesgos sin afectar indebidamente la libertad de expresión o la innovación tecnológica.

4.5.4. Supervisión pública y gobernanza democrática

La creciente influencia de las plataformas digitales ha impulsado demandas de mayor supervisión pública. Diversos gobiernos han promovido reformas regulatorias destinadas a incrementar la transparencia algorítmica, fortalecer la protección de consumidores y mejorar los mecanismos de rendición de cuentas.

No obstante, la supervisión de plataformas plantea desafíos significativos debido a la naturaleza global de estas empresas. Las decisiones adoptadas por una autoridad nacional pueden generar impactos que trascienden ampliamente sus fronteras.

Desde la perspectiva de las Relaciones Internacionales 6.0, la regulación de plataformas constituye uno de los principales escenarios donde convergen economía, tecnología, democracia y gobernanza global.

4.6 Estándares tecnológicos y poder regulatorio en la configuración de mercados internacionales

La competencia internacional ya no se desarrolla exclusivamente mediante comercio, capacidades militares o recursos naturales. En la economía digital, la capacidad para definir estándares tecnológicos constituye una fuente creciente de influencia económica y geopolítica. Los estándares determinan cómo funcionan los sistemas tecnológicos, establecen requisitos de interoperabilidad y condicionan el acceso a mercados internacionales.

Aunque suelen percibirse como cuestiones técnicas, los estándares representan instrumentos de poder capaces de moldear industrias enteras y generar ventajas competitivas significativas para quienes participan en su definición.

4.6.1. El poder invisible de los estándares

Los estándares tecnológicos establecen reglas comunes que permiten la compatibilidad entre productos, servicios y sistemas. Su importancia se extiende a sectores tan diversos

como telecomunicaciones, inteligencia artificial, ciberseguridad, comercio electrónico y computación en la nube.

Farrell y Newman (2019) argumentan que quienes controlan nodos estratégicos de la economía global poseen una capacidad creciente para ejercer influencia estructural. Los estándares representan una manifestación particularmente relevante de esta forma de poder, ya que determinan las condiciones bajo las cuales operan los mercados internacionales.

La historia económica demuestra que la definición de estándares puede proporcionar ventajas duraderas. Quienes consiguen que sus tecnologías sean adoptadas globalmente suelen beneficiarse de economías de escala, expansión de mercados y fortalecimiento de ecosistemas industriales nacionales.

4.6.2. Competencia regulatoria y liderazgo tecnológico

La transformación digital ha intensificado la competencia entre distintas potencias por influir en la arquitectura regulatoria global.

Estados Unidos, China y la Unión Europea impulsan visiones diferenciadas sobre gobernanza digital, inteligencia artificial y protección de datos. Estas diferencias no responden únicamente a cuestiones técnicas; reflejan modelos distintos de organización económica, prioridades políticas y concepciones sobre la relación entre Estado, mercado y tecnología.

Bradford (2020) sostiene que la Unión Europea ha desarrollado una forma particular de influencia internacional basada en su capacidad regulatoria. Mediante la adopción de estándares estrictos, las regulaciones europeas terminan produciendo efectos más allá de sus fronteras debido a la importancia económica de su mercado.

Esta capacidad normativa constituye una de las expresiones más relevantes del poder regulatorio contemporáneo.

4.6.3. Inteligencia artificial y estandarización internacional

La rápida expansión de la inteligencia artificial ha incrementado la importancia de los procesos de estandarización. Aspectos relacionados con seguridad, transparencia, calidad

de datos, evaluación de riesgos y auditoría algorítmica requieren marcos comunes que faciliten la cooperación internacional.

La ausencia de estándares compartidos podría favorecer la fragmentación tecnológica y dificultar la interoperabilidad entre sistemas desarrollados en diferentes países.

Por esta razón, organismos internacionales, asociaciones técnicas y gobiernos participan activamente en la elaboración de estándares destinados a fortalecer la confianza y la seguridad en el desarrollo de sistemas de inteligencia artificial.

4.6.4. Estándares como instrumento geopolítico

La competencia por definir estándares tecnológicos refleja una dimensión menos visible, pero profundamente estratégica, de la geopolítica contemporánea.

Quienes establecen las reglas técnicas del ecosistema digital influyen indirectamente sobre:

- Mercados internacionales.
- Cadenas globales de valor.
- Flujos tecnológicos.
- Procesos de innovación.
- Inversiones futuras.

Desde la perspectiva de las Relaciones Internacionales 6.0, la estandarización constituye una forma de poder estructural que permite configurar el funcionamiento de la economía global sin necesidad de recurrir a mecanismos tradicionales de coerción.

4.7 Cooperación multilateral y participación del Sur Global en la definición de reglas digitales

El carácter global de las tecnologías digitales exige respuestas colectivas capaces de trascender los límites de los Estados individuales. Sin embargo, la construcción de reglas internacionales para la economía digital ocurre en un contexto caracterizado por profundas asimetrías de poder tecnológico, económico y científico. Estas desigualdades generan interrogantes fundamentales acerca de quién participa en la definición de las reglas digitales y quién se beneficia de ellas.

La participación efectiva del Sur Global constituye uno de los principales desafíos para la legitimidad y sostenibilidad de la gobernanza digital internacional.

4.7.1. Multilateralismo en la era digital

Desde el final de la Segunda Guerra Mundial, el multilateralismo ha desempeñado un papel fundamental en la construcción del orden internacional. Organismos multilaterales permitieron coordinar políticas, reducir incertidumbres y promover cooperación en áreas de interés común.

La revolución digital ha ampliado la necesidad de estos mecanismos. Temas como inteligencia artificial, ciberseguridad, protección de datos y comercio digital requieren espacios institucionales donde los actores puedan negociar reglas compartidas.

Sin embargo, las tensiones geopolíticas contemporáneas dificultan la consolidación de consensos internacionales amplios. La creciente rivalidad tecnológica entre grandes potencias genera incentivos para promover arquitecturas digitales diferenciadas y modelos regulatorios competitivos.

4.7.2. Asimetrías tecnológicas y exclusión regulatoria

Las capacidades tecnológicas mundiales se encuentran distribuidas de manera profundamente desigual. La mayor parte de la infraestructura digital avanzada, la investigación en inteligencia artificial, los centros de datos y las plataformas globales se concentran en un número reducido de países.

Esta concentración influye también sobre la elaboración de reglas internacionales. Los actores que controlan recursos estratégicos suelen poseer mayor capacidad para participar en procesos regulatorios y promover sus intereses.

Como consecuencia, numerosos países del Sur Global enfrentan dificultades para influir en decisiones que afectan directamente su desarrollo económico y tecnológico.

4.7.3. El papel estratégico de América Latina, África y Asia emergente

Durante los próximos años, regiones como América Latina, África y partes de Asia desempeñarán un papel cada vez más relevante en la economía digital global.

Estas regiones poseen recursos estratégicos fundamentales para la transformación tecnológica, incluyendo:

- Minerales críticos.
- Mercados digitales en expansión.
- Capital humano en crecimiento.
- Potencial para energías renovables.

Sin embargo, transformar estas ventajas potenciales en capacidad de influencia internacional requiere fortalecer ecosistemas de innovación, inversión en investigación y mecanismos de cooperación regional.

4.7.4. Hacia una gobernanza digital más inclusiva

La construcción de un orden digital legítimo exige ampliar la participación de actores tradicionalmente subrepresentados.

Desde la perspectiva de las Relaciones Internacionales 6.0, una gobernanza digital sostenible debe incorporar:

- Diversidad geográfica.
- Equidad regulatoria.
- Transferencia de capacidades tecnológicas.
- Cooperación científica.
- Inclusión institucional.

La legitimidad futura de las reglas digitales dependerá en gran medida de su capacidad para reflejar intereses verdaderamente globales y no únicamente las preferencias de las principales potencias tecnológicas.

EDITORIAL ANDES COGNITIO

CAPÍTULO V

DIPLOMACÍA, CIBERSEGURIDAD Y CONFLICTOS EN ENTORNOS VIRTUALES



CAPÍTULO V

DIPLOMACIA, CIBERSEGURIDAD Y CONFLICTOS EN ENTORNOS DIGITALES

5.1 Diplomacia digital: negociación, representación y comunicación estratégica

5.1.1. Conceptualización y evolución de la diplomacia digital

La diplomacia digital puede entenderse como el conjunto de prácticas, estrategias y mecanismos mediante los cuales los Estados y otros actores internacionales utilizan las tecnologías de información y comunicación para alcanzar objetivos de política exterior, desarrollar relaciones institucionales, gestionar negociaciones y ejercer influencia en el entorno internacional. Su desarrollo está relacionado con la expansión de Internet, las redes sociales, las plataformas de comunicación virtual y los sistemas de gestión de información, que han transformado las condiciones bajo las cuales se construyen y mantienen las relaciones diplomáticas.

Tradicionalmente, la diplomacia se ha caracterizado por la interacción directa entre representantes oficiales, la negociación reservada, el intercambio de comunicaciones institucionales y la representación permanente de los intereses nacionales ante otros Estados. Sin embargo, la digitalización ha ampliado los canales mediante los cuales se desarrollan estas actividades, permitiendo una comunicación más inmediata, una mayor exposición pública de las posiciones gubernamentales y una participación más amplia de actores no estatales.

Bjola y Holmes (2015) sostienen que la diplomacia digital debe comprenderse como una transformación de las prácticas diplomáticas mediante la utilización de herramientas tecnológicas y mecanismos de colaboración virtual. Desde esta perspectiva, no representa la desaparición de la diplomacia tradicional, sino una adaptación de sus procedimientos a un entorno internacional caracterizado por la conectividad y la circulación acelerada de información.

La transformación digital de la diplomacia puede analizarse a través de tres dimensiones fundamentales:

- Dimensión institucional: comprende la incorporación de plataformas digitales en los ministerios de relaciones exteriores, embajadas, consulados y organismos internacionales para gestionar información, coordinar actividades y desarrollar procedimientos administrativos.

- Dimensión comunicacional: se relaciona con el empleo de redes sociales, portales oficiales, transmisiones virtuales y medios digitales para difundir posiciones gubernamentales, informar a la ciudadanía y proyectar la imagen internacional de un Estado.

- Dimensión estratégica: comprende la utilización de tecnologías digitales para identificar oportunidades de negociación, analizar acontecimientos internacionales, anticipar escenarios de conflicto y fortalecer la capacidad de influencia de los gobiernos.

En consecuencia, la diplomacia digital no debe limitarse al uso de redes sociales por parte de los representantes gubernamentales. Su alcance comprende la transformación de los procesos de formulación de política exterior, la gestión de relaciones internacionales, la cooperación multilateral y la construcción de mecanismos de confianza entre los actores del sistema internacional.

La evolución de esta modalidad diplomática también ha puesto de manifiesto la importancia de la denominada diplomacia híbrida, entendida como la articulación de mecanismos presenciales y virtuales. Las reuniones multilaterales, las consultas bilaterales y las negociaciones internacionales pueden desarrollarse mediante plataformas digitales o combinar encuentros presenciales con mecanismos de interacción remota. Esta modalidad adquirió particular relevancia durante la pandemia de COVID-19, cuando numerosos procesos diplomáticos tuvieron que adaptarse a las restricciones de movilidad y contacto físico (Bjola & Holmes, 2015; Bjola & Manor, 2022).

5.1.2. Transformación de los procesos de negociación internacional

La negociación constituye uno de los instrumentos esenciales de la actividad diplomática, debido a que permite conciliar intereses, gestionar desacuerdos y establecer compromisos entre Estados y organizaciones internacionales. En el entorno digital, estos procesos han

incorporado herramientas que modifican tanto las condiciones de interacción como los mecanismos de preparación, desarrollo y seguimiento de los acuerdos.

Las plataformas de videoconferencia, los sistemas de intercambio documental, las salas virtuales de negociación y los repositorios electrónicos permiten que los representantes diplomáticos mantengan comunicación permanente, incluso cuando se encuentran en diferentes regiones geográficas. Estas herramientas reducen los costos de desplazamiento, facilitan la coordinación institucional y amplían las posibilidades de participación en reuniones internacionales.

Desde una perspectiva estratégica, la digitalización de la negociación presenta varias ventajas:

a) Ampliación de los canales de comunicación. Las tecnologías digitales permiten establecer contactos inmediatos entre delegaciones diplomáticas, equipos técnicos y autoridades gubernamentales. Esta capacidad resulta especialmente importante durante situaciones de crisis internacional, cuando la rapidez de las comunicaciones puede contribuir a prevenir interpretaciones equivocadas y reducir las tensiones.

b) Acceso y procesamiento de información. Los negociadores pueden consultar documentos, estadísticas, antecedentes jurídicos, tratados internacionales y posiciones institucionales mediante repositorios digitales. Esto facilita la preparación de propuestas y permite fundamentar las decisiones con información más amplia.

c) Coordinación de equipos multidisciplinarios. Las negociaciones contemporáneas requieren la participación de especialistas en economía, derecho internacional, tecnología, medioambiente, seguridad y comercio. Las herramientas digitales permiten integrar estos conocimientos en equipos de trabajo que operan desde diferentes instituciones y países.

d) Seguimiento de compromisos internacionales. Los sistemas de gestión documental y las plataformas colaborativas facilitan el registro de acuerdos, la identificación de responsabilidades y el seguimiento de los compromisos asumidos por las partes.

No obstante, la negociación digital también presenta limitaciones. La comunicación virtual puede reducir la percepción de señales no verbales, dificultar la construcción de

confianza interpersonal y limitar los intercambios informales que tradicionalmente han acompañado a las negociaciones presenciales. Asimismo, las diferencias de conectividad, seguridad tecnológica y capacidades institucionales pueden generar desigualdades entre las delegaciones participantes.

Por consiguiente, la eficacia de la negociación digital depende no solamente de la disponibilidad de herramientas tecnológicas, sino también de las capacidades políticas, comunicacionales y técnicas de los representantes diplomáticos. La tecnología facilita el intercambio de información, pero no sustituye la capacidad de interpretar intereses, construir consensos y desarrollar relaciones de confianza.

5.1.3. Representación diplomática en los entornos digitales

La representación diplomática constituye una función fundamental de los Estados en el sistema internacional. Tradicionalmente, esta actividad se desarrolla mediante embajadas, consulados, misiones permanentes y representantes acreditados ante organismos internacionales. Sin embargo, la expansión de los espacios digitales ha generado nuevas formas de representación y presencia institucional.

Los ministerios de relaciones exteriores utilizan plataformas digitales para comunicar decisiones de política exterior, difundir información consular, establecer contactos con ciudadanos residentes en el extranjero y proyectar la identidad nacional ante públicos internacionales. De esta manera, la representación diplomática adquiere una dimensión pública más amplia, en la cual los gobiernos pueden interactuar directamente con comunidades extranjeras, organizaciones sociales, medios de comunicación y actores económicos.

Una característica relevante de este proceso es la reducción de la intermediación informativa. En el modelo tradicional, los mensajes oficiales frecuentemente circulaban mediante comunicados institucionales y medios de comunicación convencionales. En la actualidad, las autoridades pueden difundir sus posiciones directamente mediante plataformas digitales, generando espacios de comunicación inmediata y participación internacional.

Sin embargo, esta mayor exposición también implica riesgos. Las declaraciones oficiales pueden ser reproducidas fuera de su contexto, interpretadas de manera equivocada o

utilizadas para desarrollar campañas de desinformación. Por ello, la representación digital requiere coherencia institucional, protocolos de comunicación y mecanismos de verificación de información.

Además, es necesario considerar que la presencia digital de un Estado no equivale necesariamente a su capacidad efectiva de influencia. La cantidad de seguidores, visualizaciones o interacciones constituye un indicador de alcance comunicacional, pero no demuestra por sí misma que una estrategia diplomática haya alcanzado sus objetivos. Bjola (2016) señala que la evaluación de la diplomacia digital requiere considerar la naturaleza del impacto, los objetivos estratégicos y la calidad de la interacción, evitando reducir su efectividad a métricas cuantitativas.

En este sentido, la representación diplomática digital debe sustentarse en tres condiciones: legitimidad institucional, credibilidad informativa y coherencia entre el discurso público y las decisiones gubernamentales.

5.1.4. Comunicación estratégica y construcción de influencia internacional

La comunicación estratégica es un componente esencial de la diplomacia contemporánea, debido a que permite transmitir mensajes, posicionar intereses y construir percepciones sobre la actuación de los Estados. En el entorno digital, esta actividad adquiere una dimensión particularmente relevante por la velocidad de circulación de información y la capacidad de las plataformas para amplificar determinados contenidos.

La comunicación estratégica diplomática comprende la planificación y difusión de mensajes institucionales orientados a alcanzar objetivos específicos de política exterior. Entre ellos se encuentran fortalecer la imagen internacional del Estado, explicar decisiones gubernamentales, promover iniciativas multilaterales, generar confianza y contrarrestar información falsa o distorsionada.

Una estrategia de comunicación diplomática debe considerar los siguientes elementos:

1. Identificación del público objetivo: determinar si los mensajes están dirigidos a gobiernos extranjeros, organismos multilaterales, ciudadanos residentes en el exterior, comunidades académicas, organizaciones sociales o actores económicos.

2. Definición de objetivos comunicacionales: establecer qué percepción, comportamiento o resultado institucional se pretende promover.

3. Selección de canales digitales: elegir las plataformas apropiadas de acuerdo con el público, el contenido y el nivel de formalidad del mensaje.

4. Coherencia discursiva: garantizar que las comunicaciones sean consistentes con los principios de política exterior y las posiciones oficiales del Estado.

5. Evaluación del impacto: analizar el alcance, la interacción, la credibilidad y los resultados políticos o institucionales de las acciones comunicacionales.

La diplomacia digital también se relaciona con la diplomacia pública, mediante la cual los Estados buscan establecer relaciones de comunicación con sociedades extranjeras, no exclusivamente con sus gobiernos. Esta interacción permite promover valores culturales, iniciativas educativas, oportunidades comerciales, cooperación científica y posicionamientos sobre asuntos internacionales.

No obstante, las plataformas digitales también pueden convertirse en espacios de confrontación narrativa. La desinformación, las campañas coordinadas de manipulación y la difusión de contenidos falsificados pueden afectar la reputación de los Estados y debilitar la confianza entre sociedades. Por esta razón, la comunicación estratégica requiere mecanismos de verificación, transparencia y responsabilidad institucional.

En definitiva, la diplomacia digital representa una transformación de las capacidades de representación, negociación y comunicación de los Estados. Su eficacia depende de la articulación entre innovación tecnológica, conocimiento diplomático y capacidad de construir relaciones internacionales basadas en la confianza.

5.1.5. Desafíos y perspectivas de la diplomacia digital

A pesar de sus ventajas, la diplomacia digital enfrenta desafíos relacionados con la desigualdad tecnológica, la protección de información sensible, la manipulación de contenidos y la dependencia de plataformas privadas. Estas condiciones pueden generar nuevas asimetrías de poder, particularmente entre Estados que poseen infraestructuras tecnológicas avanzadas y aquellos que dependen de servicios digitales desarrollados y administrados en otras jurisdicciones.

Otro desafío corresponde a la protección de las comunicaciones diplomáticas. La interceptación de mensajes, el acceso no autorizado a documentos y la vulneración de plataformas institucionales pueden comprometer negociaciones, revelar información confidencial y afectar las relaciones bilaterales.

Asimismo, la utilización de plataformas privadas para desarrollar comunicaciones oficiales plantea interrogantes sobre la soberanía tecnológica, el tratamiento de datos y la dependencia de proveedores extranjeros.

En consecuencia, los Estados necesitan desarrollar políticas de transformación digital que contemplen capacitación especializada, infraestructura segura, protocolos de comunicación y mecanismos de cooperación internacional. La formación de diplomáticos debe incorporar conocimientos sobre ciberseguridad, análisis de información, gobernanza digital, inteligencia artificial y gestión de crisis comunicacionales.

La diplomacia digital, por tanto, no constituye únicamente una modernización instrumental de las relaciones internacionales, sino una nueva dimensión de la capacidad estatal para ejercer representación, construir consensos y participar en la gobernanza global.

5.2 Inteligencia artificial en la actividad diplomática: aplicaciones y responsabilidad de las decisiones

5.2.1. Incorporación de la inteligencia artificial en las relaciones internacionales

La inteligencia artificial (IA) constituye uno de los principales factores de transformación tecnológica del sistema internacional contemporáneo. Su desarrollo ha permitido automatizar tareas, identificar patrones en grandes volúmenes de información, generar contenidos, procesar lenguaje natural y construir modelos predictivos que apoyan diferentes actividades institucionales.

En el ámbito diplomático, estas capacidades representan oportunidades para mejorar la recopilación de información, fortalecer los procesos de análisis estratégico y optimizar la preparación de decisiones relacionadas con la política exterior. Los ministerios de relaciones exteriores y las organizaciones internacionales pueden utilizar sistemas de IA

para procesar documentos multilaterales, analizar discursos oficiales, identificar tendencias geopolíticas y examinar información procedente de diferentes fuentes.

La inteligencia artificial comprende diversas técnicas computacionales, entre ellas el aprendizaje automático (machine learning), el procesamiento del lenguaje natural, la visión artificial, los sistemas expertos y los modelos generativos. Cada una ofrece posibilidades particulares para apoyar las actividades diplomáticas.

Desde una perspectiva institucional, es importante distinguir entre la inteligencia artificial como instrumento de asistencia y la inteligencia artificial como mecanismo de automatización decisional. En el primer caso, el sistema procesa información y proporciona resultados que son examinados por especialistas humanos. En el segundo, determinados procedimientos pueden ejecutarse automáticamente de acuerdo con parámetros previamente establecidos.

Esta distinción resulta fundamental porque las decisiones de política exterior pueden producir consecuencias jurídicas, económicas, políticas y humanitarias de considerable magnitud. Por tanto, aunque los sistemas de IA pueden mejorar la eficiencia del análisis, no deben sustituir el juicio político, la responsabilidad institucional ni la deliberación humana.

La UNESCO (2021) establece que los sistemas de inteligencia artificial deben desarrollarse y utilizarse respetando los derechos humanos, la dignidad, la transparencia, la proporcionalidad y la supervisión humana. Estos principios adquieren especial relevancia en la actividad diplomática, donde la interpretación de los acontecimientos internacionales requiere considerar factores históricos, culturales, jurídicos y políticos que no siempre pueden representarse adecuadamente mediante modelos computacionales.

5.2.2. Principales aplicaciones de la inteligencia artificial en la actividad diplomática

La incorporación de la IA en las instituciones responsables de las relaciones exteriores puede analizarse a partir de diferentes áreas funcionales.

a) Análisis de información geopolítica y estratégica

Los sistemas de aprendizaje automático permiten procesar grandes cantidades de información procedente de medios de comunicación, documentos gubernamentales, bases de datos internacionales, informes económicos y publicaciones especializadas.

Mediante estas herramientas es posible identificar patrones de comportamiento, reconocer cambios en las relaciones entre países y detectar acontecimientos que podrían modificar los escenarios internacionales.

Por ejemplo, un sistema de análisis de lenguaje natural puede examinar discursos de representantes gubernamentales y clasificar sus contenidos de acuerdo con temas como seguridad, comercio, cooperación, migración o cambio climático. Posteriormente, los resultados pueden utilizarse para identificar modificaciones en las prioridades de política exterior o en las posiciones negociadoras de determinados Estados.

No obstante, estos resultados deben interpretarse considerando las limitaciones de los datos y los posibles sesgos de los algoritmos.

b) Traducción y comunicación multilingüe

La traducción automática constituye una de las aplicaciones más relevantes de la inteligencia artificial en la diplomacia. Los sistemas de procesamiento del lenguaje natural facilitan la traducción de documentos oficiales, tratados, informes técnicos y comunicaciones internacionales.

Estas herramientas contribuyen a reducir las barreras lingüísticas y facilitan la participación de delegaciones que utilizan diferentes idiomas. También permiten agilizar la preparación de documentos y mejorar la accesibilidad de la información institucional.

Sin embargo, los textos diplomáticos requieren especial precisión, debido a que determinadas expresiones jurídicas o políticas pueden tener significados diferentes según el contexto cultural y normativo. Por ello, las traducciones generadas mediante IA deben someterse a revisión humana, especialmente cuando se trata de tratados internacionales, declaraciones conjuntas y documentos oficiales.

c) Análisis predictivo y anticipación de escenarios internacionales

Los modelos predictivos pueden utilizarse para analizar variables económicas, políticas, sociales y territoriales con el propósito de identificar tendencias y construir escenarios posibles.

Entre sus aplicaciones se encuentran el análisis de riesgos de conflictos, la evaluación de vulnerabilidades económicas, la identificación de tendencias migratorias y la estimación de impactos derivados de decisiones comerciales o sanciones internacionales.

Por ejemplo, un modelo de aprendizaje automático podría integrar indicadores de inflación, desempleo, inseguridad alimentaria, desplazamiento poblacional y conflictividad social para identificar territorios con condiciones de vulnerabilidad. La información resultante permitiría orientar la cooperación internacional y fortalecer los mecanismos de prevención de crisis.

Es importante precisar que los modelos predictivos no determinan de manera infalible el comportamiento futuro de los actores internacionales. Sus resultados representan estimaciones condicionadas por la calidad de los datos, las variables consideradas y los supuestos metodológicos.

d) Automatización de procesos administrativos y consulares

La IA puede apoyar la clasificación documental, la gestión de solicitudes, la organización de archivos y la atención automatizada de consultas frecuentes.

En el ámbito consular, los asistentes virtuales pueden proporcionar información sobre requisitos de documentación, procedimientos migratorios, servicios disponibles y recomendaciones generales para ciudadanos residentes en el extranjero.

Estas aplicaciones permiten reducir tiempos administrativos y facilitar el acceso a los servicios institucionales. Sin embargo, las decisiones que afecten derechos individuales, situaciones migratorias complejas o condiciones de protección internacional deben permanecer sujetas a evaluación y responsabilidad de autoridades competentes.

e) Monitoreo de desinformación y análisis de narrativas

La inteligencia artificial puede contribuir a identificar patrones de difusión de información falsa, detectar redes de cuentas automatizadas y analizar la propagación de contenidos manipulados.

Mediante técnicas de clasificación textual y análisis de redes es posible examinar cómo determinados mensajes circulan entre diferentes comunidades digitales y qué actores participan en su amplificación.

Estas herramientas pueden apoyar las estrategias de comunicación pública y la protección de la integridad informativa. No obstante, la identificación automática de contenidos potencialmente falsos debe considerar la libertad de expresión, la pluralidad de opiniones y el riesgo de clasificar incorrectamente información legítima.

f) Apoyo a la preparación de negociaciones internacionales

Los modelos de IA pueden utilizarse para organizar antecedentes, comparar propuestas, identificar coincidencias entre documentos y sintetizar posiciones expresadas durante reuniones multilaterales.

También pueden facilitar el análisis de tratados anteriores y la identificación de cláusulas que presentan similitudes o diferencias respecto de nuevas propuestas.

En este contexto, la inteligencia artificial funciona como una herramienta de asistencia técnica que permite a los negociadores disponer de información organizada y reducir el tiempo destinado a tareas documentales.

5.2.3. Inteligencia artificial generativa y transformación de la práctica diplomática

La aparición de la inteligencia artificial generativa ha ampliado las posibilidades de aplicación tecnológica en las relaciones internacionales. Estos sistemas pueden producir textos, resumir documentos, traducir contenidos, generar presentaciones y elaborar escenarios hipotéticos a partir de instrucciones proporcionadas por los usuarios.

En las instituciones diplomáticas, su utilización puede contribuir a preparar borradores de discursos, organizar informes de coyuntura, sintetizar documentos multilaterales y desarrollar materiales de comunicación institucional.

Por ejemplo, ante una reunión internacional sobre cambio climático, un sistema generativo podría procesar documentos de organismos internacionales, identificar los principales compromisos establecidos en acuerdos anteriores y elaborar una síntesis de las posiciones de los países participantes. El equipo diplomático podría utilizar esta información como punto de partida para preparar su intervención.

Sin embargo, estos sistemas pueden producir información incorrecta, referencias inexistentes o interpretaciones que no corresponden al contexto político y jurídico de un asunto determinado. Este fenómeno, conocido como alucinación de inteligencia artificial, constituye un riesgo importante cuando los resultados se utilizan en documentos oficiales o procesos de negociación.

Por consiguiente, la incorporación de inteligencia artificial generativa debe sustentarse en procedimientos de verificación documental, protección de información confidencial y supervisión profesional.

Además, las instituciones deben evitar introducir información clasificada, datos personales o documentos reservados en plataformas que no garanticen condiciones adecuadas de seguridad y confidencialidad.

5.2.4. Responsabilidad institucional y supervisión humana de las decisiones

La utilización de inteligencia artificial en la diplomacia plantea un problema central: determinar quién asume la responsabilidad cuando una decisión apoyada por sistemas automatizados produce consecuencias negativas.

Aunque los algoritmos pueden procesar información y formular recomendaciones, no poseen responsabilidad jurídica o política equivalente a la de los funcionarios y las instituciones que los utilizan. Por ello, la responsabilidad no puede trasladarse al sistema tecnológico ni justificarse exclusivamente mediante la supuesta objetividad del algoritmo.

La UNESCO (2021) establece principios de responsabilidad, transparencia, explicabilidad y supervisión humana para garantizar que la IA se utilice de manera compatible con los derechos humanos. De forma complementaria, la OCDE (2019, actualizada en 2024) plantea que los sistemas de IA deben ser robustos, seguros, transparentes y responsables durante todo su ciclo de vida.

En el ámbito diplomático, estos principios pueden traducirse en los siguientes mecanismos:

1. Supervisión humana: las decisiones estratégicas deben permanecer bajo la autoridad de funcionarios competentes, quienes deben evaluar críticamente las recomendaciones generadas por los sistemas de IA.
2. Transparencia: las instituciones deben identificar cuándo utilizan inteligencia artificial y establecer procedimientos que permitan comprender el funcionamiento general de los sistemas empleados.
3. Trazabilidad: los procesos de análisis deben conservar registros de los datos utilizados, las versiones de los modelos, las recomendaciones producidas y las intervenciones humanas.
4. Protección de datos: los sistemas deben garantizar la confidencialidad de la información diplomática y el cumplimiento de las normas de protección de datos personales.
5. Evaluación de sesgos: es necesario identificar posibles distorsiones derivadas de datos incompletos, desactualizados o representativos de perspectivas culturales y políticas limitadas.
6. Rendición de cuentas: las instituciones deben establecer responsables para supervisar, evaluar y corregir los sistemas de inteligencia artificial.

Un aspecto particularmente importante es evitar la automatización de decisiones que puedan afectar la soberanía estatal, los derechos fundamentales o la seguridad internacional sin una evaluación humana suficiente.

Por ejemplo, si un sistema predictivo identifica a un Estado como un riesgo potencial para la seguridad regional, esta clasificación no debe convertirse automáticamente en una decisión de imponer restricciones diplomáticas o sanciones. La evaluación debe incorporar información adicional, análisis jurídico, interpretación política y valoración de las consecuencias internacionales.

5.2.5. Riesgos éticos, políticos y jurídicos de la inteligencia artificial

La incorporación de IA en las relaciones internacionales también puede generar nuevas formas de vulnerabilidad.

Uno de los principales riesgos corresponde a los sesgos algorítmicos. Cuando los sistemas son entrenados con información incompleta o culturalmente sesgada, pueden reproducir interpretaciones discriminatorias o representaciones distorsionadas de determinados países y comunidades.

Otro problema se relaciona con la concentración tecnológica. Los Estados que controlan infraestructuras de computación, semiconductores, centros de datos y modelos avanzados de IA poseen ventajas estratégicas frente a aquellos que dependen de proveedores externos. Esta situación puede profundizar las desigualdades existentes en el sistema internacional y generar nuevas formas de dependencia tecnológica.

Asimismo, la utilización de inteligencia artificial generativa para producir contenidos falsificados, simular declaraciones oficiales o manipular imágenes y grabaciones puede afectar la credibilidad de las instituciones diplomáticas.

La OCDE (2024) destaca la necesidad de fortalecer los principios de transparencia, seguridad, robustez y responsabilidad en los sistemas de inteligencia artificial. Por su parte, los principios de las Naciones Unidas para el uso ético de la IA en el sistema de la ONU incorporan la protección de derechos, la supervisión humana, la inclusión y la rendición de cuentas como condiciones fundamentales de su utilización institucional (United Nations System Chief Executives Board for Coordination, 2022).

En consecuencia, la inteligencia artificial debe incorporarse a la actividad diplomática bajo un enfoque de responsabilidad institucional, cooperación internacional y respeto al derecho internacional.

5.2.6. Gobernanza internacional de la inteligencia artificial y perspectivas diplomáticas

La gobernanza internacional de la inteligencia artificial comprende los principios, normas, instituciones y mecanismos de cooperación destinados a orientar el desarrollo y la utilización de estas tecnologías.

Debido a su naturaleza transfronteriza, la IA requiere mecanismos de coordinación entre Estados, organismos internacionales, universidades, empresas tecnológicas y organizaciones de la sociedad civil.

La Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO, adoptada en noviembre de 2021, constituye uno de los principales referentes internacionales en esta materia. Su enfoque establece que la IA debe respetar la dignidad humana, los derechos fundamentales, la diversidad cultural y la sostenibilidad, incorporando mecanismos de transparencia, responsabilidad y supervisión humana (UNESCO, 2021).

Por otra parte, la OCDE ha promovido principios internacionales orientados a desarrollar sistemas de IA innovadores, confiables y compatibles con los valores democráticos y los derechos humanos (OECD, 2019/2024).

Desde la perspectiva diplomática, estos instrumentos permiten identificar la necesidad de establecer acuerdos sobre:

- Protección internacional de datos personales.
- Transparencia y evaluación de sistemas algorítmicos.
- Prevención de usos discriminatorios de la inteligencia artificial.
- Responsabilidad por daños derivados de sistemas automatizados.
- Cooperación científica y transferencia tecnológica.
- Reducción de las brechas digitales entre países.
- Prevención de aplicaciones de IA que incrementen los riesgos para la paz y la seguridad internacionales.

En definitiva, la inteligencia artificial representa una herramienta de transformación de la actividad diplomática, pero su legitimidad depende de la capacidad de los Estados para establecer límites, responsabilidades y mecanismos de supervisión que garanticen su utilización en beneficio de la cooperación internacional.

5.3 Ciberseguridad internacional: amenazas, atribución de operaciones y protección de infraestructuras críticas

5.3.1. Conceptualización de la ciberseguridad en el sistema internacional

La ciberseguridad internacional constituye un componente esencial de la seguridad contemporánea, debido a la creciente dependencia de los Estados respecto de las tecnologías digitales para desarrollar sus actividades económicas, administrativas, militares, financieras y sociales. La expansión de las redes de comunicación, los sistemas

informáticos, los servicios en la nube y las infraestructuras conectadas ha generado un entorno de interdependencia tecnológica en el cual las vulnerabilidades de un país pueden producir consecuencias que trascienden sus fronteras.

La ciberseguridad comprende el conjunto de políticas, capacidades, procedimientos y mecanismos técnicos destinados a proteger los sistemas informáticos, las redes, los dispositivos y la información frente a accesos no autorizados, alteraciones, interrupciones y actividades maliciosas. Desde una perspectiva internacional, su alcance supera la protección de los activos tecnológicos nacionales, puesto que incorpora la prevención de conflictos, la cooperación entre Estados, la protección de infraestructuras críticas y el establecimiento de normas de comportamiento responsable en el ciberespacio.

El ciberespacio constituye un entorno complejo integrado por infraestructuras físicas, sistemas informáticos, redes de telecomunicaciones, programas, datos y usuarios. No se limita a Internet, debido a que también comprende redes privadas, sistemas industriales, dispositivos de control y plataformas que permiten el funcionamiento de servicios esenciales.

Esta característica convierte al ciberespacio en un ámbito estratégico de competencia internacional. Los Estados pueden utilizar sus capacidades tecnológicas para proteger sus intereses nacionales, desarrollar actividades de inteligencia, fortalecer sus sistemas de defensa y responder ante amenazas externas. Al mismo tiempo, actores criminales, organizaciones no estatales y grupos respaldados por gobiernos pueden utilizar estas mismas tecnologías para ejecutar operaciones que afecten la seguridad de otros países.

La Organización de las Naciones Unidas ha reconocido que las tecnologías de información y comunicación presentan implicaciones directas para la paz y la seguridad internacionales. El informe del Grupo de Expertos Gubernamentales de Naciones Unidas sobre el comportamiento responsable de los Estados en el ciberespacio destaca la importancia de desarrollar normas, mecanismos de cooperación y medidas de confianza destinadas a prevenir el uso de las tecnologías digitales de manera incompatible con la estabilidad internacional (United Nations General Assembly, 2021a).

5.3.2. Principales amenazas cibernéticas en el entorno internacional

Las amenazas cibernéticas presentan diferentes niveles de complejidad, motivaciones y consecuencias. Algunas tienen objetivos económicos, mientras que otras buscan obtener información estratégica, afectar instituciones gubernamentales, debilitar capacidades de defensa o generar inestabilidad política.

Entre las principales amenazas se encuentran las siguientes:

a) Ciberespionaje

El ciberespionaje consiste en la utilización de técnicas informáticas para obtener información confidencial sin autorización. Puede dirigirse contra instituciones gubernamentales, organismos de defensa, empresas estratégicas, centros de investigación y organizaciones internacionales.

Su finalidad puede incluir la obtención de documentos diplomáticos, información militar, investigaciones científicas, datos comerciales o comunicaciones reservadas.

Desde la perspectiva de las relaciones internacionales, el ciberespionaje representa una amenaza porque puede comprometer la confidencialidad de las negociaciones, revelar posiciones estratégicas y generar desconfianza entre los Estados.

b) Ransomware o secuestro de información

El ransomware es un tipo de programa malicioso que bloquea el acceso a sistemas o información mediante mecanismos de cifrado y exige un pago para recuperar su disponibilidad.

Los ataques de esta naturaleza pueden afectar hospitales, instituciones públicas, empresas financieras, universidades y operadores de servicios esenciales. Sus consecuencias pueden extenderse más allá de las pérdidas económicas, especialmente cuando interrumpen servicios relacionados con la salud, la energía o la administración pública.

En determinadas circunstancias, las operaciones de ransomware pueden presentar conexiones con organizaciones criminales transnacionales o estructuras que operan desde territorios distintos de aquellos donde se encuentran sus víctimas.

c) Ataques de denegación de servicio distribuido (DDoS)

Los ataques DDoS consisten en generar un volumen elevado de solicitudes hacia un servidor o una infraestructura digital con el propósito de saturar sus recursos e impedir que los usuarios legítimos accedan al servicio.

Pueden dirigirse contra portales gubernamentales, instituciones financieras, plataformas de comunicación y servicios de información. Aunque no necesariamente implican la extracción o modificación de datos, pueden producir interrupciones significativas y afectar la confianza pública en las instituciones.

d) Ataques a la cadena de suministro digital

Las cadenas de suministro tecnológicas están integradas por proveedores de hardware, software, servicios de mantenimiento, almacenamiento de datos y componentes de comunicación. Una vulnerabilidad en cualquiera de estos elementos puede comprometer a numerosas organizaciones que dependen del mismo proveedor.

Este tipo de amenaza adquiere especial relevancia porque permite que una operación maliciosa se introduzca mediante componentes o servicios aparentemente legítimos. En consecuencia, la seguridad de una institución depende no solamente de sus propios controles, sino también de las prácticas de protección de sus proveedores y socios tecnológicos.

e) Manipulación de información y operaciones de influencia

Las operaciones de influencia digital buscan modificar percepciones, debilitar la confianza institucional o generar divisiones sociales mediante la difusión coordinada de contenidos manipulados.

Estas actividades pueden incluir cuentas automatizadas, perfiles falsos, noticias engañosas, imágenes alteradas y materiales generados mediante inteligencia artificial. Cuando se desarrollan en contextos electorales, crisis diplomáticas o conflictos internacionales, pueden afectar la estabilidad política y dificultar la comunicación entre los gobiernos y sus ciudadanos.

f) Ataques contra sistemas industriales y operacionales

Los sistemas de tecnología operacional (OT) controlan procesos físicos relacionados con la producción industrial, la distribución de energía, el tratamiento de agua, las telecomunicaciones y otros servicios esenciales.

Una vulneración de estos sistemas puede ocasionar interrupciones operativas y, en determinadas circunstancias, daños materiales o riesgos para la seguridad de las personas.

La convergencia entre las tecnologías de información (IT) y las tecnologías operacionales (OT) ha incrementado la exposición de infraestructuras industriales que anteriormente funcionaban en redes más aisladas.

Estas amenazas evidencian que la ciberseguridad internacional no se limita a proteger información digital, sino que también comprende la protección de procesos físicos y servicios indispensables para el funcionamiento de las sociedades.

5.3.3. Atribución de operaciones cibernéticas: dimensiones técnicas, políticas y jurídicas

Uno de los principales desafíos de la seguridad internacional en el ciberespacio consiste en determinar quién es responsable de una operación maliciosa. A diferencia de los conflictos convencionales, en los cuales las fuerzas militares, los territorios y los medios utilizados pueden ser relativamente identificables, las operaciones cibernéticas pueden ejecutarse mediante infraestructuras distribuidas, servidores comprometidos, redes privadas y herramientas diseñadas para ocultar su origen.

La atribución cibernética es el proceso mediante el cual se identifican los actores responsables de una operación informática y se determina su posible relación con organizaciones criminales, grupos independientes o estructuras estatales.

Este proceso no consiste únicamente en identificar la dirección IP desde la cual se originó una conexión. Requiere integrar evidencias técnicas, información de inteligencia, análisis de comportamiento, antecedentes operativos y elementos de contexto político.

La atribución puede analizarse desde tres dimensiones complementarias:

a) Atribución técnica

Consiste en examinar los rastros digitales generados durante una operación. Entre los elementos analizados se encuentran:

- Direcciones IP y registros de conexión.
- Servidores utilizados para ejecutar o coordinar operaciones.
- Código malicioso y características de los programas empleados.
- Patrones de comportamiento de los atacantes.
- Herramientas, técnicas y procedimientos utilizados.
- Registros de actividad y evidencias forenses digitales.

Los especialistas comparan estos elementos con incidentes anteriores para identificar similitudes y posibles conexiones entre diferentes operaciones.

Sin embargo, los atacantes pueden utilizar servidores de terceros, redes privadas virtuales, dispositivos comprometidos y otras técnicas de ocultamiento. Por ello, una coincidencia técnica no demuestra necesariamente la identidad del responsable.

b) Atribución política y estratégica

La atribución política consiste en valorar si una operación responde a intereses de un Estado o de determinados actores políticos. Para ello, se consideran elementos como los objetivos seleccionados, los beneficios potenciales, el contexto geopolítico y los patrones de comportamiento de los posibles responsables.

Un ataque contra una institución diplomática, por ejemplo, podría tener como finalidad obtener información para una negociación, debilitar la posición internacional de un gobierno o generar incertidumbre en un proceso político.

No obstante, la existencia de un posible beneficio estratégico no constituye por sí sola una prueba de responsabilidad estatal. Es necesario contrastar las hipótesis con evidencias verificables.

c) Atribución jurídica

La atribución jurídica busca determinar si una conducta puede ser imputada a un Estado conforme a las reglas del derecho internacional.

En este ámbito es importante diferenciar entre la identificación técnica de un actor y la atribución de responsabilidad internacional a un Estado. Que una operación sea ejecutada por un grupo ubicado en determinado territorio no significa automáticamente que el gobierno de ese país sea responsable.

La atribución jurídica requiere examinar las circunstancias concretas, la naturaleza del vínculo entre el actor y el Estado y las reglas aplicables sobre responsabilidad internacional.

Esta distinción es fundamental para evitar que una acusación basada en información insuficiente produzca respuestas diplomáticas o medidas coercitivas injustificadas.

5.3.4. Dificultades y consecuencias de la atribución cibernética

La atribución de operaciones cibernéticas presenta dificultades técnicas, jurídicas y políticas que pueden afectar la estabilidad internacional.

En primer lugar, existe una asimetría entre la capacidad de ejecutar una operación y la capacidad de identificar a su responsable. Un actor con recursos relativamente limitados puede aprovechar vulnerabilidades tecnológicas para afectar organizaciones que poseen infraestructuras mucho más complejas.

En segundo lugar, los atacantes pueden utilizar mecanismos de suplantación y ocultamiento que dificultan la identificación del origen de las operaciones. También pueden comprometer dispositivos de terceros para ejecutar actividades maliciosas, generando evidencias que conducen hacia actores que no participaron directamente.

En tercer lugar, la atribución requiere cooperación internacional. Las evidencias pueden encontrarse distribuidas en diferentes jurisdicciones y depender de proveedores privados de servicios digitales. Esto genera dificultades relacionadas con el acceso a registros, la protección de datos y los procedimientos de asistencia jurídica internacional.

Egloff y Smeets (2021) destacan que la atribución pública de operaciones cibernéticas constituye una decisión estratégica compleja, debido a que requiere evaluar no solamente la evidencia técnica, sino también las circunstancias geopolíticas, los intereses de los aliados y las posibles consecuencias de hacer pública una acusación.

La atribución pública puede cumplir diferentes objetivos:

- Informar a la comunidad internacional sobre una amenaza.
- Deslegitimar las operaciones consideradas contrarias a las normas internacionales.
- Fortalecer la cooperación entre Estados afectados.
- Justificar medidas diplomáticas o económicas.
- Promover mecanismos de rendición de cuentas.
- Generar costos políticos y reputacionales para los responsables.

Sin embargo, también puede incrementar las tensiones internacionales cuando se realiza sin evidencia suficiente o cuando las partes interpretan la acusación como una provocación.

Por esta razón, la atribución debe sustentarse en procedimientos rigurosos de investigación, evaluación de evidencias y coordinación diplomática.

5.3.5. Infraestructuras críticas y seguridad nacional

Las infraestructuras críticas son los sistemas, activos y servicios cuya interrupción o destrucción puede producir consecuencias graves para la seguridad, la economía, la salud pública y el funcionamiento institucional de un país.

Su importancia radica en que constituyen la base operativa de las sociedades contemporáneas. Una interrupción prolongada de los servicios energéticos, las telecomunicaciones o el abastecimiento de agua puede generar efectos en cadena sobre diferentes sectores económicos y sociales.

Entre las principales infraestructuras críticas se encuentran:

1. Infraestructura energética. Comprende centrales de generación eléctrica, redes de transmisión y distribución, instalaciones de almacenamiento y sistemas de control

industrial. Una operación cibernética contra estos componentes puede interrumpir el suministro de energía y afectar actividades económicas y servicios esenciales.

2. Infraestructura de telecomunicaciones. Incluye redes de fibra óptica, centros de datos, sistemas de comunicación móvil, satélites y plataformas de intercambio de información. Su funcionamiento es indispensable para las comunicaciones gubernamentales, las transacciones económicas y la coordinación de servicios públicos.
3. Infraestructura financiera. Comprende bancos, sistemas de pagos, plataformas de transferencias, bolsas de valores y mecanismos de compensación financiera. Los ataques contra estos sistemas pueden generar pérdidas económicas, interrupciones operativas y desconfianza en las instituciones.
4. Infraestructura sanitaria. Incluye hospitales, laboratorios, centros de investigación, sistemas de información clínica y plataformas de gestión de servicios de salud. La vulneración de estos sistemas puede comprometer información personal y afectar la continuidad de la atención médica.
5. Infraestructura de transporte. Comprende aeropuertos, puertos marítimos, redes ferroviarias, sistemas de navegación y plataformas de gestión logística. Su vulneración puede afectar la movilidad, el comercio y la seguridad de las operaciones.
6. Infraestructura hídrica y ambiental. Incluye plantas de tratamiento de agua, sistemas de distribución, instalaciones de almacenamiento, redes de monitoreo y mecanismos de control de recursos hídricos. Una alteración de estos sistemas puede comprometer la calidad del agua, su disponibilidad y la continuidad de los servicios de abastecimiento.

La protección de las infraestructuras críticas requiere un enfoque integral que considere tanto la seguridad informática como la continuidad operativa. No es suficiente instalar herramientas de protección digital; también es necesario disponer de procedimientos de respuesta, sistemas de respaldo, protocolos de recuperación y mecanismos de coordinación interinstitucional.

5.3.6. Estrategias de protección y resiliencia de las infraestructuras críticas

La protección de infraestructuras críticas debe fundamentarse en un enfoque preventivo, integral y permanente. El Instituto Nacional de Estándares y Tecnología de Estados

Unidos (NIST) propone un marco de gestión de riesgos de ciberseguridad que permite organizar las capacidades institucionales en seis funciones interrelacionadas: gobernar, identificar, proteger, detectar, responder y recuperar (National Institute of Standards and Technology [NIST], 2024).

Estas funciones pueden aplicarse de la siguiente manera:

Tabla 4.1

Aplicación en la protección de infraestructuras críticas

Función	Aplicación en la protección de infraestructuras críticas
Gobernar	Establecer políticas, responsabilidades, protocolos y mecanismos de supervisión.
Identificar	Reconocer activos, sistemas, vulnerabilidades y riesgos potenciales.
Proteger	Implementar controles de acceso, autenticación, cifrado y medidas preventivas.
Detectar	Identificar actividades anómalas, intrusiones y posibles incidentes.
Responder	Activar procedimientos de contención, análisis y comunicación de incidentes.
Recuperar	Restablecer los servicios y fortalecer la infraestructura para evitar nuevas afectaciones.

Fuente: Elaboración propia a partir del marco NIST Cybersecurity Framework 2.0 (NIST, 2024).

La aplicación de este enfoque requiere considerar algunos mecanismos específicos:

Gestión de riesgos tecnológicos. Las instituciones deben identificar los activos más importantes, evaluar las vulnerabilidades y establecer prioridades de protección de acuerdo con el impacto potencial de una interrupción.

Segmentación de redes. La separación de los sistemas críticos de las redes administrativas y de acceso público permite limitar la propagación de incidentes informáticos.

Autenticación y control de acceso. Los mecanismos de autenticación multifactor, la gestión de privilegios y la supervisión de usuarios contribuyen a reducir los accesos no autorizados.

Monitoreo permanente. Los sistemas de detección permiten identificar comportamientos anómalos y responder oportunamente ante posibles amenazas.

Continuidad operativa. Las organizaciones deben disponer de respaldos, sistemas alternativos y procedimientos de recuperación que permitan mantener o restablecer los servicios esenciales.

Cooperación público-privada. Debido a que numerosas infraestructuras críticas son operadas por empresas privadas, su protección requiere acuerdos de colaboración, intercambio de información y mecanismos de coordinación con las autoridades nacionales.

5.3.7. Cooperación internacional y regulación de la ciberseguridad

La naturaleza transfronteriza de las amenazas cibernéticas exige fortalecer los mecanismos de cooperación internacional. Ningún Estado puede garantizar por sí solo la seguridad de todas las redes, plataformas y sistemas de los que depende su economía.

En este contexto, Naciones Unidas ha desarrollado procesos de negociación orientados a establecer normas de comportamiento responsable de los Estados en el uso de las tecnologías de información y comunicación.

El informe del Grupo de Expertos Gubernamentales de 2021 reconoce la importancia de aplicar el derecho internacional al ciberespacio y fortalecer las normas voluntarias de comportamiento responsable, las medidas de fomento de la confianza y la cooperación internacional (United Nations General Assembly, 2021a).

Entre las principales áreas de cooperación se encuentran:

- Intercambio de información sobre amenazas y vulnerabilidades.
- Cooperación para investigar incidentes transnacionales.
- Desarrollo de capacidades técnicas y jurídicas.
- Protección de infraestructuras críticas.

- Establecimiento de canales de comunicación durante crisis cibernéticas.
- Promoción de normas de comportamiento responsable.
- Fortalecimiento de mecanismos de asistencia técnica entre países.

La cooperación regional también resulta fundamental para los países con capacidades tecnológicas limitadas, debido a que permite compartir conocimientos, desarrollar protocolos comunes y mejorar los mecanismos de respuesta ante incidentes.

En consecuencia, la ciberseguridad internacional debe abordarse como un componente de la gobernanza global, en el cual la prevención, la cooperación y el respeto al derecho internacional constituyen condiciones esenciales para preservar la estabilidad del sistema internacional.

5.4 Disuasión y escalada en el ciberespacio: desafíos para la estabilidad internacional

5.4.1. Conceptualización de la disuasión en el entorno cibernético

La disuasión constituye un concepto central de los estudios estratégicos y de seguridad internacional. Tradicionalmente, se refiere a la capacidad de un Estado para influir en el comportamiento de otro actor mediante la amenaza creíble de imponer costos o impedir que alcance determinados objetivos.

En el ámbito militar convencional, la disuasión se ha sustentado históricamente en la capacidad de respuesta, la superioridad tecnológica, la defensa territorial y la posibilidad de imponer consecuencias significativas ante una agresión. Sin embargo, la incorporación del ciberespacio como dominio de competencia estratégica ha modificado las condiciones bajo las cuales se desarrolla este mecanismo.

La disuasión cibernética comprende las estrategias mediante las cuales los Estados buscan prevenir o limitar operaciones digitales maliciosas mediante capacidades defensivas, mecanismos de respuesta, medidas diplomáticas, sanciones económicas y cooperación internacional.

A diferencia de los escenarios militares tradicionales, el ciberespacio presenta dificultades particulares para establecer amenazas creíbles. La atribución de los ataques puede ser

incierta, los costos de ejecución de determinadas operaciones pueden ser relativamente bajos y las respuestas no necesariamente se producen en el mismo dominio tecnológico en el que ocurrió la agresión.

Por ejemplo, un Estado que enfrenta un ataque contra sus instituciones financieras podría responder mediante medidas diplomáticas, sanciones económicas, cooperación judicial, fortalecimiento de sus defensas o, dependiendo de las circunstancias, otras acciones permitidas por el derecho internacional.

Esta diversidad de respuestas evidencia que la disuasión cibernética no depende exclusivamente de la capacidad de ejecutar operaciones informáticas ofensivas, sino también de la fortaleza institucional, la resiliencia tecnológica y la capacidad de construir coaliciones internacionales.

5.4.2. Principales modalidades de disuasión cibernética

La disuasión en el ciberespacio puede desarrollarse mediante diferentes mecanismos complementarios.

a) Disuasión por negación

La disuasión por negación busca impedir que un potencial adversario alcance los objetivos de una operación maliciosa. Se fundamenta en la capacidad de proteger los sistemas, reducir las vulnerabilidades y garantizar la continuidad de los servicios esenciales.

Un Estado que dispone de redes resilientes, sistemas de respaldo, mecanismos de detección y protocolos de respuesta puede reducir significativamente los beneficios esperados de un ataque.

Esta modalidad tiene una importancia particular porque no requiere necesariamente identificar o amenazar al responsable antes de que ocurra una operación. Su fundamento es disminuir las posibilidades de éxito del ataque.

b) Disuasión por castigo

La disuasión por castigo consiste en comunicar que una operación maliciosa tendrá consecuencias para el actor responsable. Estas consecuencias pueden adoptar diferentes formas:

- Sanciones económicas.
- Restricciones comerciales.
- Medidas diplomáticas.
- Procesos judiciales.
- Suspensión de mecanismos de cooperación.
- Respuestas cibernéticas u otras medidas compatibles con el derecho internacional.

La efectividad de esta modalidad depende de la credibilidad de la respuesta y de la capacidad para atribuir las operaciones con suficiente fundamento.

c) Disuasión mediante normas y cooperación internacional

Esta modalidad busca prevenir comportamientos perjudiciales mediante el establecimiento de principios, compromisos y mecanismos de confianza entre los Estados.

Las normas internacionales contribuyen a definir expectativas de comportamiento y permiten reducir la incertidumbre sobre las consecuencias de determinadas acciones.

El informe del Grupo de Expertos Gubernamentales de Naciones Unidas de 2021 destaca la importancia de las normas voluntarias de comportamiento responsable, la aplicación del derecho internacional y las medidas de fomento de la confianza para fortalecer la estabilidad del ciberespacio (United Nations General Assembly, 2021a).

d) Disuasión mediante resiliencia institucional

La resiliencia constituye la capacidad de una organización o Estado para resistir, adaptarse y recuperarse frente a incidentes cibernéticos. Un sistema nacional con instituciones coordinadas, personal especializado, infraestructura redundante y mecanismos de recuperación puede reducir las consecuencias de una operación maliciosa.

Por ello, la resiliencia no solamente representa una capacidad defensiva, sino también un instrumento estratégico de disuasión, porque limita los resultados que un potencial adversario podría obtener.

5.4.3. Dificultades para establecer una disuasión efectiva en el ciberespacio

La disuasión cibernética presenta limitaciones que dificultan su aplicación como mecanismo de estabilidad internacional.

Primera dificultad: incertidumbre en la atribución. La identificación de los responsables de una operación puede requerir investigaciones prolongadas y la cooperación de diferentes jurisdicciones. Esta situación dificulta la formulación de respuestas inmediatas y puede reducir la credibilidad de las amenazas de represalia.

Segunda dificultad: asimetría de capacidades. Los Estados no poseen los mismos niveles de desarrollo tecnológico, infraestructura, recursos económicos ni personal especializado. Un actor con capacidades limitadas puede ocasionar daños significativos cuando explota vulnerabilidades de sistemas estratégicos.

Tercera dificultad: diversidad de actores. El ciberespacio no está integrado exclusivamente por Estados. También participan organizaciones criminales, empresas privadas, grupos independientes y actores que pueden operar con diferentes niveles de vinculación gubernamental.

Cuarta dificultad: dificultad para establecer proporcionalidad. No siempre resulta sencillo determinar la magnitud real de una operación cibernética. Un incidente puede afectar inicialmente un sistema informático y posteriormente generar consecuencias económicas, sociales o físicas.

Quinta dificultad: incertidumbre sobre las intenciones. Una misma operación puede responder a diferentes objetivos, como espionaje, preparación estratégica, sabotaje o presión política. La interpretación equivocada de estas intenciones puede producir respuestas desproporcionadas.

Estas características hacen que la disuasión en el ciberespacio requiera una combinación de capacidades técnicas, mecanismos diplomáticos, coordinación institucional y comprensión del derecho internacional.

5.4.4. Escalada de conflictos y riesgos de confrontación internacional

La escalada en el ciberespacio se refiere al proceso mediante el cual un incidente o una operación digital genera respuestas sucesivas que incrementan la intensidad del enfrentamiento entre los actores involucrados.

Este proceso puede comenzar con una operación limitada de espionaje o interrupción de servicios y evolucionar hacia medidas diplomáticas, sanciones económicas, operaciones cibernéticas de respuesta o confrontaciones en otros dominios.

La escalada puede producirse de manera deliberada o como consecuencia de errores de interpretación, fallas de comunicación y percepciones equivocadas sobre las intenciones del adversario.

Entre los principales factores que pueden favorecerla se encuentran:

a) Interpretación equivocada de una operación.

Una actividad de reconocimiento informático puede confundirse con la preparación de un ataque destructivo. Si el Estado afectado interpreta que existe una amenaza inmediata contra su seguridad nacional, podría adoptar medidas de respuesta antes de disponer de información suficiente.

b) Atribución incorrecta de responsabilidades.

Cuando una operación se ejecuta mediante infraestructuras comprometidas de terceros países, existe el riesgo de responsabilizar a actores que no participaron directamente en el incidente.

c) Respuestas desproporcionadas.

Una respuesta que excede la magnitud del incidente inicial puede provocar nuevas represalias y aumentar la intensidad del conflicto.

d) Convergencia entre el ciberespacio y otros dominios.

Las operaciones digitales pueden afectar sistemas vinculados con actividades militares, energéticas, financieras y de transporte. Esto puede generar una interacción entre amenazas cibernéticas y conflictos convencionales.

e) Ausencia de canales de comunicación.

Cuando los Estados carecen de mecanismos de consulta y comunicación durante una crisis cibernética, aumenta la posibilidad de que interpreten incorrectamente las acciones del otro actor.

La Organización del Tratado del Atlántico Norte reconoce que las amenazas cibernéticas pueden ser complejas, destructivas y coercitivas, y que la defensa cibernética forma parte de sus tareas de disuasión, defensa y gestión de crisis (NATO, 2024).

Esta perspectiva evidencia que los incidentes digitales deben analizarse dentro de un marco más amplio de seguridad internacional, considerando sus posibles conexiones con la estabilidad política, militar y económica.

5.4.5. Relación entre disuasión cibernética y derecho internacional

Uno de los debates más relevantes de la seguridad internacional consiste en determinar cómo se aplican las normas del derecho internacional a las operaciones desarrolladas en el ciberespacio.

El hecho de que una operación se ejecute mediante tecnologías digitales no significa que quede fuera del marco jurídico internacional. Los principios de soberanía, no intervención, prohibición del uso de la fuerza, solución pacífica de controversias y responsabilidad internacional continúan siendo relevantes para evaluar el comportamiento de los Estados.

El Grupo de Expertos Gubernamentales de Naciones Unidas ha reconocido que el derecho internacional, incluida la Carta de las Naciones Unidas, resulta aplicable al uso de las tecnologías de información y comunicación por parte de los Estados (United Nations General Assembly, 2021a).

Sin embargo, su aplicación a situaciones concretas puede generar debates jurídicos relacionados con la intensidad de los efectos, la naturaleza de la operación y la atribución de responsabilidad.

Es importante diferenciar tres conceptos:

- Operación cibernética maliciosa: actividad digital que busca comprometer, alterar, interrumpir o explotar sistemas informáticos.
- Uso de la fuerza: conducta que, por su naturaleza, escala y efectos, puede alcanzar el umbral de prohibición establecido en el artículo 2.4 de la Carta de las Naciones Unidas.
- Ataque armado: concepto jurídico que permite analizar la aplicación del artículo 51 de la Carta de las Naciones Unidas sobre el derecho inherente de legítima defensa.

No toda operación cibernética constituye automáticamente un uso de la fuerza o un ataque armado. Su evaluación requiere examinar las circunstancias concretas, la magnitud de sus efectos y las normas jurídicas aplicables.

Asimismo, cuando las operaciones se desarrollan durante un conflicto armado, adquieren relevancia las normas del derecho internacional humanitario, particularmente los principios de distinción, proporcionalidad y precaución en la conducción de las hostilidades.

Estas consideraciones resultan fundamentales para evitar que las respuestas a incidentes cibernéticos se desarrollen al margen de las obligaciones internacionales de los Estados.

5.4.6. Medidas para prevenir la escalada y fortalecer la estabilidad internacional

La prevención de la escalada requiere desarrollar mecanismos que permitan gestionar los incidentes cibernéticos de manera coordinada, transparente y proporcional.

Entre las principales medidas se encuentran:

1. Establecimiento de canales diplomáticos de comunicación. Los Estados deben disponer de mecanismos de contacto directo que permitan intercambiar información durante incidentes y aclarar situaciones que puedan generar interpretaciones equivocadas.
2. Desarrollo de medidas de fomento de la confianza. El intercambio de información, las consultas técnicas y la cooperación institucional pueden contribuir a reducir la incertidumbre sobre las actividades desarrolladas en el ciberespacio.

3. Fortalecimiento de capacidades nacionales de respuesta. Los equipos especializados en respuesta a incidentes de seguridad informática, conocidos como CERT o CSIRT, desempeñan un papel importante en la identificación, coordinación y gestión de amenazas.
4. Promoción de normas internacionales de comportamiento responsable. Los acuerdos y compromisos internacionales permiten establecer expectativas sobre la conducta de los Estados y reducir los riesgos asociados a operaciones que afecten servicios esenciales.
5. Desarrollo de mecanismos de atribución rigurosos. Las acusaciones públicas deben sustentarse en evidencias técnicas y análisis estratégico, evitando respuestas basadas exclusivamente en especulaciones.
6. Protección de infraestructuras críticas. La resiliencia de los servicios esenciales reduce los impactos de las operaciones maliciosas y limita la posibilidad de que un incidente se transforme en una crisis internacional.
7. Cooperación entre actores públicos y privados. Las empresas tecnológicas y los operadores de infraestructura poseen información relevante sobre amenazas y vulnerabilidades. Su participación resulta indispensable para fortalecer la prevención y la respuesta.

Estas medidas deben complementarse con procesos de capacitación, investigación científica y cooperación internacional que permitan reducir las desigualdades tecnológicas y fortalecer las capacidades de los países en desarrollo.

5.4.7. Disuasión cibernética y estabilidad estratégica internacional

La estabilidad estratégica en el ciberespacio depende de la capacidad de los Estados para evitar que las operaciones digitales maliciosas se conviertan en fuentes permanentes de confrontación.

A diferencia de los escenarios convencionales, en los cuales determinadas capacidades militares pueden identificarse mediante mecanismos de observación y evaluación, el ciberespacio presenta un entorno de mayor incertidumbre. Los Estados pueden desconocer las capacidades reales de sus adversarios, las vulnerabilidades existentes y las consecuencias potenciales de determinadas operaciones.

Esta incertidumbre genera dificultades para establecer límites claros entre las actividades de inteligencia, las acciones de preparación operativa y las operaciones destinadas a producir daños.

Por consiguiente, la estabilidad estratégica requiere desarrollar mecanismos que reduzcan la posibilidad de errores de cálculo y fortalezcan la confianza entre los actores internacionales.

En este sentido, la disuasión no debe depender exclusivamente de la amenaza de represalias, sino también de la capacidad de prevenir ataques, mantener servicios esenciales, compartir información y resolver controversias mediante mecanismos diplomáticos.

La resiliencia tecnológica, la cooperación internacional y la aplicación del derecho internacional constituyen elementos complementarios para construir un entorno digital más seguro.

Finalmente, la evolución de las capacidades de inteligencia artificial, automatización y computación avanzada plantea nuevos desafíos para la disuasión. Los sistemas automatizados pueden acelerar la identificación de amenazas y las respuestas defensivas, pero también pueden incrementar el riesgo de decisiones precipitadas cuando operan con información incompleta o interpretaciones erróneas.

Por esta razón, la intervención humana, la transparencia institucional y los mecanismos de consulta internacional deben mantenerse como componentes centrales de la gestión de crisis cibernéticas.

5.5 Operaciones de influencia, desinformación y contenidos sintéticos en las disputas de poder

5.5.1. Conceptualización de las operaciones de influencia en el sistema internacional

Las operaciones de influencia constituyen un conjunto de acciones estratégicas orientadas a modificar las percepciones, actitudes, opiniones y comportamientos de determinados públicos con el propósito de alcanzar objetivos políticos, económicos, diplomáticos o militares. En el contexto de las relaciones internacionales, estas operaciones representan instrumentos de poder que permiten a los Estados y otros actores ejercer influencia sobre

sociedades, instituciones y procesos de decisión sin recurrir necesariamente a mecanismos convencionales de confrontación militar.

Históricamente, la influencia política ha estado presente en las relaciones entre los Estados mediante la propaganda, la diplomacia pública, la difusión cultural, las campañas de comunicación y las estrategias de persuasión. Sin embargo, la expansión de Internet, las redes sociales y las tecnologías de inteligencia artificial ha modificado significativamente la escala, velocidad y alcance de estas actividades.

En el entorno digital contemporáneo, las operaciones de influencia pueden desarrollarse mediante la difusión coordinada de mensajes, la manipulación de contenidos audiovisuales, la utilización de cuentas automatizadas, la amplificación artificial de determinadas narrativas y la explotación de divisiones sociales existentes. Estas actividades pueden tener como finalidad debilitar la confianza en las instituciones, influir en procesos electorales, deteriorar la imagen internacional de un gobierno o modificar las percepciones de la opinión pública respecto de un conflicto.

Es importante diferenciar las operaciones de influencia de la comunicación estratégica legítima. Mientras que la diplomacia pública busca proyectar posiciones e intereses mediante mensajes institucionales y mecanismos de persuasión, las operaciones de manipulación informativa pueden recurrir al ocultamiento de sus patrocinadores, la fabricación de evidencias y la difusión deliberada de contenidos engañosos.

Desde esta perspectiva, las operaciones de influencia forman parte de una dimensión contemporánea de la competencia estratégica, en la cual la información se convierte en un recurso de poder. Los actores internacionales no solamente compiten por el control de territorios, recursos naturales, mercados o capacidades tecnológicas, sino también por la capacidad de construir interpretaciones de la realidad y orientar las percepciones de las sociedades.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2024) advierte que la desinformación puede afectar diferentes ámbitos de las políticas públicas, comprometer la confianza en las instituciones democráticas y profundizar las divisiones sociales. Además, señala que la digitalización y el desarrollo de la inteligencia artificial

generativa incrementan las posibilidades de producir y distribuir contenidos engañosos a gran escala.

Por consiguiente, las operaciones de influencia deben analizarse como un fenómeno multidimensional que relaciona comunicación, tecnología, política exterior, seguridad internacional y gobernanza de la información.

5.5.2. Desinformación, información errónea y manipulación informativa

La comprensión de las disputas informativas requiere diferenciar conceptos que, aunque se encuentran relacionados, presentan características y consecuencias distintas.

a) Información errónea (misinformation).

Se refiere a la difusión de información falsa, inexacta o engañosa sin que necesariamente exista una intención deliberada de perjudicar o manipular. Puede producirse por errores periodísticos, interpretaciones equivocadas, desconocimiento de los acontecimientos o reproducción involuntaria de contenidos no verificados.

b) Desinformación (disinformation).

Consiste en la producción y difusión deliberada de información falsa o manipulada con la intención de engañar, influir o generar determinados efectos políticos, económicos o sociales.

c) Información maliciosa (malinformation).

Se refiere a información basada en hechos reales que se utiliza de manera descontextualizada, manipulada o divulgada con la finalidad de causar perjuicio. Puede incluir la exposición de documentos privados, la publicación selectiva de comunicaciones confidenciales o la utilización de datos personales para afectar la reputación de individuos e instituciones.

Estas distinciones permiten comprender que no toda información incorrecta constituye una operación de desinformación y que las respuestas institucionales deben considerar tanto la naturaleza del contenido como la intención y el contexto de su difusión.

Wardle y Derakhshan (2017) proponen comprender el desorden informativo como un fenómeno que involucra diferentes tipos de contenidos, agentes, motivaciones y mecanismos de distribución. Su planteamiento resulta relevante porque permite superar una interpretación limitada de la desinformación como simple circulación de noticias falsas y analizarla como un proceso complejo de producción, transformación y difusión de información.

En el ámbito internacional, estas prácticas pueden utilizarse para cuestionar la legitimidad de gobiernos, desacreditar organismos multilaterales, debilitar alianzas estratégicas o generar percepciones negativas sobre determinados países.

Por ejemplo, durante una crisis diplomática, un actor interesado podría difundir documentos alterados, declaraciones fuera de contexto o imágenes manipuladas para presentar a un gobierno como responsable de acontecimientos cuya autoría todavía no ha sido establecida. La repetición de estos contenidos en diferentes plataformas puede generar una percepción pública difícil de corregir, incluso cuando posteriormente se demuestra su falsedad.

5.5.3. Mecanismos tecnológicos utilizados en las operaciones de influencia

Las tecnologías digitales han permitido desarrollar mecanismos de influencia que combinan automatización, segmentación de audiencias, análisis de datos y producción masiva de contenidos.

Entre los principales mecanismos se encuentran los siguientes:

a) Redes de cuentas automatizadas o bots

Los bots son programas informáticos que ejecutan determinadas acciones de manera automática en plataformas digitales. Pueden utilizarse para publicar mensajes, compartir contenidos, seguir usuarios o amplificar determinadas narrativas.

En operaciones coordinadas, estas cuentas pueden generar una percepción artificial de popularidad o consenso social. Cuando numerosos perfiles reproducen simultáneamente un mensaje, los usuarios pueden interpretar que existe un respaldo ciudadano amplio, aunque la actividad proceda de una red automatizada.

b) Redes de perfiles falsos y comportamiento coordinado

Los actores que desarrollan operaciones de influencia pueden utilizar identidades ficticias o perfiles que aparentan representar a ciudadanos, organizaciones sociales o medios de comunicación.

Estas redes pueden difundir contenidos de manera coordinada, interactuar entre sí y construir narrativas destinadas a influir en determinadas comunidades digitales.

c) Microsegmentación de audiencias

La microsegmentación consiste en utilizar información demográfica, geográfica, conductual o psicográfica para dirigir mensajes específicos a grupos determinados.

Esta técnica puede emplearse legítimamente en campañas informativas y comunicación institucional. Sin embargo, también puede utilizarse para explotar temores, prejuicios y vulnerabilidades de determinados sectores de la población mediante mensajes diseñados para provocar reacciones emocionales.

d) Amplificación algorítmica

Las plataformas digitales utilizan sistemas de recomendación que seleccionan y priorizan contenidos de acuerdo con diferentes indicadores de interacción, preferencias y comportamiento de los usuarios.

La amplificación artificial puede aprovechar estos mecanismos para aumentar la visibilidad de determinados mensajes, generando una exposición desproporcionada respecto de su relevancia o credibilidad.

e) Manipulación de tendencias digitales

Consiste en promover artificialmente la circulación de palabras clave, etiquetas y contenidos con el propósito de posicionar determinados temas en las conversaciones públicas.

Esta práctica puede modificar la agenda informativa y desplazar la atención hacia asuntos seleccionados estratégicamente.

La utilización combinada de estos mecanismos permite desarrollar operaciones de influencia que pueden resultar difíciles de identificar, especialmente cuando se mezclan con conversaciones legítimas y participación ciudadana auténtica.

5.5.4. Contenidos sintéticos, inteligencia artificial generativa y deepfakes

Uno de los cambios más significativos en las disputas contemporáneas de poder corresponde al desarrollo de contenidos sintéticos mediante inteligencia artificial generativa.

Los contenidos sintéticos son materiales audiovisuales, textuales o gráficos producidos o modificados mediante sistemas computacionales. Pueden incluir imágenes artificiales, voces generadas, videos manipulados, documentos simulados y representaciones digitales de personas reales.

Dentro de esta categoría adquieren especial relevancia los deepfakes, que son contenidos audiovisuales generados o modificados mediante técnicas avanzadas de inteligencia artificial con el propósito de representar de manera convincente situaciones, declaraciones o acciones que no ocurrieron realmente.

Estas tecnologías permiten crear videos en los que una autoridad parece pronunciar declaraciones que nunca realizó, reproducir artificialmente la voz de un representante diplomático o generar imágenes que aparentan documentar acontecimientos inexistentes.

Chesney y Citron (2019) advierten que los deepfakes pueden producir consecuencias importantes para la seguridad nacional, la privacidad, la reputación y la confianza pública. Su capacidad de imitar la apariencia y la voz de personas reales introduce nuevos desafíos para la verificación de evidencias y la credibilidad de las comunicaciones institucionales.

En el contexto internacional, los contenidos sintéticos pueden utilizarse para:

- Simular declaraciones de autoridades gubernamentales.
- Fabricar evidencias audiovisuales sobre supuestas operaciones militares.
- Alterar discursos diplomáticos y comunicaciones oficiales.
- Crear materiales falsos para desacreditar a representantes internacionales.
- Difundir información manipulada durante procesos electorales.

- Generar confusión durante negociaciones o situaciones de crisis.
- Deteriorar las relaciones entre países mediante acusaciones falsas.

Un escenario especialmente preocupante se presenta cuando un contenido audiovisual falso se difunde durante un acontecimiento internacional de alta sensibilidad. Si un video manipulado atribuye a un jefe de Estado una declaración amenazante, su circulación puede generar reacciones diplomáticas antes de que las instituciones dispongan de tiempo suficiente para verificar su autenticidad.

Además, los contenidos sintéticos generan un fenómeno adicional: la posibilidad de desacreditar materiales auténticos alegando que han sido manipulados. Esta situación, denominada frecuentemente dividendo del mentiroso (liar's dividend), permite que determinados actores cuestionen evidencias legítimas aprovechando la creciente dificultad de distinguir entre materiales reales y artificiales (Chesney & Citron, 2019).

Por ello, la amenaza no reside exclusivamente en la producción de contenidos falsos, sino también en el debilitamiento general de la confianza en las evidencias audiovisuales.

5.5.5. Información como instrumento de poder y competencia geopolítica

En el sistema internacional, la información constituye un recurso estratégico porque influye en la percepción de los acontecimientos, la legitimidad de las decisiones y la capacidad de los actores para construir alianzas.

Las disputas de poder contemporáneas incluyen una dimensión informativa en la que los Estados buscan posicionar sus interpretaciones sobre acontecimientos internacionales, defender sus intereses y contrarrestar narrativas adversas.

La competencia informativa puede manifestarse en diferentes escenarios:

a) Conflictos armados. Las partes involucradas pueden difundir información destinada a fortalecer su legitimidad, desacreditar al adversario o influir en la percepción internacional de las operaciones militares.
b) Disputas territoriales. Los actores pueden desarrollar campañas informativas para reforzar sus argumentos históricos, jurídicos y políticos sobre determinados territorios.

c) Competencia económica y tecnológica. La información puede utilizarse para afectar la reputación de empresas estratégicas, influir en decisiones de inversión o generar incertidumbre respecto de la seguridad de determinadas tecnologías.
d) Procesos electorales. Las operaciones de influencia pueden buscar alterar la percepción ciudadana sobre candidatos, partidos, instituciones o políticas gubernamentales, afectando la confianza en los procedimientos democráticos.
e) Negociaciones multilaterales. La difusión selectiva de documentos, declaraciones y posiciones puede utilizarse para modificar las condiciones políticas de una negociación o ejercer presión sobre determinados representantes.

En estos escenarios, la capacidad de influir sobre la opinión pública puede generar ventajas estratégicas sin necesidad de recurrir directamente a la fuerza.

La OCDE (2024) plantea que enfrentar la desinformación requiere fortalecer la integridad del ecosistema informativo mediante políticas de transparencia, pluralidad, responsabilidad institucional y resiliencia social. Esto implica comprender que la solución no consiste únicamente en eliminar contenidos falsos, sino en fortalecer las condiciones que permiten a las sociedades acceder a información confiable y desarrollar capacidades críticas.

5.5.6. Consecuencias de las operaciones de influencia para la estabilidad internacional

Las operaciones de influencia pueden producir consecuencias que afectan tanto la política interna de los Estados como sus relaciones exteriores.

Entre sus principales efectos se encuentran:

1. Erosión de la confianza institucional: la difusión sistemática de información manipulada puede debilitar la credibilidad de gobiernos, organismos internacionales y medios de comunicación.

2. Polarización social: la segmentación de contenidos y la amplificación de narrativas extremas pueden profundizar divisiones políticas y sociales.

3. Deterioro de las relaciones diplomáticas: las declaraciones falsas atribuidas a autoridades pueden provocar tensiones entre países y dificultar los procesos de negociación.

4. Desestabilización política: las campañas coordinadas pueden afectar procesos electorales, generar incertidumbre y debilitar la legitimidad de determinadas instituciones.

5. Manipulación de percepciones durante conflictos: la difusión de contenidos falsos puede incrementar la hostilidad, dificultar la verificación de acontecimientos y favorecer interpretaciones extremas.

6. Debilitamiento de la confianza en la evidencia: la proliferación de contenidos sintéticos puede dificultar que las sociedades distingan entre información auténtica y manipulada.

Estos efectos demuestran que la integridad informativa constituye una condición relevante para la seguridad internacional. Cuando la información pierde credibilidad, se reducen las posibilidades de construir consensos, gestionar crisis y desarrollar mecanismos de cooperación.

5.5.7. Estrategias internacionales para prevenir y contrarrestar la desinformación

La prevención de las operaciones de influencia requiere mecanismos tecnológicos, institucionales, educativos y diplomáticos.

En junio de 2024, Naciones Unidas presentó los Global Principles for Information Integrity, que establecen recomendaciones para fortalecer la integridad del ecosistema informativo mediante cinco dimensiones: confianza social y resiliencia, incentivos saludables, empoderamiento público, medios independientes, libres y plurales, y transparencia e investigación (United Nations, 2024).

Estos principios permiten identificar varias líneas de acción:

a) Verificación de información. Las instituciones deben establecer procedimientos para contrastar documentos, imágenes, videos y declaraciones antes de difundirlos o utilizarlos como fundamento de decisiones oficiales.

b) Alfabetización mediática y digital. La ciudadanía debe desarrollar capacidades para identificar fuentes confiables, reconocer contenidos manipulados y evaluar críticamente los mensajes que circulan en las plataformas digitales.
c) Transparencia de las plataformas. Los proveedores tecnológicos deben fortalecer los mecanismos de identificación de comportamientos coordinados, publicidad política y contenidos sintéticos, respetando los derechos fundamentales.
d) Protección de las comunicaciones oficiales. Los gobiernos necesitan canales institucionales verificables para informar a la ciudadanía y responder oportunamente ante la circulación de declaraciones falsas.
e) Cooperación internacional. Los Estados y organismos multilaterales deben intercambiar información sobre campañas de manipulación y desarrollar mecanismos de coordinación para responder ante amenazas transnacionales.
f) Identificación de contenidos sintéticos. La utilización de mecanismos de procedencia y autenticidad de contenidos, marcas de agua y tecnologías de detección puede contribuir a establecer el origen y las modificaciones de determinados materiales digitales.
g) Protección de la libertad de expresión. Las respuestas contra la desinformación deben evitar la censura arbitraria, la criminalización de opiniones legítimas y la concentración excesiva del control informativo en instituciones gubernamentales.

En definitiva, las operaciones de influencia representan una dimensión estratégica de las disputas contemporáneas de poder. Su prevención requiere fortalecer la confianza pública, desarrollar capacidades tecnológicas y garantizar que las políticas de integridad informativa respeten los derechos humanos y la pluralidad democrática.

5.6 Sistemas autónomos y usos militares de la inteligencia artificial: control humano y dilemas jurídicos

5.6.1. Conceptualización de los sistemas autónomos en el ámbito militar

La incorporación de inteligencia artificial en el sector de la defensa ha transformado las capacidades de planificación, vigilancia, reconocimiento, análisis de información y conducción de operaciones militares. Los avances en aprendizaje automático, robótica, procesamiento de imágenes y sistemas de navegación han permitido desarrollar

tecnologías capaces de ejecutar determinadas funciones con niveles crecientes de autonomía.

Los sistemas autónomos militares son tecnologías que pueden realizar tareas específicas mediante procesos automatizados y, dependiendo de su diseño, seleccionar determinadas acciones en función de la información que reciben del entorno.

Es necesario distinguir entre sistemas automatizados y sistemas autónomos. Los primeros ejecutan procedimientos previamente programados bajo condiciones definidas, mientras que los segundos pueden seleccionar o modificar determinadas acciones a partir de la información procesada y de los objetivos establecidos.

Esta distinción adquiere particular relevancia en los sistemas de armas autónomas, debido a que algunos pueden seleccionar objetivos y aplicar fuerza sin intervención humana en las funciones críticas de selección y ataque.

El Comité Internacional de la Cruz Roja (CICR, 2021) describe los sistemas de armas autónomas como aquellos que, después de ser activados, pueden seleccionar y atacar objetivos sin intervención humana en esas funciones. Esta característica genera importantes preocupaciones humanitarias, jurídicas y éticas, especialmente cuando las decisiones afectan directamente la vida de las personas.

La incorporación de estos sistemas no debe interpretarse únicamente como una evolución tecnológica de los armamentos tradicionales. Representa una transformación de la relación entre el ser humano, la tecnología y el ejercicio de la fuerza, debido a que introduce procesos algorítmicos en actividades que históricamente han requerido juicio humano y responsabilidad militar.

5.6.2. Principales aplicaciones militares de la inteligencia artificial

La inteligencia artificial puede utilizarse en diferentes ámbitos de la actividad militar, desde tareas de apoyo administrativo hasta funciones relacionadas con la planificación y conducción de operaciones.

a) Vigilancia, reconocimiento e identificación de objetos

Los sistemas de visión artificial permiten analizar imágenes obtenidas mediante satélites, aeronaves no tripuladas, sensores y cámaras de vigilancia.

Estas tecnologías pueden identificar objetos, reconocer patrones de movimiento y clasificar determinadas características del entorno. Su utilización facilita el análisis de grandes volúmenes de información y puede contribuir a mejorar la capacidad de vigilancia de las fuerzas militares.

Sin embargo, los sistemas de reconocimiento pueden cometer errores cuando las imágenes presentan baja resolución, condiciones ambientales adversas o elementos que generan confusión visual.

b) Análisis de inteligencia militar

Los sistemas de IA pueden procesar información procedente de múltiples fuentes, identificar patrones y elaborar informes que faciliten la evaluación de escenarios estratégicos.

Estas aplicaciones permiten organizar datos geográficos, imágenes, comunicaciones e información logística para apoyar la planificación militar.

c) Logística y mantenimiento predictivo

Los modelos predictivos pueden estimar necesidades de mantenimiento, identificar posibles fallas en equipos y optimizar la distribución de recursos.

Su utilización permite reducir interrupciones operativas y mejorar la administración de inventarios, transporte y abastecimiento.

d) Sistemas no tripulados

Los vehículos aéreos, terrestres y marítimos no tripulados pueden incorporar capacidades automatizadas de navegación, reconocimiento y seguimiento.

Aunque no todos estos sistemas son armas autónomas, su desarrollo evidencia la creciente integración entre robótica, sensores e inteligencia artificial en el ámbito militar.

e) Sistemas de defensa y protección

La IA puede utilizarse para detectar comportamientos anómalos, identificar posibles amenazas y apoyar sistemas de protección de instalaciones militares e infraestructuras estratégicas.

Estas aplicaciones pueden contribuir a reducir los tiempos de respuesta, aunque su utilización requiere mecanismos de supervisión y validación de resultados.

f) Sistemas de apoyo a la toma de decisiones

Los sistemas de análisis automatizado pueden procesar información sobre diferentes escenarios operativos y presentar alternativas a los responsables militares.

Sin embargo, la velocidad de procesamiento no garantiza que las recomendaciones sean correctas. Los modelos pueden presentar errores, sesgos y limitaciones que deben ser considerados antes de adoptar decisiones con consecuencias estratégicas.

5.6.3. Sistemas de armas autónomas y decisiones relacionadas con el uso de la fuerza

Los sistemas de armas autónomas representan uno de los aspectos más controvertidos de la aplicación militar de la inteligencia artificial.

Su principal característica consiste en la capacidad de seleccionar y aplicar fuerza contra objetivos mediante procesos que no requieren intervención humana directa en el momento de ejecutar determinadas funciones críticas.

Esta autonomía plantea interrogantes relacionados con la identificación de objetivos, la evaluación del contexto operativo y la capacidad de anticipar las consecuencias de una acción militar.

La preocupación central consiste en determinar si un sistema tecnológico puede operar de manera compatible con las normas del derecho internacional humanitario, especialmente cuando debe distinguir entre combatientes y civiles, evaluar la proporcionalidad de un ataque y adoptar precauciones para reducir los daños incidentales.

El CICR (2021) considera necesario establecer límites jurídicos internacionales a los sistemas de armas autónomas. Entre sus recomendaciones se encuentran prohibir los

sistemas cuyo comportamiento no pueda comprenderse, predecirse y controlarse suficientemente, así como establecer restricciones estrictas sobre aquellos que puedan ser utilizados dentro de parámetros compatibles con el derecho internacional humanitario.

En este sentido, es fundamental diferenciar entre el empleo de inteligencia artificial como herramienta de apoyo a las operaciones militares y la delegación de decisiones sobre el uso de la fuerza a sistemas autónomos.

La primera posibilidad puede facilitar tareas de análisis y planificación, mientras que la segunda plantea un problema de responsabilidad relacionado con la intervención de máquinas en decisiones que afectan directamente la vida humana.

5.6.4. Control humano significativo y responsabilidad en las operaciones militares

El control humano constituye uno de los principios fundamentales del debate internacional sobre sistemas de armas autónomas.

Su importancia radica en garantizar que las decisiones relacionadas con el uso de la fuerza permanezcan sujetas a criterios humanos de juicio, responsabilidad y evaluación contextual.

El concepto de control humano significativo implica que las personas responsables de las operaciones militares deben disponer de información suficiente para comprender el funcionamiento del sistema, evaluar sus capacidades y limitaciones, determinar las condiciones de utilización y ejercer una intervención efectiva cuando sea necesario.

No se trata únicamente de que una persona active un dispositivo o autorice una operación de manera inicial. El control debe considerar las condiciones concretas en las que se desarrolla la misión y la posibilidad de modificarla o detenerla cuando las circunstancias lo requieran.

Desde una perspectiva operativa, el control humano debe incorporar los siguientes elementos:

1. Comprensión del funcionamiento del sistema. Los responsables deben conocer las capacidades, limitaciones y posibles errores de los sistemas utilizados.

2. Delimitación de objetivos. Las funciones asignadas deben establecer claramente las características de los objetivos, las condiciones de utilización y las restricciones operativas.
3. Control temporal y geográfico. Las operaciones deben encontrarse delimitadas por períodos, espacios y condiciones previamente establecidos.
4. Supervisión durante la operación. Deben existir mecanismos que permitan observar el comportamiento del sistema y detectar posibles desviaciones.
5. Capacidad de intervención. Los operadores deben disponer de mecanismos efectivos para modificar, suspender o cancelar una operación cuando las circunstancias lo requieran.
6. Responsabilidad institucional. Las organizaciones militares deben establecer procedimientos para identificar quién autoriza, supervisa y evalúa la utilización de estos sistemas.

El documento de trabajo CCW/GGE.1/2024/WP.3, presentado en el marco de las discusiones sobre sistemas de armas autónomas, destaca la importancia de conservar el control humano durante el ciclo de vida de estos sistemas y de establecer límites sobre los objetivos, la duración, el alcance geográfico y las condiciones de utilización (United Nations, 2024).

Por consiguiente, el control humano no debe considerarse un elemento complementario de la tecnología, sino una condición esencial para preservar la responsabilidad en las decisiones militares.

5.6.5. Dilemas jurídicos de los sistemas autónomos en el derecho internacional humanitario

La utilización de sistemas autónomos en operaciones militares plantea interrogantes sobre la aplicación de las normas del derecho internacional humanitario (DIH).

El derecho internacional humanitario establece reglas destinadas a limitar los efectos de los conflictos armados y proteger a las personas que no participan directamente en las hostilidades, así como a quienes han dejado de participar en ellas.

Su aplicación a los sistemas autónomos requiere considerar especialmente los siguientes principios:

a) Principio de distinción

Este principio establece la obligación de distinguir entre personas civiles y combatientes, así como entre bienes civiles y objetivos militares.

Los sistemas autónomos pueden presentar dificultades para interpretar determinadas situaciones, especialmente cuando los comportamientos humanos no permiten establecer con claridad si una persona participa directamente en las hostilidades.

Por ejemplo, un sistema de reconocimiento podría identificar un objeto o una persona mediante patrones visuales, pero no necesariamente comprender el contexto que determina su condición jurídica.

b) Principio de proporcionalidad

El principio de proporcionalidad prohíbe los ataques cuando sea previsible que ocasionen daños incidentales a civiles o bienes civiles que resulten excesivos en relación con la ventaja militar concreta y directa prevista.

Su aplicación requiere valorar circunstancias operativas, consecuencias previsibles y elementos contextuales que pueden modificarse durante una operación.

La utilización de sistemas autónomos plantea el desafío de determinar si un algoritmo puede realizar una evaluación suficientemente contextualizada de estas circunstancias.

c) Principio de precaución

Este principio exige adoptar todas las precauciones factibles para evitar o reducir los daños a la población civil.

En los sistemas autónomos, su aplicación implica evaluar previamente las capacidades tecnológicas, realizar pruebas rigurosas, establecer restricciones operativas y disponer de mecanismos para interrumpir una acción cuando exista riesgo de daños indebidos.

d) Responsabilidad internacional

La utilización de sistemas autónomos no elimina la responsabilidad de los Estados por sus actuaciones ni las obligaciones de las personas que participan en las operaciones militares.

La complejidad tecnológica no puede convertirse en un argumento para justificar la ausencia de responsabilidad cuando se producen violaciones del derecho internacional humanitario.

Además, el artículo 36 del Protocolo adicional I de 1977 a los Convenios de Ginebra establece la obligación de los Estados de determinar, durante el estudio, desarrollo, adquisición o adopción de nuevas armas, si su empleo estaría prohibido en algunas o en todas las circunstancias por el derecho internacional aplicable.

Este mecanismo de revisión jurídica adquiere especial importancia ante la incorporación de inteligencia artificial y capacidades autónomas en nuevos sistemas militares.

5.6.6. Dilemas éticos y filosóficos de la autonomía militar

Más allá de las cuestiones jurídicas, los sistemas de armas autónomas plantean problemas éticos relacionados con la delegación de decisiones sobre la vida y la muerte.

Una de las principales interrogantes consiste en determinar si resulta moralmente aceptable que una máquina seleccione y ataque objetivos humanos sin una intervención humana efectiva en el proceso decisional.

La decisión de utilizar la fuerza requiere valorar circunstancias que trascienden la identificación técnica de un objetivo. Implica considerar la necesidad militar, las consecuencias humanitarias, la proporcionalidad y las condiciones específicas del conflicto.

Los sistemas algorítmicos pueden procesar información y ejecutar operaciones con rapidez, pero carecen de responsabilidad moral equivalente a la de las personas e instituciones que toman decisiones.

Entre los principales dilemas éticos se encuentran:

- Delegación de decisiones letales: determina hasta qué punto las personas pueden transferir a sistemas autónomos decisiones relacionadas con la vida humana.
- Deshumanización de la guerra: plantea el riesgo de reducir la percepción de las consecuencias humanas de las operaciones militares.
- Opacidad algorítmica: dificulta explicar cómo se produjo una determinada decisión cuando el sistema utiliza modelos complejos.
- Sesgos tecnológicos: pueden ocasionar identificaciones incorrectas o resultados discriminatorios.
- Responsabilidad fragmentada: puede dificultar la determinación de responsabilidades entre desarrolladores, fabricantes, operadores y autoridades militares.
- Reducción de barreras para el uso de la fuerza: la percepción de que las operaciones pueden realizarse con menor riesgo para las propias tropas podría modificar los cálculos políticos de intervención militar.

El Secretario General de Naciones Unidas y la presidencia del CICR advirtieron conjuntamente en 2023 sobre los riesgos humanitarios, jurídicos y estratégicos de los sistemas de armas autónomas, destacando la necesidad de preservar el control humano sobre las decisiones relacionadas con el uso de la fuerza (United Nations, 2023).

5.6.7. Gobernanza internacional y regulación de los sistemas de armas autónomas

La regulación internacional de los sistemas de armas autónomas constituye uno de los debates centrales del desarme contemporáneo.

El principal espacio multilateral de discusión ha sido la Convención sobre Ciertas Armas Convencionales (CCW), en cuyo marco se desarrolla el Grupo de Expertos Gubernamentales sobre Sistemas de Armas Autónomas Letales.

Este proceso reúne a representantes estatales, especialistas jurídicos y técnicos para examinar las implicaciones humanitarias, éticas y jurídicas de estas tecnologías.

Las discusiones internacionales reflejan diferentes posiciones respecto de la necesidad de prohibir determinados sistemas, establecer restricciones vinculantes o desarrollar principios y estándares de utilización.

El CICR (2021) recomienda adoptar nuevas normas jurídicamente vinculantes que prohíban sistemas impredecibles y el uso de armas autónomas para atacar directamente a personas, además de establecer restricciones para otros sistemas que puedan utilizarse bajo condiciones de control humano efectivo.

Por otra parte, los trabajos desarrollados en el marco de la CCW durante 2024 muestran la importancia de examinar aspectos como la previsibilidad, la fiabilidad, la evaluación jurídica y la conservación del control humano durante el ciclo de vida de los sistemas (United Nations, 2024).

Desde una perspectiva diplomática, los principales desafíos regulatorios comprenden:

1. Establecer definiciones comunes sobre los sistemas de armas autónomas.
2. Determinar qué niveles de autonomía requieren restricciones específicas.
3. Definir obligaciones de supervisión humana.
4. Fortalecer los mecanismos de revisión jurídica de nuevas armas.
5. Establecer responsabilidades por daños derivados de su utilización.
6. Garantizar la compatibilidad con el derecho internacional humanitario.
7. Promover mecanismos internacionales de transparencia y cooperación tecnológica.

La gobernanza de estas tecnologías requiere un equilibrio entre los avances científicos, las necesidades legítimas de defensa y la protección de la dignidad humana.

5.6.8. Perspectivas estratégicas de la inteligencia artificial militar

La inteligencia artificial continuará transformando las capacidades militares y las relaciones de poder entre los Estados. Su desarrollo puede generar ventajas estratégicas para aquellos países que dispongan de infraestructuras tecnológicas avanzadas, capacidad de investigación, recursos económicos y personal especializado.

Sin embargo, la competencia por desarrollar sistemas militares cada vez más automatizados también puede generar nuevas formas de carrera tecnológica y aumentar las tensiones internacionales.

La falta de normas suficientemente desarrolladas puede favorecer interpretaciones divergentes sobre el uso legítimo de estas tecnologías y generar incertidumbre sobre los límites de la autonomía militar.

Por ello, la incorporación de inteligencia artificial en la defensa debe desarrollarse bajo principios de responsabilidad, supervisión humana, transparencia y cumplimiento del derecho internacional.

En definitiva, el principal desafío no consiste únicamente en determinar qué pueden hacer los sistemas autónomos, sino en establecer qué decisiones deben permanecer bajo responsabilidad humana y cuáles son los límites jurídicos y éticos que los Estados deben respetar.

5.7 Prevención de conflictos y construcción de confianza: diplomacia preventiva, cooperación técnica y gestión de crisis

5.7.1. Conceptualización de la prevención de conflictos en las relaciones internacionales

La prevención de conflictos constituye uno de los componentes fundamentales de la política exterior y de los mecanismos contemporáneos de seguridad internacional. Su finalidad consiste en identificar, analizar y gestionar situaciones de tensión antes de que evolucionen hacia enfrentamientos violentos o crisis de mayor magnitud. Desde esta perspectiva, la prevención representa una estrategia orientada a preservar la paz, fortalecer la estabilidad institucional y promover mecanismos de solución pacífica de controversias.

Tradicionalmente, la seguridad internacional se ha concentrado en la capacidad de los Estados para responder ante amenazas militares y conflictos armados. Sin embargo, la evolución del sistema internacional ha demostrado que las crisis pueden originarse en factores políticos, económicos, sociales, tecnológicos, ambientales y territoriales que, cuando no reciben una atención oportuna, pueden generar situaciones de inestabilidad.

En este contexto, la prevención de conflictos implica desarrollar capacidades institucionales para identificar factores de riesgo, establecer mecanismos de diálogo, fortalecer la cooperación y generar condiciones que reduzcan las posibilidades de confrontación.

Las Naciones Unidas consideran que la prevención constituye una función esencial de su mandato de mantenimiento de la paz y la seguridad internacionales. El Departamento de Asuntos Políticos y de Consolidación de la Paz destaca que la diplomacia preventiva comprende las medidas diplomáticas destinadas a evitar que las controversias escalen hasta convertirse en conflictos y a limitar su propagación cuando ya existen situaciones de tensión (United Nations Department of Political and Peacebuilding Affairs [DPPA], s. f.).

La prevención contemporánea requiere, por tanto, superar una concepción exclusivamente reactiva de la seguridad. En lugar de actuar únicamente cuando se produce una confrontación, los Estados y organismos internacionales deben desarrollar capacidades anticipatorias que permitan reconocer señales tempranas de inestabilidad y actuar mediante instrumentos diplomáticos, jurídicos, económicos y técnicos.

En el ámbito de la seguridad digital, esta perspectiva adquiere una importancia particular debido a que los incidentes cibernéticos pueden generar tensiones internacionales incluso cuando no existe una confrontación militar directa. Una operación contra infraestructuras críticas, una campaña de desinformación o una acusación de espionaje pueden deteriorar las relaciones entre países y provocar respuestas que incrementen el riesgo de escalada.

Por consiguiente, la prevención de conflictos en el entorno digital requiere combinar mecanismos tradicionales de diplomacia con instrumentos tecnológicos de monitoreo, intercambio de información y cooperación internacional.

5.7.2. Diplomacia preventiva como instrumento de estabilidad internacional

La diplomacia preventiva comprende el conjunto de iniciativas políticas y diplomáticas destinadas a evitar el surgimiento, la intensificación o la expansión de controversias internacionales.

Su fundamento consiste en reconocer que numerosos conflictos pueden prevenirse cuando existen mecanismos adecuados de comunicación, negociación y cooperación entre las partes involucradas.

La diplomacia preventiva puede desarrollarse mediante consultas bilaterales, mediación internacional, buenos oficios, misiones diplomáticas, mecanismos de alerta temprana y procesos de negociación multilateral.

A diferencia de la diplomacia orientada principalmente a resolver controversias ya establecidas, la diplomacia preventiva busca intervenir en etapas tempranas, cuando todavía existen posibilidades de gestionar las diferencias sin recurrir a medidas coercitivas o confrontaciones.

Entre sus principales características se encuentran:

a. Anticipación de situaciones de riesgo. Consiste en identificar acontecimientos políticos, económicos, sociales o tecnológicos que puedan generar tensiones entre Estados o dentro de una sociedad.
b. Comunicación permanente. Busca mantener canales de diálogo entre los actores involucrados para reducir las interpretaciones equivocadas y evitar que las diferencias se conviertan en confrontaciones.
c. Facilitación del entendimiento. Promueve espacios de negociación en los que las partes puedan identificar intereses comunes y establecer mecanismos de solución pacífica.
d. Neutralidad y legitimidad institucional. Los procesos preventivos requieren actores que puedan facilitar el diálogo y generar confianza entre las partes.
e. Continuidad del seguimiento. La prevención no concluye con la celebración de una reunión diplomática, sino que requiere supervisar los compromisos y evaluar la evolución de los factores que originaron la controversia.

La diplomacia preventiva también se desarrolla mediante mecanismos de buenos oficios, en los cuales un tercero facilita la comunicación entre las partes sin necesariamente intervenir directamente en el contenido de las negociaciones.

Las Naciones Unidas desempeñan un papel importante en este ámbito mediante las funciones del Secretario General, las misiones políticas especiales y el Departamento de

Asuntos Políticos y de Consolidación de la Paz. Estas estructuras permiten desarrollar análisis de conflictos, apoyar procesos de mediación y facilitar mecanismos de diálogo en diferentes regiones del mundo (DPPA, s. f.).

5.7.3. Alerta temprana y análisis de riesgos para la prevención de conflictos

Los mecanismos de alerta temprana permiten identificar condiciones que podrían generar conflictos y proporcionar información relevante para adoptar medidas preventivas.

Su funcionamiento requiere recopilar, organizar y analizar datos procedentes de diferentes fuentes, con el propósito de reconocer patrones que indiquen posibles escenarios de inestabilidad.

Tradicionalmente, los sistemas de alerta temprana han utilizado indicadores relacionados con la conflictividad social, la situación económica, los desplazamientos poblacionales, las tensiones políticas y las condiciones de seguridad.

En la actualidad, la incorporación de tecnologías digitales y herramientas de inteligencia artificial ha ampliado las posibilidades de análisis, permitiendo integrar grandes volúmenes de información y reconocer tendencias que podrían pasar inadvertidas mediante procedimientos convencionales.

La integración de estas dimensiones permite construir modelos de análisis de riesgos que consideren la interacción entre factores políticos, económicos, sociales, ambientales y tecnológicos.

Entre los principales indicadores utilizados para analizar situaciones de riesgo se encuentran:

Tabla 5.1

Indicadores de alerta temprana

Dimensión	Indicadores de alerta temprana
Política	Crisis institucionales, ruptura del diálogo, tensiones electorales y deterioro de las relaciones diplomáticas.
Económica	Inflación elevada, desempleo, inseguridad alimentaria y disputas comerciales.
Social	Protestas, polarización, desplazamientos poblacionales y conflictos comunitarios.
Militar	Incremento de tensiones fronterizas, movilización de fuerzas y amenazas de uso de la fuerza.
Tecnológica	Ataques cibernéticos, vulneraciones de infraestructuras críticas y campañas coordinadas de desinformación.
Ambiental	Escasez de agua, degradación de ecosistemas, eventos climáticos extremos y disputas por recursos naturales.

Por ejemplo, una situación de escasez hídrica en una región fronteriza puede generar tensiones cuando varios países dependen de una misma cuenca hidrográfica. Si esta situación coincide con una crisis económica, debilidad institucional y ausencia de mecanismos de cooperación, el riesgo de confrontación puede incrementarse.

De manera similar, una serie de ataques cibernéticos contra instituciones públicas durante una crisis diplomática puede interpretarse como una señal de escalada, especialmente cuando no existen canales de comunicación que permitan verificar su origen y finalidad.

La inteligencia artificial puede apoyar la construcción de modelos predictivos mediante técnicas de aprendizaje automático, análisis de series temporales y procesamiento del lenguaje natural. Estas herramientas permiten identificar asociaciones entre variables y estimar escenarios de riesgo.

Sin embargo, es necesario reconocer que los modelos predictivos no pueden determinar con certeza el comportamiento político de los actores internacionales. Sus resultados dependen de la calidad de los datos, la selección de variables y los supuestos utilizados.

Por ello, las estimaciones deben complementarse con análisis cualitativo, conocimiento territorial y evaluación de especialistas.

La alerta temprana resulta efectiva cuando la información obtenida se transforma en decisiones preventivas. La identificación de riesgos carece de utilidad si las instituciones no disponen de mecanismos para responder oportunamente.

5.7.4. Construcción de confianza como fundamento de la cooperación internacional

La construcción de confianza constituye una condición indispensable para desarrollar relaciones internacionales estables y mecanismos de cooperación sostenibles.

En términos generales, la confianza internacional puede entenderse como la expectativa de que los actores respetarán determinados compromisos, actuarán con transparencia y evitarán comportamientos que puedan generar daños injustificados a otros participantes del sistema internacional.

Esta confianza no implica la desaparición de las diferencias políticas o estratégicas entre los Estados. Su importancia radica en permitir que las controversias puedan gestionarse mediante procedimientos institucionales, evitando que la incertidumbre se transforme en confrontación.

La construcción de confianza requiere mecanismos de comunicación, intercambio de información, transparencia y cumplimiento de compromisos.

En el ámbito digital, estas condiciones adquieren particular relevancia debido a las dificultades para identificar a los responsables de determinadas operaciones y establecer las intenciones que las motivan.

Un ataque informático puede interpretarse como una actividad de espionaje, sabotaje o preparación de una operación más amplia. Cuando no existen mecanismos de consulta, el Estado afectado puede adoptar decisiones basadas en interpretaciones incompletas.

Por ello, la construcción de confianza en el ciberespacio requiere desarrollar mecanismos específicos que permitan:

- Intercambiar información sobre incidentes de seguridad digital.
- Establecer contactos directos entre autoridades competentes.

- Compartir buenas prácticas para la protección de infraestructuras críticas.
- Promover la transparencia sobre determinadas políticas y estrategias nacionales.
- Desarrollar procedimientos para consultar situaciones de riesgo.
- Facilitar investigaciones técnicas mediante cooperación internacional.
- Promover el cumplimiento de normas de comportamiento responsable.

La construcción de confianza también requiere reconocer las diferencias existentes entre los países en cuanto a capacidades tecnológicas, recursos económicos y desarrollo institucional. La cooperación debe contribuir a reducir estas desigualdades y evitar que las brechas digitales se conviertan en nuevas fuentes de vulnerabilidad internacional.

5.7.5. Medidas de fomento de la confianza en el ciberespacio

Las medidas de fomento de la confianza, conocidas internacionalmente como Confidence-Building Measures (CBMs), constituyen instrumentos destinados a reducir las tensiones, mejorar la comunicación y evitar interpretaciones equivocadas sobre las actividades de los Estados.

En el entorno cibernético, estas medidas buscan disminuir la incertidumbre respecto de las capacidades, intenciones y comportamientos de los actores internacionales.

El desarrollo de estas iniciativas responde a la necesidad de establecer mecanismos de transparencia y comunicación en un ámbito donde las operaciones pueden ejecutarse de manera remota y sus consecuencias pueden afectar a diferentes países.

Entre las principales medidas se encuentran las siguientes:

a) Establecimiento de puntos de contacto nacionales

Los Estados pueden designar autoridades responsables de mantener comunicación directa con sus homólogos internacionales durante incidentes cibernéticos.

Estos puntos de contacto permiten intercambiar información, coordinar consultas y facilitar respuestas institucionales.

b) Intercambio de información técnica

La cooperación puede incluir el intercambio de alertas sobre vulnerabilidades, indicadores de compromiso, patrones de amenazas y recomendaciones de protección.

Esta información contribuye a fortalecer las capacidades de prevención y respuesta de los países participantes.

c) Notificación de incidentes relevantes

Los mecanismos de notificación permiten comunicar oportunamente incidentes que puedan afectar infraestructuras críticas o generar consecuencias transfronterizas.

Su finalidad consiste en reducir la incertidumbre y facilitar la coordinación antes de que una situación se transforme en una crisis diplomática.

d) Ejercicios conjuntos de simulación

Los Estados pueden desarrollar ejercicios técnicos y diplomáticos para evaluar su capacidad de respuesta ante escenarios hipotéticos de ataques informáticos, interrupciones de servicios o crisis internacionales.

Estos ejercicios permiten identificar debilidades institucionales y fortalecer los procedimientos de coordinación.

e) Intercambio de políticas y buenas prácticas

La presentación de estrategias nacionales, marcos regulatorios y protocolos de respuesta facilita la comprensión de los enfoques adoptados por otros Estados.

f) Mecanismos de consulta y resolución de controversias

Los canales de consulta permiten aclarar situaciones de tensión y reducir el riesgo de respuestas basadas en atribuciones incorrectas.

Las medidas de fomento de la confianza no eliminan las diferencias estratégicas entre los Estados, pero proporcionan instrumentos para gestionar esas diferencias de manera pacífica.

En consecuencia, su aplicación constituye una dimensión importante de la gobernanza internacional del ciberespacio y de la prevención de conflictos.

5.7.6. Cooperación técnica internacional y fortalecimiento de capacidades

La cooperación técnica constituye uno de los mecanismos fundamentales para reducir las vulnerabilidades tecnológicas y fortalecer las capacidades de los Estados frente a amenazas transnacionales.

Su importancia radica en que la seguridad digital depende de conocimientos especializados, infraestructura tecnológica, recursos humanos y mecanismos institucionales que no se encuentran distribuidos de manera uniforme entre los países.

Mientras algunos Estados disponen de centros avanzados de investigación, sistemas nacionales de respuesta y capacidades especializadas de análisis, otros enfrentan limitaciones presupuestarias, falta de profesionales y dependencia de proveedores externos.

Estas diferencias pueden generar asimetrías que afectan la capacidad de prevenir incidentes y participar en condiciones de mayor igualdad en los procesos internacionales de gobernanza digital.

La cooperación técnica busca superar estas limitaciones mediante iniciativas de formación, transferencia de conocimientos, asistencia tecnológica y desarrollo de capacidades institucionales.

Entre sus principales modalidades se encuentran:

1. Formación de especialistas. Los programas de capacitación permiten desarrollar competencias en ciberseguridad, análisis forense digital, protección de infraestructuras críticas, inteligencia artificial y gestión de incidentes.
2. Fortalecimiento de equipos de respuesta. La creación y consolidación de equipos nacionales CERT o CSIRT permite mejorar la detección, coordinación y gestión de incidentes de seguridad informática.
3. Transferencia de conocimientos tecnológicos. La cooperación universitaria y científica facilita el acceso a metodologías, herramientas y conocimientos especializados.

4. Desarrollo de infraestructuras seguras. Los proyectos de cooperación pueden contribuir a fortalecer centros de datos, redes de comunicación, sistemas de almacenamiento y mecanismos de respaldo.
5. Investigación conjunta. La colaboración entre universidades, centros de investigación y organismos gubernamentales permite desarrollar soluciones adaptadas a las necesidades de cada país.
6. Asistencia técnica internacional. Los organismos multilaterales y las instituciones especializadas pueden proporcionar asesoramiento para elaborar estrategias nacionales de ciberseguridad, marcos regulatorios y protocolos de gestión de crisis.

La cooperación técnica también debe contemplar la dimensión académica y científica. Las universidades desempeñan un papel relevante en la formación de profesionales, el desarrollo de investigación aplicada y la generación de conocimientos para enfrentar amenazas tecnológicas.

En este sentido, la colaboración entre instituciones de educación superior, organismos gubernamentales y centros internacionales de investigación puede fortalecer las capacidades nacionales y contribuir a una gobernanza digital más inclusiva.

5.7.7. Gestión de crisis internacionales en el entorno digital

La gestión de crisis comprende el conjunto de procedimientos políticos, diplomáticos, técnicos e institucionales destinados a controlar situaciones que amenazan la estabilidad de los Estados o las relaciones internacionales.

En el entorno digital, una crisis puede originarse por un ataque cibernético contra una infraestructura crítica, una vulneración de información diplomática, una operación de desinformación o una interrupción significativa de servicios esenciales.

La particularidad de estas situaciones radica en que pueden desarrollarse rápidamente, involucrar actores ubicados en diferentes jurisdicciones y producir consecuencias que afectan simultáneamente a diversos sectores.

Una crisis cibernética puede adquirir dimensiones internacionales cuando los Estados interpretan un incidente como una acción hostil, cuando se comprometen servicios

transfronterizos o cuando las consecuencias de una operación afectan intereses estratégicos.

La gestión de estas situaciones requiere integrar capacidades técnicas y diplomáticas.

Entre sus principales etapas se encuentran:

Primera etapa: identificación y evaluación de la crisis.

Consiste en reconocer el incidente, determinar los sistemas afectados y estimar sus posibles consecuencias.

En esta fase es fundamental diferenciar entre fallas técnicas, errores operativos y actividades deliberadamente maliciosas.

Segunda etapa: activación de mecanismos institucionales.

Las autoridades competentes deben activar los protocolos de respuesta, establecer responsabilidades y coordinar las acciones entre organismos gubernamentales y operadores privados.

Tercera etapa: comunicación y consulta diplomática.

Cuando existen posibles implicaciones internacionales, deben utilizarse canales diplomáticos para informar a las partes involucradas y reducir el riesgo de interpretaciones equivocadas.

Cuarta etapa: contención y respuesta técnica.

Comprende las acciones destinadas a limitar los efectos del incidente, proteger los sistemas y restablecer los servicios afectados.

Quinta etapa: evaluación de responsabilidades.

Una vez recopiladas las evidencias, deben examinarse las posibles causas, los actores involucrados y las implicaciones jurídicas y políticas.

Sexta etapa: recuperación y aprendizaje institucional.

Después de controlar la crisis, es necesario evaluar las respuestas, identificar debilidades y actualizar los protocolos de prevención.

Este proceso demuestra que la gestión de crisis no puede depender exclusivamente de los equipos técnicos. Requiere coordinación entre autoridades políticas, instituciones de seguridad, organismos jurídicos, especialistas tecnológicos y representantes diplomáticos.

5.7.8. Comunicación de crisis y prevención de errores de interpretación

La comunicación constituye un elemento determinante durante la gestión de crisis internacionales.

Cuando ocurre un incidente cibernético, la ausencia de información confiable puede favorecer la circulación de rumores, interpretaciones equivocadas y acusaciones prematuras.

Por esta razón, las instituciones deben desarrollar protocolos de comunicación que permitan transmitir información verificada, explicar las acciones adoptadas y mantener canales de diálogo con los actores involucrados.

Una comunicación de crisis efectiva debe considerar los siguientes principios:

- Veracidad: los mensajes deben fundamentarse en información comprobada y distinguir los hechos confirmados de las hipótesis.
- Oportunidad: las instituciones deben informar con rapidez, evitando vacíos informativos que puedan ser aprovechados por actores maliciosos.
- Coherencia: las declaraciones de las diferentes instituciones deben mantener consistencia con las posiciones oficiales del Estado.
- Proporcionalidad: la comunicación debe evitar declaraciones que incrementen innecesariamente las tensiones.
- Transparencia: es necesario proporcionar información suficiente para fortalecer la confianza pública, respetando los límites de confidencialidad y seguridad.
- Coordinación internacional: cuando el incidente tiene implicaciones transfronterizas, los mensajes deben acompañarse de mecanismos de consulta diplomática.

La comunicación de crisis también debe considerar el riesgo de contenidos sintéticos y campañas de desinformación. En consecuencia, las autoridades necesitan mecanismos para verificar la autenticidad de declaraciones, imágenes y documentos que circulan durante situaciones de emergencia.

Una respuesta comunicacional descoordinada puede agravar una crisis técnica y transformarla en un problema político o diplomático.

Por el contrario, la información verificable y la existencia de canales institucionales de comunicación pueden contribuir a reducir la incertidumbre y evitar la escalada.

5.7.9. Cooperación multilateral y mecanismos internacionales para la prevención de conflictos

La prevención de conflictos y la construcción de confianza requieren mecanismos multilaterales que permitan coordinar acciones entre Estados y organizaciones internacionales.

Las Naciones Unidas desempeñan un papel central en este ámbito mediante su mandato de mantenimiento de la paz y la seguridad internacionales, la mediación de controversias y el desarrollo de normas de comportamiento responsable.

El Grupo de Expertos Gubernamentales sobre el comportamiento responsable de los Estados en el ciberespacio destacó la importancia de aplicar el derecho internacional, promover normas voluntarias de comportamiento responsable y fortalecer las medidas de fomento de la confianza y la cooperación internacional (United Nations General Assembly, 2021).

Estos mecanismos pueden complementarse con iniciativas regionales, acuerdos bilaterales y programas de cooperación técnica.

La participación de organismos regionales resulta particularmente importante porque permite considerar las características geográficas, políticas, económicas y culturales de cada entorno.

En América Latina, por ejemplo, la cooperación en ciberseguridad y prevención de conflictos puede orientarse al fortalecimiento de infraestructuras críticas, la protección de

servicios públicos, el desarrollo de capacidades nacionales y la coordinación ante amenazas transfronterizas.

Los países de la región enfrentan desafíos relacionados con la desigualdad tecnológica, la dependencia de proveedores externos, la protección de datos y la necesidad de fortalecer sus instituciones de seguridad digital.

Por ello, la cooperación regional debe incorporar mecanismos de intercambio de información, capacitación especializada, investigación científica y desarrollo de marcos de gobernanza compatibles con el respeto a los derechos fundamentales.

5.7.10. Prevención de conflictos, gobernanza tecnológica y estabilidad internacional

La prevención de conflictos en el entorno contemporáneo requiere comprender que la seguridad internacional depende de factores interrelacionados. Las tecnologías digitales, la inteligencia artificial, las infraestructuras críticas y los sistemas de comunicación se han convertido en componentes esenciales de la estabilidad económica, política y social.

En consecuencia, los Estados deben desarrollar estrategias que integren la diplomacia preventiva con la cooperación técnica y la gestión de riesgos tecnológicos.

La gobernanza internacional debe promover mecanismos de transparencia, diálogo y coordinación que permitan reducir la incertidumbre sobre las actividades de los diferentes actores.

Asimismo, resulta necesario fortalecer la participación de universidades, centros de investigación, organizaciones internacionales y empresas tecnológicas, debido a que poseen conocimientos y capacidades indispensables para enfrentar amenazas complejas.

La construcción de confianza requiere reconocer que la seguridad de un Estado no puede alcanzarse de manera aislada. La interdependencia tecnológica implica que una vulnerabilidad en un país puede afectar a otros mediante redes de comunicación, servicios en la nube, sistemas financieros y cadenas globales de suministro.

Por ello, la cooperación internacional no debe limitarse a responder ante incidentes, sino que debe orientarse a desarrollar capacidades preventivas y mecanismos permanentes de coordinación.

En definitiva, la diplomacia preventiva, la cooperación técnica y la gestión de crisis constituyen instrumentos complementarios para preservar la estabilidad internacional. Su articulación permite transformar la competencia tecnológica en oportunidades de colaboración y reducir los riesgos de que las diferencias políticas se conviertan en confrontaciones.

REFERENCIAS BIBLIOGRÁFICAS

Allison, G. (2017). Destined for war: Can America and China escape Thucydides's trap? Houghton Mifflin Harcourt.

Baldwin, R. (2016). The great convergence: Information technology and the new globalization. Harvard University Press.

Bjola, C., & Holmes, M. (Eds.). (2015). Digital diplomacy: Theory and practice. Routledge.

Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.

Bull, H. (2012). The anarchical society: A study of order in world politics (4th ed.). Palgrave Macmillan.

Castells, M. (2010). The rise of the network society (2nd ed.). Wiley-Blackwell.

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820.

Dahl, R. A. (1957). The concept of power. Behavioral Science, 2(3), 201–215.

Drucker, P. F. (1993). Post-capitalist society. HarperBusiness.

European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union, L 119, 1–88.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42–79. https://doi.org/10.1162/isec_a_00351

Floridi, L. (2014). The fourth revolution: How the infosphere is reshaping human reality. Oxford University Press.

Gilpin, R. (2001). Global political economy: Understanding the international economic order. Princeton University Press.

Held, D., & McGrew, A. (2007). Globalization/anti-globalization: Beyond the great divide (2nd ed.). Polity Press.

Ikenberry, G. J. (2018). The end of liberal international order? International Affairs, 94(1), 7–23.

Keck, M. E., & Sikkink, K. (1998). Activists beyond borders: Advocacy networks in international politics. Cornell University Press.

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

Keohane, R. O., & Nye, J. S. (2012). Power and interdependence (4th ed.). Longman.

Kissinger, H. (2014). World order. Penguin Press.

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

Lee, K.-F. (2018). AI superpowers: China, Silicon Valley, and the new world order. Houghton Mifflin Harcourt.

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

Mearsheimer, J. J. (2001). The tragedy of great power politics. W. W. Norton & Company.

Miller, C. (2022). Chip war: The fight for the world's most critical technology. Scribner.

Morgenthau, H. J. (2006). Politics among nations: The struggle for power and peace (7th ed.). McGraw-Hill.

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

O'Brien, R., & Williams, M. (2020). Global political economy: Evolution and dynamics (6th ed.). Red Globe Press.

Osiander, A. (2001). Sovereignty, international relations, and the Westphalian myth. International Organization, 55(2), 251–287.

Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.

Scharre, P. (2018). Army of none: Autonomous weapons and the future of war. W. W. Norton & Company.

Schwab, K. (2016). The fourth industrial revolution. World Economic Forum.

Slaughter, A.-M. (2004). A new world order. Princeton University Press.

Srnicek, N. (2017). Platform capitalism. Polity Press.

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

Teschke, B. (2003). The myth of 1648: Class, geopolitics, and the making of modern international relations. Verso.

Waltz, K. N. (1979). Theory of international politics. Addison-Wesley.

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

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

Fuentes de organismos internacionales

National Institute of Standards and Technology. (2024). A plan for global engagement on AI standards (NIST Trustworthy and Responsible AI, NIST AI 100-5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-5

Organisation for Economic Co-operation and Development. (2019). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). OECD.

Organisation for Economic Co-operation and Development. (2024). Recommendation of the Council on Artificial Intelligence: Amended on 3 May 2024 (OECD/LEGAL/0449). OECD.

United Nations General Assembly. (2021). Advancing responsible State behaviour in cyberspace in the context of international security: Report of the Group of Governmental Experts (A/76/135). United Nations.

United Nations General Assembly. (2023). Interim report: Governing AI for humanity. United Nations.

United Nations General Assembly. (2024). Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (A/RES/78/265). United Nations.

United Nations Conference on Trade and Development. (2024). Digital economy report 2024: Shaping an environmentally sustainable and inclusive digital future. United Nations.

United Nations Educational, Scientific and Cultural Organization. (2021). Recommendation on the ethics of artificial intelligence. UNESCO.

EDITORIAL ANDES COGNITIO



Adriana Yamilet Herrera Granizo

Economista (Universidad Nacional de Chimborazo), Máster en Economía Circular y Desarrollo Sostenible (Universidad Internacional de Valencia) y Máster en Gestión de Proyectos (Universidad Internacional de Valencia). Ha trabajado como Consultor Senior en INFODATOS), desarrollando actividades de consultoría especializada y asesoría empresarial en el sector privado. Jefe de Auditoría en Hiladera Guijarro, responsable de la planificación, ejecución y supervisión de procesos de auditoría interna. Editor en CEFRO, encargado de la revisión, edición y gestión de contenidos institucionales y editoriales. Editor en jefe del Rist-Dírham de los Emiratos Árabes Unidos y ScriptSpace Journals de la India, liderando la dirección editorial, coordinación de publicaciones y control de calidad de contenidos. Docente de la Universidad de las Fuerzas Armadas (ESPE), impartiendo asignaturas de formación profesional y contribuyendo al desarrollo académico de estudiantes universitarios. Autora de artículos sobre sostenibilidad, teoría de juegos y economía circular en revistas indexadas. Actualmente lidera proyectos sobre inversiones circulares en parques ecoindustriales y simbiosis hídrica.



Norelyn Tatiana Mejia Basantes

Economista (Universidad Nacional de Chimborazo), Magíster en Gestión de Proyectos (Universidad Técnica Particular de Loja) y Doctoranda en Economía y Finanzas (UIIX). Ha participado en programas de movilidad académica internacional en la Universidad Popular Autónoma del Estado de Puebla (México) y en la Universidad EAFIT (Colombia), fortaleciendo sus competencias en investigación, innovación y cooperación académica. Cuenta con experiencia en docencia, investigación y gestión de proyectos, participando en actividades orientadas al desarrollo académico y científico. Es autora de trabajos de investigación en las áreas de desarrollo económico, competitividad empresarial, sostenibilidad, responsabilidad social corporativa, capital intelectual e innovación organizacional. Sus intereses de investigación se centran en el análisis de los factores que impulsan la competitividad y el desarrollo sostenible de las organizaciones, contribuyendo a la generación de conocimiento científico para la toma de decisiones y el desarrollo económico.



Jhonathan Alexis Meneses Flores

Economista por la Universidad Nacional de Chimborazo y candidato a Máster Universitario en Economía Internacional por la Universidad Internacional de La Rioja (UNIR), España. Cuenta con experiencia profesional en análisis financiero, evaluación de proyectos, gestión administrativa, coordinación institucional y elaboración de herramientas e indicadores para la toma de decisiones, desarrollada en organizaciones públicas y privadas de Ecuador y España. Su trayectoria incluye actividades relacionadas con análisis de rentabilidad y viabilidad de proyectos, proyecciones financieras, estudios de mercado, gestión de cartera, evaluación crediticia y elaboración de reportes e instrumentos de seguimiento. Asimismo, ha participado en proyectos socioeconómicos vinculados con inclusión financiera y desarrollo productivo, además de brindar consultoría financiera a emprendedores y pequeñas empresas. En el ámbito académico e investigativo, ha participado en trabajos de investigación y producción científica en áreas vinculadas con economía, finanzas, regulación y desarrollo, con contribuciones aceptadas y publicadas en revistas académicas internacionales.



Marlene Isabel Coronel Grados

Ingeniera en Empresas Turísticas y Áreas Naturales por la Universidad Tecnológica Equinoccial (UTE), con un Máster en Dirección de Proyectos de Ocio, Cultura, Turismo, Deporte y Recreación por la Universidad de Deusto (España) y una Maestría en Gestión de Turismo Sostenible por la Universidad para la Cooperación Internacional (Costa Rica). Cuenta con certificación de inglés B1 y amplia experiencia en docencia universitaria, dirección de tesis y gestión académica en el ámbito turístico. Actualmente es docente y directora de tesis en la Carrera de Turismo de la Universidad de las Fuerzas Armadas – ESPE y docente del Instituto Superior Tecnológico Internacional (ITI). Su experiencia comprende gestión de destinos, guianza, animación turística y procesos de acreditación académica. Mantiene una trayectoria investigativa en administración, sostenibilidad y turismo de patrimonio cultural, con seis artículos publicados entre 2017 y 2025 sobre turismo sostenible, patrimonio cultural, gastronomía, ecoturismo y tecnologías aplicadas al turismo.



Danny Fernando Chiriboga Barba

cuenta con una destacada trayectoria académica y profesional vinculada al turismo, la investigación, la educación y la gestión cultural. Su formación comprende una Licenciatura en Administración de Empresas de Turismo, un Diplomado en Investigación Educativa, una Maestría en Educación, una Maestría en Ecoturismo y Manejo de Áreas Naturales y un Doctorado en Ciencias Económicas, obtenido en la Facultad de Turismo de la Universidad de La Habana, Cuba. Su experiencia investigativa se refleja en la publicación de artículos científicos y libros especializados en turismo cultural, gestión turística, ecoturismo, patrimonio y aprovechamiento sostenible de los recursos naturales. En el ámbito profesional, ha ejercido funciones como docente, capacitador y asesor en instituciones públicas y de educación superior, además de desempeñarse en la gestión de agencias de viajes, proyectos turísticos, seguridad turística, arte y gestión cultural.

Asimismo, ha participado en procesos de asesoría y capacitación relacionados con ecoturismo, gestión turística y desarrollo sostenible, contribuyendo al fortalecimiento de iniciativas orientadas a la conservación del patrimonio, la innovación y la competitividad del sector. Su trayectoria integra formación académica, experiencia práctica, investigación y gestión, consolidando un perfil profesional caracterizado por el liderazgo, la capacidad de gestión y el compromiso con la formación de talento humano y el desarrollo sostenible del turismo.

ISBN: 978-9907-9566-7-2