MANUAL DE CIBERDIPLOMACIA PARA LA CONVERGENCIA REGIONAL

SISTEMA ECONÓMICO
LATINOAMERICANO
Y DEL CARIBE

MANUAL DE
CIBERDIPLOMACIA
PARA LA CONVERGENCIA REGIONAL

SISTEMA ECONÓMICO
LATINOAMERICANO
Y DEL CARIBE

Manual de Ciberdiplomacia para la Convergencia Regional

Autor:
Sistema Económico Latinoamericano y del Caribe (SELA)
Dirección editorial:
Clarems Endara, Secretario Permanente del SELA
Coordinación de publicaciones:
Yeimy Ramírez Ávila. Jefe de Gabinete.
Supervisión editorial:
Yeimy Ramírez Ávila. Jefe de Gabinete.
Klibis Marín. Oficial de Comunicaciones
Maquetación:
Claudio M Gaitán
Impresión:
MACRO SRL. La Paz - Bolivia

ISBN digital: 978-980-6458-16-1

Depósito Legal: 2024000201

ÍNDICE

PRÓLOGO

América Latina y el Caribe (ALC) es una región que se destaca por su vasta riqueza cultural y natural, y por haber sido escenario de significativas transformaciones económicas en tiempos recientes. En medio de este dinamismo y de los desafíos globales existentes, la cooperación regional y la formulación de estrategias para un desarrollo sostenible adquieren una relevancia irremplazable. En este contexto, emerge el Sistema Económico Latinoamericano y del Caribe (SELA), una entidad intergubernamental fundada en 1975, dedicada a potenciar la cooperación y la integración económicas entre naciones latinoamericanas y caribeñas y cuya labor se enfoca en catalizar el diálogo intergubernamental y en promover el diseño de políticas regionales que atiendan desafíos económicos compartidos.

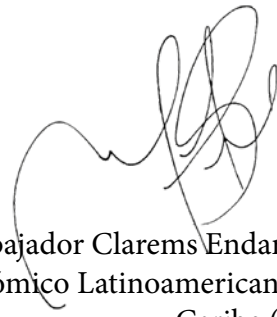
El SELA se centra actualmente en tres grandes ejes temáticos primordiales, a saber: recuperación económica, digitalización e infraestructura y desarrollo social, áreas que abarcan temáticas cruciales como comercio, tecnología, agricultura, energía, medio ambiente y otros pilares del desarrollo regional. Con una visión clara, el SELA ha impulsado esfuerzos en ámbitos como la ciberdiplomacia, tema sobre el que dicta cursos, a fin de explorar su potencial para impulsar la recuperación y el desarrollo regionales, y que da origen a este Manual de ciberdiplomacia para la convergencia regional.

La ciberdiplomacia, en particular, representa un puente hacia el futuro, donde las fronteras digitales superan las geográficas. En un mundo cada vez más interconectado, la capacidad de navegar y aprovechar las oportunidades que brinda el ciberespacio se convierte en un imperativo estratégico. Las herramientas digitales, las plataformas de comunicación y las redes sociales no son solo instrumentos de interacción, sino también canales para

construir confianza, resolver conflictos y promover intereses compartidos. En este sentido, el SELA reconoce la importancia de abordar la ciberdiplomacia como una necesidad y como una oportunidad para redefinir y fortalecer las relaciones entre países y generar un espacio de cooperación y entendimiento recíprocos.

Es esencial subrayar que la visión del SELA trasciende las meras relaciones económicas y políticas y apunta hacia la construcción de un tejido social y cultural robusto que exprese cabalmente la diversidad, la inclusión y el respeto mutuo. En este contexto, el manual aborda cómo la ciberdiplomacia puede ser una herramienta para promover valores compartidos, combatir la desinformación y fortalecer la identidad regional. Al fomentar una visión integrada y convergente que abarque los aspectos tanto técnicos como humanos de la diplomacia en el ciberespacio, aspira a ser una brújula para los líderes y ciudadanos comprometidos con el futuro próspero y unificado de ALC.

Concebido a partir del análisis y de la reflexión sobre experiencias y conocimientos previos, más que una compilación académica, este libro es un llamado a la acción. En un entorno global dinámico, la adaptación y la innovación son claves para garantizar el desarrollo sostenible, mejorar la calidad de vida e incentivar el diálogo y las acciones que promuevan no solo una mayor y más efectiva integración, sino también un horizonte económico más robusto y prometedor para la región.



Embajador Clarems Endara Vera
Secretario Permanente del Sistema Económico Latinoamericano y del Caribe (SELA)

INTRODUCCIÓN

ALC, una región rica en diversidad cultural, histórica y geográfica, enfrenta desafíos que trascienden las fronteras convencionales. La revolución digital de las últimas décadas ha transformado la manera en que las personas y los Estados interactúan, colaboran y, en ocasiones, compiten en el escenario internacional. En este contexto dinámico, la ciberdiplomacia emerge como una herramienta crucial para fortalecer la convergencia regional y promover un desarrollo sostenible y equitativo.

La cuarta revolución industrial ha traído consigo una serie de transformaciones radicales en todos los aspectos de la sociedad, desde la economía hasta la cultura y la política. En la región, el rápido avance de las tecnologías digitales ha generado oportunidades significativas, pero también ha exacerbado las brechas existentes en términos de acceso, capacitación y gobernanza digital.

El desafío actual radica en adaptarse a las constantes y necesarias transformaciones tecnológicas y digitales que están alterando no solo la economía, sino también los procesos de integración. Tal revolución tecnológica presenta tanto desafíos como oportunidades importantes en áreas como el comercio electrónico, la economía digital y la automatización de procesos productivos. Estas representan campos donde podemos promover una integración más sólida y efectiva. Por esta razón, y buscando una integración mayor y mejor, el SELA (2023a) pone un fuerte énfasis en promover la adopción de nuevas tecnologías y el desarrollo de capacidades digitales en la región, con el objetivo de abordar de manera integral la gestión de la brecha digital. En este escenario, la ciberdiplomacia se presenta como un

instrumento esencial para navegar por las complejidades de un mundo interconectado, protegiendo al mismo tiempo sus intereses y valores.

La ciberdiplomacia y la diplomacia digital, ambas relacionadas con el uso estratégico de las tecnologías de la información y la comunicación (TIC) para conducir las relaciones internacionales, ofrecen oportunidades sin precedentes. Más allá de los desafíos particulares en materia de desarrollo económico, social y político, puede encontrarse en la ciberdiplomacia un vehículo para potenciar la cooperación, mejorar la gobernanza sobre el mundo digital y enfrentar amenazas cibernéticas transnacionales.

Si bien la digitalización presenta oportunidades sin igual para el crecimiento económico, la inclusión social y la innovación, también plantea desafíos significativos en términos de seguridad cibernética, privacidad de datos y soberanía digital. Por lo tanto, no solo se trata de establecer relaciones diplomáticas en el ámbito virtual, sino también de abordar estos desafíos de manera colaborativa y estratégica. A través de la cooperación regional, los países latinoamericanos y caribeños pueden fortalecer sus capacidades cibernéticas, promover normas y estándares comunes y construir una infraestructura digital resiliente y segura.

El SELA, como organismo comprometido con la integración económica y el desarrollo sostenible, reconoce la importancia de adaptarse a este nuevo paradigma diplomático. Por ello, este manual tiene como objetivo proporcionar una guía sobre cómo los países latinoamericanos y caribeños pueden aprovechar las herramientas y estrategias de la ciberdiplomacia para avanzar hacia una mayor convergencia regional. De esta manera, el SELA se posiciona como una plataforma para el intercambio de mejores prácticas y para el establecimiento de lineamientos generales en materia de ciberseguridad y gobernanza digital.

El presente manual, por ende, busca contribuir a los esfuerzos de este organismo y de otros actores regionales para fortalecer la convergencia digital en ALC, asegurando que la región no solo participe activamente en el escenario internacional, sino que también defienda y promueva sus intereses y valores en el ámbito digital.

A lo largo de sus páginas, se explican los principios fundamentales de la ciberdiplomacia, se analizan casos de éxito y desafíos y se ofrecen recomendaciones para elaborar políticas cibernéticas efectivas. Al hacerlo, se aspira a contribuir al fortalecimiento de la cooperación regional, la construcción de confianza entre Estados y la promoción de un espacio digital seguro, abierto e inclusivo para todos los ciudadanos latinoamericanos y caribeños.

En última instancia, este manual busca ser una herramienta para diplomáticos, funcionarios públicos, académicos y otros actores interesados en el futuro de ALC en la era digital de la información. Por ello, se invita a los lectores a embarcarse en este viaje hacia una ciberdiplomacia regional que refleje los valores, los intereses y las aspiraciones compartidas por los países de la región.

Algunas consideraciones sobre la ciberdiplomacia y la diplomacia digital

En la era digital o de la información, términos como ciberdiplomacia (*cyber diplomacy*), diplomacia digital (*Digiplomacy o eDiplomacy*) y diplomacia electrónica o e-diplomacia (e-diplomacy) a menudo se utilizan indistintamente, generando confusión sobre sus significados y aplicaciones específicas. Sin embargo, es muy necesario comprender las diferencias sutiles entre estos conceptos para navegar eficazmente en el complejo panorama de las relaciones internacionales en línea.

La ciberdiplomacia se refiere al uso estratégico de las tecnologías cibernéticas y de la información en el ámbito de las relaciones internacionales y a la capacidad de los Estados para ponerse de acuerdo en la regulación del mundo digital. Este enfoque va más allá de la mera comunicación en línea para incluir aspectos como la ciberseguridad, la gobernanza del ciberespacio y la protección de infraestructuras críticas. Implica la adopción de políticas, estrategias y acciones específicas para promover los intereses nacionales en un entorno digital, abordando tanto las oportunidades como los desafíos que presenta el ciberespacio en el ámbito internacional. No debe perderse de vista que el ciberespacio no solo está regido por normas estatales (en tanto impuestas por los distintos Estados nación), sino por los códigos, las contraseñas, los algoritmos, los usos y costumbres de sus usuarios, etc.

(Riordan, 2019). Esto implica un desafío a la comunidad internacional para regularlo sin que se pierda la libertad de expresión en estos espacios.

La gobernanza del ciberespacio es, entonces, determinante, ya que este es un espacio político, entre otras cosas. **En ese sentido, la ciberdiplomacia se refiere al empleo de la diplomacia para proteger los intereses de un país en el mundo digital.** Esto incluye temas como la seguridad en línea, la lucha contra delitos cibernéticos y cómo se maneja y regula internet (Barrinha y Renard, 2017). Los diplomáticos trabajan en este campo, tanto en conversaciones entre dos países como en discusiones con muchos países en organizaciones como Naciones Unidas (ONU). Además, no solo hablan con otros países, sino también con los siguientes actores: importantes empresas de tecnología o *big tech companies*, como Meta o Google, emprendedores del mundo digital y grupos de personas que centran sus preocupaciones en los usos de internet.

Por otro lado, la diplomacia digital se centra, principalmente, en el uso de plataformas y herramientas para facilitar la comunicación, la cooperación y la negociación entre Estados y actores internacionales. Esto incluye el uso de redes sociales, aplicaciones de mensajería y plataformas en línea para promover el diálogo diplomático, la diplomacia pública y la participación ciudadana en los asuntos internacionales. Efectivamente, "los medios de comunicación desempeñan cada día un papel más relevante en la creación de opinión; la cuestión es que hoy esos medios no son solo los tradicionales" (Rodríguez Gómez, 2015, p. 920). La diplomacia digital se enfoca, entonces, en el aprovechamiento de las tecnologías digitales para mejorar la eficiencia, la transparencia y la accesibilidad de las prácticas diplomáticas tradicionales, teniendo en cuenta este contexto donde los "medios no tradicionales" han ganado terreno.

Mientras tanto, el término e-diplomacia se utiliza, a menudo, como un concepto más amplio que abarca tanto la diplomacia digital como otros aspectos de la diplomacia electrónica, como el intercambio de información, la gestión de datos y la colaboración en línea entre Estados y organizaciones internacionales. La e-diplomacia engloba una variedad de herramientas y prácticas que facilitan la comunicación y la cooperación en el ámbito di-

plomático y permiten a los actores internacionales adaptarse y responder de manera efectiva a los desafíos y oportunidades de la era digital. Hoy la política exterior ya no se limita a lo oficial, pues ahora tanto empresas privadas como individuos también participan activamente en ella, en especial, en las áreas de diplomacia pública y corporativa en diferentes formas (Rodríguez Gómez, 2015).

Además de la distinción conceptual entre ciberdiplomacia, diplomacia digital y diplomacia electrónica, es esencial reconocer cómo estos términos se interrelacionan en la práctica y cómo han evolucionado con el advenimiento de nuevas tecnologías y dinámicas globales. La digitalización ha transformado no solo la forma en que los Estados interactúan entre sí, sino también cómo se comunican, negocian y colaboran en un mundo cada vez más conectado. En este contexto, la ciberdiplomacia se ha convertido en un campo emergente que exige una comprensión profunda de las dimensiones técnicas, políticas y estratégicas del ciberespacio.

Una de las principales características distintivas de la ciberdiplomacia es su enfoque holístico, que, además de la comunicación y la cooperación, abarca otros aspectos cruciales como la seguridad cibernética, la soberanía y la protección de los derechos humanos en el ámbito digital. Esto contrasta con la diplomacia digital, que, si bien se centra en las herramientas y plataformas digitales, puede no abordar plenamente los desafíos y amenazas específicos asociados con el ciberespacio, como los ciberataques, la desinformación y la manipulación en línea.

Por otro lado, la e-diplomacia ofrece un marco más amplio que permite a los actores internacionales adaptarse y responder de manera proactiva a las rápidas transformaciones tecnológicas y geopolíticas, dado que facilita la colaboración transnacional, el intercambio de mejores prácticas y la construcción de capacidades en áreas clave como la ciberseguridad, la gobernanza del ciberespacio y la innovación tecnológica. Al integrar herramientas y enfoques de la ciberdiplomacia y la diplomacia digital, la e-diplomacia permite a los Estados y organizaciones internacionales desarrollar estrategias más cohesivas y eficaces para enfrentar los complejos desafíos y oportunidades de la era digital. En este sentido es que a menudo se con-

funden dos ideas distintas: el uso de herramientas digitales por parte de diplomáticos y la diplomacia en el mundo digital. Mientras que la primera configura tanto la e-diplomacia como la diplomacia digital, que es cuando los diplomáticos usan tecnologías y redes sociales en su trabajo tradicional, la segunda se refiere al tema de interés de este manual: la diplomacia enfocada en el ciberespacio (Barrinha y Renard, 2017; Riordan, 2019).

Sin embargo, a pesar de que la ciberdiplomacia, la diplomacia digital y la e-diplomacia tienen sus propias especificidades y enfoques es muy necesario reconocer su interdependencia y complementariedad en la construcción de un orden internacional más justo, seguro y equitativo. A medida que el mundo continúa digitalizándose rápidamente, la capacidad de los Estados y los actores internacionales para navegar, adaptarse y aprovechar las oportunidades del ciberespacio será fundamental para forjar un futuro más resiliente y colaborativo en el escenario mundial.

En conclusión, aunque los términos ciberdiplomacia, diplomacia digital y e-diplomacia suelen utilizarse de manera intercambiable, es importante distinguir sus diferencias conceptuales y prácticas para comprender plenamente su impacto y relevancia en el panorama contemporáneo de las relaciones internacionales. Al hacerlo, los Estados y los actores internacionales pueden desarrollar estrategias más efectivas para explotar las oportunidades y los desafíos del ciberespacio en el ámbito diplomático. En palabras de Rodríguez Gómez (2015), "la diplomacia digital supone un nuevo modelo de diplomacia que exige una reestructuración de formas, sistemas y medios, además de una reconversión del personal que ejerza estas funciones para adaptarse al nuevo medio" (p. 935).

Tabla 1

Tabla comparativa entre ciberdiplomacia, diplomacia digital y la e-diplomacia

Aspecto/término	Ciberdiplomacia	E-diplomacia	Diplomacia digital
Características distintivas	Se enfoca en la regulación del ciberespacio, la ciberseguridad y la gobernanza digital.	Engloba el intercambio de información, la gestión de datos y la colaboración online.	Se refiere al uso de plataformas digitales para promover la comunicación y la cooperación entre actores internacionales.
Objetivos	Proteger intereses nacionales en el ciberespacio, abordar la ciberseguridad y la gobernanza.	Adaptarse a las transformaciones tecnológicas, facilitar la colaboración transnacional.	Modernizar prácticas diplomáticas tradicionales, mejorar la eficiencia y la transparencia.
Aplicaciones	Regulación del ciberespacio, lucha contra delitos cibernéticos, cooperación internacional en ciberseguridad.	Intercambio de información entre Estados, gestión de datos, colaboración online.	Uso de redes sociales, plataformas en línea para promover el diálogo diplomático y la participación ciudadana.

Nota. Elaboración propia sobre la base de *Cyber-diplomacy: the making of an international society in the digital age.* En: Global Affairs, pp. 353-364, por Barrinha y Renard, 2017. Disponible en: https://www.tandfonline.com/doi/full/10.1080/23340460.2017.1414924

Importancia y potencialidad de la ciberdiplomacia en el contexto regional

En el contexto dinámico actual, la ciberdiplomacia surge como una herramienta muy relevante para fortalecer la cooperación y la integración regionales. Esta disciplina proporciona un marco estratégico que facilita el intercambio de información, mejores prácticas y capacidades técnicas entre los países, lo que les permite abordar desafíos comunes como la ciberseguridad, la gobernanza digital y la protección de infraestructuras críticas.

Además de impulsar la cooperación, la ciberdiplomacia tiene el potencial de catalizar el desarrollo económico y la innovación en la región. La economía digital abre nuevas oportunidades para fomentar el crecimiento, la competitividad y la inversión en tecnologías emergentes como la inteligencia artificial, las criptomonedas y la economía de plataformas. En este sentido, permite a los países de ALC posicionarse estratégicamente en la

escena internacional, promoviendo políticas y regulaciones que estimulen la innovación y la colaboración en el ámbito tecnológico.

Sin embargo, la ciberdiplomacia va más allá de la economía y la tecnología: también es fundamental para proteger los derechos humanos y fortalecer la gobernanza democrática en línea. En un entorno digital en constante evolución, la cooperación regional en ciberdiplomacia permite desarrollar políticas y mecanismos que equilibren la seguridad cibernética con la protección de la privacidad, la libertad de expresión y otros derechos elementales en el ciberespacio.

La ciberdiplomacia desempeña un papel determinante en el fortalecimiento de la seguridad regional y en la defensa cibernética contra amenazas transnacionales. A través de la colaboración, los países de la región pueden desarrollar una capacidad de respuesta conjunta, compartir inteligencia y establecer normas comunes en materia de ciberseguridad y defensa, asegurando así un entorno digital más seguro, resiliente y confiable para todos los ciudadanos de ALC.

Se ha mostrado un creciente interés en abordar temas relacionados con la ciberdiplomacia y la ciberseguridad. Aunque la región aún se encuentra en una etapa de desarrollo en términos de regulaciones y programas específicos de ciberdiplomacia, se han observado avances significativos tanto a nivel regional como nacional. En el ámbito regional, la Organización de los Estados Americanos (OEA) ha desempeñado un decisivo al tratar cuestiones de ciberseguridad y gobernanza del ciberespacio (Vega, 2023). A través de diversas iniciativas, conferencias y programas de capacitación, la OEA ha buscado fortalecer la cooperación entre los Estados miembros en áreas como la protección de infraestructuras críticas, la educación en ciberseguridad y la respuesta coordinada a amenazas cibernéticas transnacionales. El SELA también ha desarrollado cursos y actividades sobre la temática en alianza con el Instituto Europeo de Estudios Internacionales (IEEI), con la colaboración de la Universidad Pontificia de Salamanca (España), que lo han posicionado como uno de los organismos de la región involucrados en el desarrollo de la ciberdiplomacia.

Por otro lado, a nivel nacional, varios países de la región han implementado estrategias de ciberseguridad y han establecido entidades especializadas en la materia. Estas iniciativas buscan fortalecer la protección de infraestructuras críticas, promover la concienciación en ciberseguridad y fomentar la cooperación internacional en temas cibernéticos. Además, se han firmado acuerdos para facilitar la colaboración en la lucha contra el ciberdelito, compartir información y desarrollar capacidades conjuntas en ciberseguridad. Organismos como la OEA o el Banco Interamericano de Desarrollo (BID) se han orientado más a la ciberseguridad mediante de un observatorio específico sobre el tema. Otras instituciones regionales, como el Mercosur, la Alianza del Pacífico, en Suramérica, o el Sistema de Integración Centroamericano (SICA), se han enfocado en aspectos económicos y comerciales y han incluido la ciberdiplomacia en sus agendas (Vega, 2023).

Sin embargo, a pesar de estos avances, la región enfrenta desafíos significativos en materia de ciberdiplomacia y ciberseguridad. Entre los más relevantes, se encuentran la falta de capacidades especializadas —técnicas y humanas—, la necesidad de fortalecer la cooperación regional y la adaptación rápida a las nuevas amenazas y desafíos del ciberespacio. Además, la armonización de marcos normativos y la protección de derechos fundamentales en el ámbito digital continúan siendo áreas de atención y debate.

Por todo lo mencionado, la ciberdiplomacia representa un pilar esencial para avanzar hacia una integración más profunda y sostenible en ALC. Al aprovechar su potencialidad, los países pueden trabajar juntos para construir un futuro digital inclusivo y seguro que refleje, como ya fue dicho, los valores, los intereses y las aspiraciones compartidas por sus ciudadanos.

Figura 1

Aspectos y actores relacionados con la ciberdiplomacia

Presentación de los contenidos

En un mundo cada vez más interconectado, la ciberdiplomacia emerge como una herramienta clave para la convergencia regional y la integración en ALC. El objetivo de este manual es ofrecer una visión y una práctica sobre cómo los países latinoamericanos y caribeños pueden utilizar estratégicamente las tecnologías digitales para fortalecer sus relaciones diplomáticas, promover el desarrollo económico, garantizar la seguridad cibernética y proteger los derechos humanos en el ciberespacio.

Desde la cooperación en materia de ciberseguridad hasta la promoción de normas y estándares regionales, pasando por la diplomacia digital en tiempos de crisis, se busca proporcionar una guía para los actores primarios en la región, con el objeto de abordar estos desafíos de manera integral y ofrecer recomendaciones y estrategias adaptadas a las realidades y necesidades específicas de estas latitudes.

Se comienza aquí explorando las definiciones de ciberdiplomacia y diplomacia digital y las diferencias entre ellas, estableciendo un marco conceptual que permite comprender las diversas dimensiones y aplicaciones de estos términos en el contexto regional. Seguidamente, el manual se adentra en el mundo de los nuevos medios y plataformas digitales y examina cómo la sociedad red o reticular y la economía de plataformas están transformando la comunicación y la interacción no solo entre las personas, sino también entre los Estados.

A continuación, se tratan temas cruciales, como la diplomacia en el siglo XXI, el uso estratégico de las redes sociales en las relaciones internacionales y la emergente diplomacia del metaverso. También se exponen aspectos fundamentales de la ciberseguridad y se analiza cómo los países pueden cooperar para establecer normas comunes, fortalecer sus capacidades de defensa y enfrentar las amenazas cibernéticas transnacionales.

La intersección entre ciberdiplomacia, derechos humanos y economía digital ocupa un lugar central en este manual. Se explora cómo la tecnología, incluidas la inteligencia artificial (IA) y las monedas digitales, está redefiniendo el panorama diplomático y el económico en este continente, al tiempo que es posible plantear desafíos y debates éticos relacionados con su uso y su regulación.

Finalmente, se concluye con una serie de recomendaciones para construir una ciberdiplomacia efectiva en la región. Al hacerlo, se aspira a proporcionar una guía para que diplomáticos, funcionarios públicos, académicos y otros actores interesados puedan navegar por sus complejidades, sortear los desafíos que presenta y aprovechar las oportunidades que ofrece.

Se invita al lector a embarcarse en este viaje con la esperanza de que el manual sirva como un recurso para fortalecer la convergencia regional y promover un desarrollo sostenible y equitativo en ALC.

NUEVOS MEDIOS Y PLATAFORMAS: SUS USOS Y SUS REGLAS

En el panorama geopolítico contemporáneo, la ciberdiplomacia emerge como un catalizador transformador que desdibuja las fronteras En el panorama geopolítico contemporáneo, la ciberdiplomacia emerge como un catalizador transformador que desdibuja las fronteras tradicionales y crea un entorno dinámico en el que las naciones convergen digitalmente. En este contexto, el presente capítulo se adentra de forma breve en el tejido conceptual que sustenta no solo la ciberdiplomacia, sino también los cambios ocurridos tanto en lo social como en lo económico y lo político durante las últimas décadas. De esta manera, se delinean y precisan los conceptos que sirven de brújula para comprender la intersección de la diplomacia y la era digital en pos de la convergencia regional.

La ciberdiplomacia, en su definición más básica, trasciende las prácticas diplomáticas convencionales, ya que amalgama las herramientas digitales con los principios fundamentales de la disciplina. Es por ello por lo que este capítulo aborda las complejidades inherentes a los nuevos medios de comunicación, las plataformas y las redes sociales. A partir de estas reflexiones, es posible examinar cómo las tecnologías emergentes (por ejemplo, la IA, las amenazas cibernéticas y las redes sociales) están dando forma a las estrategias diplomáticas y generando nuevas oportunidades para la colaboración y la convergencia en la esfera internacional.

Con este propósito, es necesario retomar la definición de ciberdiplomacia anteriormente planteada. **La ciberdiplomacia puede describirse como la práctica diplomática en y sobre el mundo digital.** En otras palabras, implica la utilización de recursos y funciones diplomáticas para proteger los intereses nacionales relacionados con el ciberespacio. Estos intereses suelen estar definidos en estrategias nacionales de ciberseguridad que, a su vez, hacen referencia a la agenda diplomática. Los temas clave en la agenda de la ciberdiplomacia abarcan la seguridad cibernética, la lucha contra la ciberdelincuencia, la promoción de la confianza, la libertad en internet y la gobernanza de la red (Barrinha y Renard, 2017). Por ello, no debemos confundirla con la e-diplomacia ni con la diplomacia digital: estos conceptos aluden al mero uso de herramientas digitales para perseguir fines

diplomáticos, no a la aplicación de la diplomacia al ciberespacio, que es lo que caracteriza a la ciberdiplomacia (Riordan, 2019).

En el ciberespacio, la ausencia de fronteras, normativas y gobernanza destaca la necesidad de establecer reglas que deben ser acordadas y coordinadas a nivel internacional. Este entorno requiere la intervención diplomática gubernamental en áreas como seguridad, gobernanza de la red, regulación de datos y protección a los usuarios o consumidores. Al no seguir la lógica de la soberanía territorial, el ciberespacio plantea desafíos significativos para la estabilidad, la seguridad y el desarrollo de los Estados. La ciberdiplomacia, más que la expansión digital de las redes diplomáticas, se presenta como una política de Estado con metas claras en diversos temas, especialmente, en ciberseguridad. La falta de comprensión del ciberespacio, la carencia de regulaciones internacionales y los riesgos asociados, como la ciberinseguridad, son preocupaciones urgentes.

La ciberdiplomacia se vuelve esencial para abordar problemas políticos y geopolíticos en este nuevo dominio en el que la gobernanza del ciberespacio y la regulación de la economía digital carecen de normas internacionales y la situación de inseguridad en el mundo digital puede afectar la paz internacional, el desarrollo sostenible y los derechos humanos. La capacidad tecnológica y el desarrollo digital muestran las diferencias entre Estados, mientras que las big tech companies ejercen un poder geopolítico guiando la formación de normas (SELA, 2023c). Aunque estas grandes empresas no buscan ni pueden ser supraestatales, poseen un inmenso poder económico y actúan de manera transfronteriza, por lo que la negociación de los Estados con ellas se apoya en la regulación del hardware ubicado en territorios soberanos. Por ello, dado que el derecho internacional brinda un marco que establece limitaciones en delitos cibernéticos y que la ciberdiplomacia puede impulsar normativas internacionales y relaciones formales con las empresas, el dilema de la ciberseguridad y de la atribución de responsabilidad en operaciones cibernéticas enfatiza la importancia del contacto cara a cara en la diplomacia.

Pensar en un enfoque estratégico de ciberseguridad pone de relieve la naturaleza social y técnica de los desafíos, la cooperación internacional y

la construcción de normas de conducta, por lo que la diplomacia digital no debe limitarse a representantes empresariales, ya que se requiere la participación gubernamental para abordar y guiar los aspectos políticos y geopolíticos.

El presente capítulo busca proporcionar una batería de conceptos que permita a los actores regionales comprender los desafíos y las oportunidades que plantea la ciberdiplomacia y ocuparse de ellos. De esta manera, la tarea por delante es allanar el camino hacia la convergencia regional, donde la colaboración funciones como un puente que une a las naciones en la era de la información.

Sociedad red y economía de plataformas

A partir de las transformaciones económicas y tecnológicas ocurridas a finales de la década de los sesenta y principios de la de los setenta, surgió un patrón de crecimiento informacional ligado al creciente protagonismo del sector financiero en la economía. Esta "revolución informacional" reemplazó el antiguo modelo de desarrollo industrial, reestructuró el capitalismo y colocó la información y los datos en el epicentro de estos cambios, lo que revolucionó los procesos productivos (Castells, 1995). En términos simples, se desencadenó una revolución tecnológica que posibilitó una revolución digital (Castells, 2009), contexto en el que la información dejó de ser simplemente un producto para convertirse también en una materia prima que alimenta la producción de bienes y de servicios (Castells, 1995). Este aumento en la productividad no solo transformó las relaciones entre el capital y el trabajo —con el capital apropiándose de una parte cada vez mayor del excedente—, sino que también alteró el modelo de intervención estatal, erosionando las bases de los Estados benefactores que habían primado durante las décadas anteriores y globalizando los procesos económicos (Castells, 1995).

En este contexto de cambios, es pertinente abordar el concepto de "capitalismo de plataformas" para referirse a las transformaciones más recientes en la economía y la sociedad (Srnicek, 2018). Entre ellas, la sociedad informacional se superpone —sin reemplazarla— a la sociedad industrial, lo que, a la larga, lleva a que la economía actual pueda caracterizarse como digital, ya que

la tecnología de la información afecta todos los procesos productivos, como se aprecia en los diversos eventos que incidieron en el modelo económico en los últimos años: desde los cambios ocurridos durante la década de los setenta, con la crisis del petróleo, pasando por las crisis de las empresas puntocom en los primeros años del siglo XXI, hasta la crisis económica de 2008.

El capitalismo de plataformas se ha impuesto como un modelo de extracción de datos para la creación de perfiles de consumo (Srnicek, 2018) o, en otras palabras, los datos personales se han convertido en mercancía y el modelo de negocio predominante se sostiene gracias a las ganancias obtenidas a partir de la información recopilada por las plataformas sobre sus usuarios. A partir de ello, una nueva clase domina la economía: ya no son los propietarios de los medios de producción, sino los propietarios de la información (Srnicek, 2018). Según este autor, las plataformas representan un nuevo tipo de empresa caracterizada por infraestructuras digitales que permiten la interacción de dos o más personas o grupos, y son más valiosas cuanto más numerosos sean los usuarios, ya que dependen de los "efectos de red".

Retomando lo mencionado, al explorar las prácticas y los usos de las plataformas y redes digitales, es crucial considerar que la actividad en ellas está restringida o condicionada, entre otras razones, por la "arquitectura" o el "código" (haciendo referencia al software o hardware), como señaló Lessig (1999); no obstante, hoy en día es más relevante enfocarse en los algoritmos en términos de su capacidad de regulación. En este sentido, los usuarios no navegan libremente en las redes o en las plataformas, sino que estos son espacios altamente regulados y restringidos, entre otras cosas, por contraseñas, con lo cual podría decirse que no están abiertos para todos. Sin embargo, este control no es ejercido directamente por los Gobiernos, sino que estos deben adaptarse muchas veces a las reglas de juego ya establecidas lo que muestra la importancia de observar cómo diferentes países han intentado regular estas cuestiones y el rol que la ciberdiplomacia puede tener en esta tarea.

Aquí se plantea una cuestión que debe ser atendida y que guarda profunda relación con la ciberdiplomacia —como se verá más adelante—: el rol de los Estados nacionales en la regulación, la importancia de las políticas

públicas sobre la comunicación en este siglo XXI y cómo la diplomacia no solo se ve afectada por estos cambios, sino que también puede contribuir a esta tarea. No son los mismos desafíos que existían a comienzos y mediados del siglo pasado, cuando emergieron medios como la radio y la TV, y las regulaciones se centraban en los contenidos y dejaban hacer a los privados. Tampoco son los mismos de la segunda mitad del siglo, cuando empezó a discutirse el lugar de los medios públicos y de los servicios que brindaban los Estados (Van Cuilenburg y McQuail, 2003). Las discusiones que dan distintos actores hoy en día pasan por la gobernanza de internet y la soberanía estatal en el control de la infraestructura y en el desarrollo tecnológico, además de la rendición de cuentas de las plataformas sobre el uso de los datos de los usuarios (Pohle y Thorsten, 2020).

Tabla 2

Evolución de la sociedad de la información y de la economía de plataformas

Década/período	Desarrollos clave	Impacto en la sociedad y la economía	Regulaciones y legislaciones importantes
1960	Primeras computadoras	Inicio de la era digital	Regulaciones sobre los contenidos
1970	Creación de ARPANET (precursora de internet)	Conexión global limitada	Obligación de pasar contenidos de interés público
1980	Popularización de las PC	Aumento del acceso a la tecnología.	Surgimiento de políticas públicas a nivel local o de cada país
1990	Auge de internet y de la www	Revolución en las comunicaciones y el comercio	
2000	Aparición de redes sociales	Conexión global y cambio en la interacción social	
2010	Emergencia de la economía de plataformas	Dominio de grandes empresas tecnológicas	Implementación del Reglamento General de Protección de Datos (RGPD)
2020	Integración de la IA y las tecnologías emergentes	Transformación digital y automatización	Regulaciones en torno a la IA

Fuente: elaboración propia.

En este punto, enmarcada en una concepción del Estado como emprendedor, en tanto que es capaz de financiar o cofinanciar el desarrollo digital (Mazzucato, 2022), la ciberdiplomacia tiene un rol fundamental al darles un encuadre internacional a estas discusiones. La transformación digital ha presentado nuevas posibilidades para que los Estados y los organismos internacionales fomenten la eficiencia, la transparencia y la participación de la ciudadanía, buscando un crecimiento más equitativo y duradero, de manera de aprovechar estas herramientas para tomar decisiones más precisas, ofrecer mejores servicios y estimular un ambiente empresarial favorable a la innovación (Campos Ríos, 2023).

Lo expuesto hasta aquí muestra que la sociedad de la información y la economía de plataformas impactan significativamente en el ámbito de la diplomacia e influyen en diversos aspectos de las relaciones internacionales y la práctica diplomática. Ello es posible porque la rapidez con que la información circula en la sociedad de la información tiene un efecto directo en la diplomacia, lleva a que la transparencia se convierta en un elemento clave y exige respuestas más inmediatas por parte de los actores diplomáticos frente a eventos internacionales. Si bien la participación ciudadana en asuntos internacionales se ve intensificada en este contexto, la sociedad de la información también presenta desafíos en forma de propaganda, desinformación, fake news y trolls. Los actores estatales y los no estatales pueden utilizar plataformas digitales para difundir información falsa lo que afecta las percepciones y las relaciones diplomáticas.

En el ámbito de la ciberseguridad, la sociedad de la información trae consigo la necesidad de los Estados de protegerse contra ciberataques, por lo que algunos emplean estrategias de "guerra cibernética" como una extensión de sus actividades diplomáticas para salvaguardar sus intereses en línea. Por otro lado, la economía de plataformas influye en las relaciones comerciales internacionales y, si bien facilita el comercio global, también plantea desafíos regulatorios y de competencia que requieren ajustes en acuerdos comerciales y políticas económicas.

La diplomacia digital se vuelve imprescindible en este panorama cambiante. Las negociaciones y los acuerdos internacionales se realizan en línea, aprovechando las plataformas digitales para facilitar la interacción entre

representantes de diferentes países y mejorar la eficiencia de las conversaciones diplomáticas. Pero no debe dejarse de lado que la sociedad de la información y la economía de plataformas cuestionan la soberanía nacional, ya que la circulación fácil de datos a través de fronteras plantea debates sobre la propiedad y la protección de la información sensible, y afecta la autonomía de los Estados.

Tabla 3

Comparación entre Estados nacionales vs. grandes empresas tecnológicas en ciberseguridad y regulación de datos.

Aspecto	Estados nacionales	Grandes empresas tecnológicas
Capacidades	Establecimiento de leyes y regulaciones nacionales y promoción de normativa internacional	Desarrollo de tecnologías de ciberseguridad
	Infraestructura para la ciberdefensa y agencias de cibervigilancia y manejo de redes	Inversiones en investigación y desarrollo
	Dirección de fuerzas de seguridad y agencias de inteligencia	Equipos especializados en seguridad informática
Responsabilidades	Proteger infraestructuras críticas	Garantizar la seguridad de los datos de los usuarios
	Vigilar y regular el uso de datos personales	Cumplir con regulaciones de privacidad (p. ej. RGPD).
	Investigar y combatir ciberdelitos	Responsabilidad frente a accionistas y usuarios
Poder y autoridad	Establecimiento de normas y sanciones	Influencia en estándares de la industria
	Negociaciones internacionales en el ciberespacio	Control sobre plataformas digitales dominantes
	Coordinación con organismos internacionales	Capacidad de lobby e influencia política
Desafíos y limitaciones	Dificultad en la regulación global	Equilibrio entre innovación y regulación
	Dependencia de tecnologías externas	Protección de datos en múltiples jurisdicciones
	Limitaciones en la respuesta a amenazas emergentes	Desafíos en la gestión de datos masivos

Fuente: elaboración propia.

Convergencia de medios

A raíz de estos cambios tecnológicos que dieron lugar a las denominadas "sociedad de la información" y "economía de la información", coexisten diversas formas de comunicar, algunas en la red y otras consideradas más tradicionales, como la televisión o la radio. En esta convivencia, todos pueden desempeñar roles como emisores y receptores de información, aunque persisten jerarquías evidentes entre distintos emisores, ya que no están en un mismo nivel un medio de comunicación y una persona particular. Es apropiado, así, hablar de la convergencia de las telecomunicaciones, internet y los medios audiovisuales.

De acuerdo con Castells (2009), en este contexto de convergencia, las identidades locales entran en conflicto con una cultura global generada por las comunicaciones, que dependen de negocios cada vez más concentrados. Diversas empresas que constituyen el núcleo de las redes globales de comunicación implementan estrategias para concentrar propiedades, establecen alianzas empresariales, diversifican sus plataformas, se adaptan a la audiencia y gestionan economías de sinergia, cada una con diferentes niveles de éxito (Castells, 2009).

La convergencia, entonces, implica un flujo de contenidos desde diversas plataformas mediáticas dirigido a diversas audiencias, o en palabras de uno de los autores más destacados sobre la temática, se refiere:

> … al flujo de contenido a través de múltiples plataformas mediáticas, la cooperación entre múltiples industrias mediáticas y el comportamiento migratorio de las audiencias mediáticas, dispuestas a ir casi a cualquier parte en busca del tipo deseado de experiencias de entretenimiento. (Jenkins, 2006, p. 14)

Este flujo que se menciona puede adaptarse según diversos criterios y lógicas, especialmente la del entretenimiento, ya que, entre otras cosas, la convergencia implica que los "nuevos medios" (digitales) no reemplazan a los "viejos", sino que estos últimos cambian su posición y su relevancia.

La convergencia no solo se da a partir de los aparatos mediáticos o de la concentración de la propiedad de los medios, sino que también ocurre en el cerebro de los consumidores y constituye un cambio cultural el cual ser un factor importante para explicar la consolidación de monopolios (Jenkins, 2006), ya que los procesos de convergencia potenciados por la digitalización y la globalización han contribuido a la mercantilización de la cultura y a la concentración en la propiedad de los medios (Becerra y Mastrini, 2017). Según estos autores, esta concentración tiende, a su vez, a la unificación de la línea editorial y la concentración geográfica, dos aspectos que, relacionados con la dinámica de las redes y la forma en que los usuarios producen y reciben información, pueden ser aún más interesantes.

Es relevante considerar que la velocidad de los cambios tecnológicos puede superar el tiempo que les lleva a diferentes sectores de la sociedad aprender sobre ellos, por lo que algunos otros autores hablan de una "desconvergencia" en paralelo, haciendo referencia a la proliferación de dispositivos, usos y prácticas, además de una separación de las empresas de comunicaciones y medios (Peil y Spaviero, 2017). En este sentido, no todos los contenidos de los medios convergen hacia una sola caja negra, como muchos podrían pensar que ocurre con los smartphones o dispositivos generales, sino que existen aparatos especializados y aparatos más genéricos (Jenkins, 2006)

Este fenómeno de convergencia de las TIC tiene un impacto significativo en el ámbito de la diplomacia. En primer lugar, facilita una comunicación instantánea entre diplomáticos y funcionarios de diferentes países gracias a la confluencia de plataformas como correos electrónicos, redes sociales y servicios de mensajería instantánea. Tal rapidez para comunicarse puede acelerar los procesos de toma de decisiones y la resolución de problemas. Asimismo, se agiliza el acceso a la información sobre políticas, eventos y desarrollos internacionales, lo que hace que los diplomáticos estén actualizados. Al mismo tiempo, la diplomacia digital se ha vuelto una práctica común que involucra negociaciones en línea, participación en conferencias virtuales y gestión de la reputación en el ámbito digital.

Sin embargo, la convergencia también conlleva desafíos. Uno de ellos es que, al propagarse rápidamente, la información puede afectar la opinión

pública, lo que exige una gestión cuidadosa de la comunicación. Otra dificultad que presenta es en cuanto a la seguridad: la dependencia de plataformas digitales puede hacer que los sistemas sean vulnerables a ciberataques. Proteger la información sensible y prevenir las amenazas son aspectos esenciales de la diplomacia moderna. Todo ello implica que la adaptación a estos cambios es esencial para los actores diplomáticos en un mundo cada vez más interconectado.

Por último, vale la pena destacar lo siguiente en relación con la convergencia:

> La ciberdiplomacia, o "diplomacia en 140 caracteres", no sustituirá en ningún modo a la acción tradicional, como la televisión, la radio o la propia web 1.0 —la de la burbuja de las puntocom de finales del siglo XX— no fueron sustitutos de nada, sino más bien complementos.
>
> (Rodríguez Gómez, 2015, p. 924)

La comunicación en el siglo XXI y las redes sociales

En el contexto de las sociedades de la información y de la convergencia de los medios, las redes sociales han transformado la manera en En el contexto de las sociedades de la información y de la convergencia de los medios, las redes sociales han transformado la manera en que las personas se comunican y también han dejado una huella significativa en el ámbito de la diplomacia.

Al poner el foco en las redes digitales y las plataformas resulta necesario considerar el impacto de los encuadres en la selección y el resaltado de información en estas redes. Simultáneamente, surgen las "cámaras de eco" o "burbujas informativas" (Calvo, 2015; Calvo y Aruguete, 2020), las cuales devuelven a los usuarios publicaciones similares a las que han compartido, dificultando la percepción de estas redes como entornos sólidos y neutrales en los que los usuarios intercambian opiniones de manera racional.

Las plataformas poseen un carácter performativo, ya que el código —o su arquitectura, en términos de Lessig (2002)— condiciona un ecosistema que exhibe características jerárquicas, corporativas, centralizadas, opacas y con

valores ideológicos, que generan un impacto a escala global. Actúan como intermediarios, pues eluden responsabilidades que recaen en los usuarios, y facilitan la conexión entre diversos actores políticos, sociales y económicos, dirigiendo la forma en que estos interactúan entre sí (Van Dijk et al., 2018). La vida moderna transcurre en una sociedad de plataformas que configuran un espacio público óptimo para la deliberación necesaria en pos del desarrollo político, según la visión de autores como Jürgen Habermas o John Rawls (Maldonado, 1998; Van Dijk et al., 2018).

La "plataformización" difumina la diferencia entre lo público y lo privado, ya que, en estas redes, puede extraerse una gran cantidad de datos de la vida de los usuarios (Van Dijk et al., 2018), lo que las convierte en centros de poder sin un punto central fijo (Maldonado, 1998). De acuerdo con Maldonado (1998), las "comunidades virtuales" en estos espacios son democráticamente débiles, ya que tienden a excluir lo diferente —fenómeno de las cámaras de eco— e internamente son homogéneas, autorreferenciales, nómadas, comunitaristas y antiestatistas. Sostiene, además, que, a pesar de la posibilidad de adoptar múltiples roles en estas redes, los usuarios suelen ser pasivos frente a los dispositivos y quedan "atrapados" en la "telaraña" de la web.

Aunque en un principio se pensaba que internet sería capaz de democratizar la sociedad, en estas redes digitales o plataformas, los algoritmos y los códigos son la norma, lo que define el funcionamiento de los filtros (Lessig, 2002; Pariser, 2017). Estos filtros están diseñados según los gustos e intereses de los usuarios, con un nivel extremo de personalización que configura una "burbuja de filtros" y no solo afecta las publicidades que los usuarios visualizan en las redes, sino también la información que consumen basada en un perfil construido sobre ellos (Pariser, 2017), además de propiciar la formación de comunidades impermeables a la diversidad. En este contexto, en relación con el "capitalismo de plataformas", estas plataformas transforman la "huella digital" y la información recopilada en un negocio mediante la creación de perfiles y el procesamiento de datos. Tras la minería de datos y el análisis del *big data*, se establecen correlaciones y se abandonan las motivaciones y las explicaciones para centrarse exclusivamente en la ocurrencia de fenómenos.

Por su parte, las redes sociales y las plataformas digitales han transformado radicalmente el panorama de la diplomacia en la era contemporánea. Estas plataformas han proporcionado a los líderes y diplomáticos una vía directa para comunicarse con audiencias globales de manera instantánea y sin intermediarios, además de que las redes sociales han democratizado —con sus límites— la participación en los asuntos diplomáticos al permitir que los ciudadanos comunes expresen sus opiniones y críticas sobre eventos internacionales. Este fenómeno ha llevado a un aumento en la transparencia y la rendición de cuentas, ya que aquellos pueden seguir de cerca las actividades diplomáticas de sus Gobiernos y representantes.

Sin embargo, esta apertura también presenta desafíos pues las redes sociales pueden ser utilizadas para difundir desinformación, *fake news* y propaganda. Los incidentes de desinformación son capaces de afectar negativamente las relaciones diplomáticas al sembrar discordia y distorsionar la verdad lo que subraya la necesidad de estrategias efectivas para contrarrestar la propagación de información falsa. Ello, sumado al hecho de que las cámaras de eco y las burbujas informacionales dificultan que el proceso por el cual se informan los usuarios sea plural y contemple diversos enfoques y posturas.

La ciberdiplomacia y la diplomacia digital, facilitadas por estas plataformas, se han convertido en herramientas cruciales para la construcción y la gestión de relaciones internacionales. Las negociaciones y discusiones entre Estados ahora ocurren en línea, y las plataformas digitales sirven como espacios para el diálogo entre líderes y representantes gubernamentales.

DIPLOMACIA DIGITAL Y USO DE LAS REDES SOCIALES

En la era digital contemporánea, el paisaje de las relaciones internacionales ha experimentado una transformación profunda, impulsada, en gran medida, por la presencia de nuevas TIC, especialmente, a partir del uso de las redes sociales. Este nuevo paradigma, que se ha definido como "diplomacia digital" y se distingue de la ciberdiplomacia redefine la forma en que los Estados interactúan entre sí, así como la manera en que se comunican y se relacionan con sus ciudadanos y el mundo en general. Las plataformas y redes sociales, desde X (antes denominada Twitter) y Facebook hasta Instagram, LinkedIn o TikTok, se han convertido en espacios donde se moldean percepciones, se construyen alianzas y se gestionan cuestiones a nivel global.

Como se mencionó en el capítulo precedente, la ciberdiplomacia se posiciona como un agente transformador que borra las fronteras convencionales y promueve la convergencia digital entre naciones. Puede conectarse con los cambios socioeconómicos y políticos recientes y va más allá de las prácticas diplomáticas tradicionales, ya que integra herramientas digitales con principios fundamentales. Se diferencia de la diplomacia digital por enfocarse, específicamente, en la gestión de intereses nacionales en el ciberespacio al tratar temas como seguridad cibernética y gobernanza de la red. Dada la naturaleza sin fronteras del ciberespacio, emerge la necesidad de establecer normas internacionales para abordar los desafíos indicados. Por otro lado, las grandes empresas tecnológicas ejercen una influencia geopolítica, lo que destaca la importancia de la ciberdiplomacia para negociar y establecer relaciones formales con estas entidades.

Este capítulo se sumerge en el mundo de la diplomacia digital y explora cómo las herramientas en línea y las redes sociales han ampliado el alcance y la velocidad de la comunicación y de las actividades que implican el ejercicio diplomático. Se identifican las características de las distintas plataformas y las posibilidades que ofrecen para la comunicación diplomática; los peligros que representan las campañas de desinformación, las fake news y las propagandas que se difunden rápidamente en el mundo digital, y cómo

las redes sociales pueden ser tanto un puente para el diálogo como un campo de batalla para conflictos y tensiones internacionales.

Tener en cuenta estas situaciones permitirá a los países latinoamericanos y caribeños comenzar a pensar en las oportunidades y los desafíos que presenta la diplomacia digital en el contexto regional, considerando sus particularidades, las estrategias que adoptar por cada Estado y las implicancias para la convergencia y la integración, uno de los principales objetivos del SELA. En este escenario dinámico y en constante evolución, comprender la intersección entre diplomacia, tecnología y redes sociales es fundamental para navegar en un mundo cada vez más interconectado y digitalizado.

Algunas definiciones generales sobre la diplomacia

Desde hace siglos, la diplomacia ha fungido como el mecanismo principal para gestionar las relaciones entre Estados y ha servido como puente para promover la paz, la cooperación y el entendimiento mutuo entre naciones. En el contexto contemporáneo, en el que la interconexión global se intensifica, el alcance de la diplomacia se extiende a esferas como la económica, cultural, científica y, de manera creciente, a la ciberespacial.

La diplomacia puede conceptualizarse como el arte y la práctica dedicada a establecer y mantener relaciones armónicas, cooperativas y beneficiosas entre diversos actores, ya sean Estados nacionales, organizaciones internacionales o entidades no estatales. Su esencia radica en facilitar el diálogo constructivo con el propósito de resolver conflictos, alcanzar acuerdos y avanzar hacia objetivos comunes que beneficien a la comunidad internacional en su conjunto. En esta trama, un agente diplomático o un embajador emerge como una figura central al ser aquella persona designada para representar oficialmente a un Estado en el ámbito internacional. Este representante puede tomar diversas formas, desde embajadores hasta cónsules, todos ellos encargados de defender y promover los intereses de su país en el extranjero.

Entre los principios fundamentales que rigen la práctica diplomática, se encuentran la soberanía, que implica el respeto mutuo a la autonomía y las decisiones internas de cada Estado; la igualdad, que establece que todos los

Estados, independientemente de su magnitud o poderío, poseen derechos y obligaciones equivalentes en el ámbito internacional; la negociación, como mecanismo central para resolver diferencias y promover consensos; la no intervención, que insta a los Estados a abstenerse de inmiscuirse en asuntos internos de otras naciones; la cooperación, que promueve la solidaridad y la colaboración entre naciones para afrontar desafíos compartidos y la reciprocidad, que implica que los Estados o actores internacionales respondan a las acciones de otros de manera similar.

En todas sus dimensiones, este servicio de los Estados continúa siendo el pilar fundamental para alcanzar la paz, la estabilidad y la cooperación en un mundo cada vez más interconectado y complejo. Ante la multiplicidad de desafíos globales, la imperativa necesidad de fortalecer la diplomacia efectiva y colaborativa se manifiesta como una prioridad ineludible para la comunidad internacional.

La ciberdiplomacia y la diplomacia digital surgen como una evolución de la diplomacia tradicional mediante el aprovechamiento de las TIC. Este enfoque digital y moderno busca promover los intereses nacionales, facilitar el diálogo exterior y gestionar las relaciones en un entorno digital interconectado conocido como "ciberespacio". A su vez, el concepto de soft power o poder blando, adquiere relevancia, dado que hace referencia a cómo los Estados pueden influir en la percepción y la opinión pública a través de medios no coactivos, como intercambios culturales, medios de comunicación y campañas informativas.

Uso de plataformas digitales en la diplomacia

Como se ha mencionado, una revolución digital e informacional ha transformado el paisaje de las relaciones internacionales, dando lugar a una nueva era en la práctica diplomática. En este contexto, el uso estratégico de plataformas digitales ha surgido como un elemento fundamental para facilitar la comunicación, la negociación y la colaboración entre Estados. En este apartado, nos enfocaremos en explorar cómo las herramientas digitales han remodelado la diplomacia contemporánea y examinaremos tanto sus beneficios como sus desafíos inherentes.

Las plataformas de videoconferencia como Zoom, Google Meet y Microsoft Teams han revolucionado la forma en que los representantes diplomáticos interactúan a nivel global. Estas herramientas ofrecen flexibilidad y eficiencia, ya que permiten superar barreras geográficas y optimizar la comunicación entre actores internacionales. Sin embargo, también plantean desafíos en términos de seguridad, accesibilidad y adaptación cultural, por lo que se requieren protocolos y medidas adecuadas para garantizar su efectividad y su confiabilidad.

Las redes sociales han ampliado el alcance y la influencia de la diplomacia pública proporcionando plataformas para proyectar imágenes o diapositivas, comunicar políticas e interactuar directamente con ciudadanos y actores internacionales. Las plataformas y las redes sociales se han convertido en herramientas clave para líderes y representantes diplomáticos a través de estrategias como el uso de hashtags, campañas temáticas y gestión de crisis. No obstante, este nuevo panorama digital también presenta riesgos, incluidos la desinformación, la exposición de información sensible y los agravios e insultos que, en ocasiones, abundan en algunas redes sociales, las cuales requieren una gestión cuidadosa y estratégica.

Además de las herramientas ampliamente utilizadas, existen plataformas especializadas para facilitar la cooperación y la coordinación diplomáticas. Estos sistemas abarcan desde herramientas de gestión de conferencias hasta bases de datos diplomáticas y protocolos de comunicación segura. Su adecuada implementación puede mejorar la eficiencia, la transparencia y la seguridad en las relaciones internacionales, aunque su uso requiere consideraciones específicas y adaptarse a las necesidades y los contextos de cada Estado o entidad diplomática.

En ALC, el uso de plataformas digitales en la diplomacia presenta particularidades y desafíos específicos. A continuación, se analizan oportunidades y obstáculos considerando aspectos políticos, económicos y culturales que proporcionan insights valiosos sobre cómo adaptar y aprovechar las herramientas digitales para fortalecer la cooperación regional e internacional.

Tabla 4

Principales plataformas y herramientas digitales utilizadas en la diplomacia

Plataforma/herramienta	Descripción	Uso en diplomacia
Zoom	Plataforma de videoconferencia que permite realizar reuniones virtuales, *webinars* y colaboraciones en tiempo real.	Utilizada para reuniones diplomáticas virtuales, conferencias y diálogos entre representantes de diferentes países.
Google Meet	Herramienta de videoconferencia integrada en el ecosistema de Google que ofrece funciones de colaboración.	Empleada para encuentros diplomáticos, negociaciones bilaterales y coordinación entre delegaciones internacionales.
Microsoft Teams	Plataforma de colaboración que incluye chat, videoconferencias, almacenamiento de archivos y aplicaciones integradas.	Utilizada para la comunicación interna entre representantes diplomáticos, coordinación de proyectos y colaboración en equipo.
X (ex-Twitter)	Red social que permite compartir actualizaciones breves, noticias y contenido multimedia.	Empleada para la diplomacia pública, difundir comunicados, interactuar con ciudadanos y seguir tendencias globales.
Facebook	Red social ampliamente utilizada para conectar personas, compartir contenido y crear comunidades en línea.	Utilizada para la diplomacia pública, promover iniciativas, interactuar con públicos específicos y difundir información.
LinkedIn	Red profesional orientada a conectar profesionales, empresas y organizaciones en diferentes sectores.	Empleada para establecer contactos diplomáticos, hacer *networking* entre representantes internacionales y promover oportunidades de colaboración
Instagram	Plataforma de redes sociales centrada en compartir fotos y videos, con un enfoque en la narrativa visual.	Utilizada para la diplomacia pública, *storytelling*, promoción cultural y alcance a audiencias más jóvenes.
TikTok	Aplicación de redes sociales que permite crear y compartir videos cortos con música, efectos y filtros.	Empleada para campañas de sensibilización, promoción cultural y acercamiento a audiencias más jóvenes en el ámbito internacional.

Fuente: elaboración propia.

La diplomacia del metaverso

En la intersección de la tecnología y las relaciones internacionales nace el concepto de "metaverso" como un espacio digital tridimensional que redefine la interacción humana y las estructuras tradicionales de poder. Este entorno inmersivo combina elementos de realidad virtual, realidad aumentada y plataformas en línea para crear experiencias interactivas y colaborativas. En este contexto, entender la diplomacia del metaverso se convierte en una prioridad para los actores globales en la era de la convergencia regional dado lo siguiente:

> Cuanta más confianza haya en la tecnología digital, mayor será la motivación de las personas a interactuar con nuevas tecnologías e innovaciones que, a su vez, mejorarán las posibilidades económicas y sociales de un país. Necesitamos más y mejores marcos regulatorios que permitan tener control sobre los procesos de transformación digital y, a la vez, gobernar el BIG DATA y la AI.
> (Campos Ríos, 2022, p. 129)

El metaverso se define como un espacio virtual donde los usuarios interactúan a través de avatares digitales, es decir, la representación gráfica o visual de un usuario en este entorno que ofrece una inmersión total en experiencias tridimensionales. Un mundo basado en la realidad virtual, que funciona como un juego de rol en línea, pero con potencialidad de ser masivo (Campos Ríos, 2022). Sus características distintivas incluyen la posibilidad de crear economías virtuales, conectar personas de todo el mundo en tiempo real y brindar oportunidades sin precedentes para la colaboración y la creatividad.

Algunas plataformas lideran el espacio del metaverso y se utilizan para actividades diplomáticas y colaborativas a nivel global. El caso más paradigmático en la región es el de Barbados, que, a fines de 2021, firmó un acuerdo con la plataforma Decentraland. Herramientas como estas ofrecen oportunidades para la participación pública y privada en la construcción de un nuevo paradigma de relaciones internacionales en la era digital.

La llegada del metaverso ha ampliado las fronteras de la diplomacia al proporcionar un espacio para el diálogo internacional, la cooperación y la negociación. Las plataformas del metaverso permiten a los diplomáticos interactuar de manera más directa y personalizada, y superar las barreras geográficas y culturales que tradicionalmente han limitado las interacciones internacionales. Por ejemplo, las cumbres virtuales entre líderes del mundo en distintas plataformas podrían redefinir las normas de la diplomacia moderna y abrir nuevas posibilidades para la construcción de relaciones internacionales.

El metaverso presenta oportunidades significativas para la diplomacia como la creación de espacios neutrales para el diálogo, la facilitación de la cooperación regional a través de proyectos y eventos virtuales, y el impulso de economías virtuales que pueden mejorar las relaciones comerciales y diplomáticas entre naciones. Sin embargo, también plantea desafíos importantes, como la necesidad de establecer regulaciones y gobernanza, garantizar la seguridad y la privacidad de los usuarios y abordar desafíos éticos relacionados con la representación y la autenticidad en este nuevo entorno digital. He aquí uno de los grandes retos de la ciberdiplomacia en la regulación de estas cuestiones.

Para aprovechar al máximo las oportunidades del metaverso en el ámbito diplomático, es fundamental establecer protocolos claros, promover la formación y la capacitación de diplomáticos en el desarrollo e instrumentación de habilidades virtuales y tecnológicas y fomentar la colaboración entre actores públicos y privados para desarrollar soluciones innovadoras en este espacio emergente. No hay que perder de vista que, en el ciberespacio, los actores no estatales como compañías, organizaciones de la sociedad civil (OSC), influencers, etc., son muy relevantes, como también lo son en el "mundo físico", lo cual exige una "diplomacia híbrida" (Riordan, 2019).

La diplomacia del metaverso representa un nuevo paradigma en las relaciones internacionales, ya que presenta oportunidades y desafíos sin precedentes para la cooperación global, la convergencia regional y la construcción de un mundo más conectado y colaborativo. A medida que el metaverso continúa evolucionando es necesario que los actores interna-

cionales adapten sus estrategias y sus enfoques para navegar con éxito en este nuevo entorno digital. Sin embargo, no deben perderse de vista los importantes problemas técnicos todavía no resueltos del metaverso, como que el acceso estará condicionado por la potencia informática. Además, aún no es un hecho consumado como internet, por lo que los Gobiernos, las empresas y los demás actores podrían cuestionar su diseño, ámbito y naturaleza unitaria. De hecho, la ciberdiplomacia podría ayudar a la construcción del metaverso, a la competencia entre los metaversos o las plataformas usadas para su conexión y sus regulaciones, y, dentro del metaverso, a la geopolítica de los avatares.

Tabla 4

Principales plataformas y herramientas digitales utilizadas en la diplomacia

Fortalezas	Debilidades
1. Interacción global: conexión global en tiempo real.	1. Acceso limitado: desafíos técnicos y exclusión digital.
2. Colaboración eficiente: cooperación regional y global.	2. Seguridad y privacidad: preocupación por los datos y la privacidad.
3. Innovación diplomática: nuevas herramientas para la diplomacia.	3. Desigualdad digital: brecha digital y recursos limitados.
Oportunidades	**Amenazas**
1. Desarrollo económico: impulso de economías virtuales.	1. Desafíos éticos: problemas de autenticidad y desinformación.
2. Regulación y gobernanza: creación de marcos regulatorios.	2. Competencia entre metaversos: conflictos entre plataformas.
3. Formación y capacitación: habilidades virtuales y tecnológicas.	3. Riesgos geopolíticos: influencia y control de actores estatales y no estatales en el metaverso.

Fuente: elaboración propia.

Estrategias efectivas de comunicación en redes sociales

Las redes sociales han reconfigurado el panorama de la comunicación diplomática a través de plataformas dinámicas y accesibles para interactuar con audiencias globales. Estas redes constituyen entidades empresariales distintivas que se definen por su infraestructura digital la cual facilita la interacción entre individuos o grupos. Asimismo, posibilitan a los usuarios interactuar, compartir información y conectarse con otros individuos o comunidades. Se distinguen por su capacidad para favorecer una comunicación bidireccional para generar contenido a través de los propios usuarios y ofrecen una variedad de formatos multimedia. Estas plataformas se caracterizan también por emplear algoritmos que personalizan el contenido mostrado según los intereses y los comportamientos de cada usuario y por permitir conexiones tanto a nivel local como global.

A continuación, se examinan las estrategias efectivas que los actores diplomáticos pueden emplear para maximizar el impacto de su comunicación en redes sociales, fortalecer las relaciones internacionales y proyectar una imagen positiva de sus respectivos países. También es necesario tener en cuenta algunos problemas y desafíos como el hecho de que una red como X exige una fluidez y una velocidad de reacción que es necesario que muchos embajadores y diplomáticos tengan, lo cual altera los procedimientos de consultas a sus respectivos ministerios de Asuntos Exteriores (Riordan, 2019). Asimismo, la cuestión de los algoritmos, que ya se ha mencionado, y la jerarquización de la información pueden resultar un desafío para los diplomáticos aunque las redes, en contraparte, les permitan no depender tanto de los medios más "tradicionales" para difundir información y conectarse con la ciudadanía (Riordan, 2019).

A estas alturas, es indudable la influencia transformadora de las redes sociales en la diplomacia y la comunicación global en general.

Por ello, se destaca cómo las plataformas han redefinido la interacción entre actores internacionales al permitir conexiones directas entre líderes y ciudadanos. No obstante, también es pertinente señalar los desafíos

como los relacionados con la existencia de "cámaras de eco", donde los usuarios ven y comparten información similar, dificultando un intercambio de opiniones plural y racional. Las plataformas, con su diseño performativo y algorítmico, pueden generar un entorno de "burbuja" que limita la diversidad informativa, lo que convierte la información y los datos en un negocio centralizado.

A pesar de sus beneficios en cuanto a la transparencia y la participación ciudadana en asuntos diplomáticos, las redes sociales también presentan riesgos, como la difusión de *fake news*, lo que destaca la importancia de estrategias para contrarrestar tales efectos. En pocas palabras, la ciberdiplomacia ha emergido como una herramienta esencial en la gestión de las relaciones internacionales en la era digital, y las redes sociales ocupan un rol clave.

> La revolución que las redes sociales han supuesto para el mundo de las comunicaciones y, por tanto, para la diplomacia en todas sus vertientes —no olvidemos que la diplomacia se basa en el uso de la comunicación y el diálogo como instrumento para la negociación, el intercambio de ideas y la acción exterior—, la aparición y el auge de redes sociales de todo tipo supone un reto que deben afrontar los diferentes actores de la diplomacia de los Estados.
>
> (Rodríguez Gómez, 2015, p. 924)

Antes de desarrollar cualquier estrategia en redes sociales, es fundamental entender y segmentar el público objetivo. Esto implica analizar características demográficas, intereses, comportamientos y expectativas para adaptar el mensaje y la plataforma adecuados a cada audiencia específica. El conocimiento profundo del público permite crear contenido relevante, generar engagement y construir relaciones duraderas basadas en la confianza y la autenticidad.

Establecer objetivos claros y medibles es esencial para guiar las acciones en redes sociales. Ya sea aumentar la visibilidad internacional, promover políticas específicas, gestionar crisis o fortalecer alianzas, cada objetivo requiere estrategias y tácticas específicas. Al definir propósitos claros, los actores diplomáticos pueden alinear su comunicación en redes sociales con las metas y las prioridades de su política exterior, optimizando recursos y maximizando el impacto.

La creación de contenido relevante y atractivo es un pilar fundamental de la comunicación efectiva en redes sociales. Esto incluye desarrollar mensajes claros, concisos y visualmente atractivos que tengan cierto impacto en la audiencia meta. Utilizar formatos variados, como imágenes, videos, infografías y artículos permite diversificar el contenido y adaptarse a las preferencias y las características de cada plataforma y audiencia.

La comunicación en redes sociales es bidireccional, es decir, requiere una participación activa y una interacción con la audiencia. Esto implica responder comentarios, preguntas y críticas de manera oportuna y profesional, a fin de fomentar el diálogo y construir relaciones sólidas. Además, la participación en conversaciones relevantes, debates y eventos en línea permite mantenerse actualizado, influir en opiniones y posicionar temas de interés diplomático en el escenario internacional.

La evaluación regular de las estrategias de comunicación en redes sociales es determinante para medir el impacto, identificar áreas de mejora y adaptar tácticas según las necesidades cambiantes y los resultados obtenidos. Utilizar herramientas analíticas, monitorear métricas clave como alcance, *engagement* y conversión y realizar ajustes estratégicos permite optimizar la comunicación en redes sociales y garantizar su efectividad a largo plazo.

PANORAMA REGIONAL

En el siglo XXI, la conexión digital ha transformado la forma en que los países interactúan entre sí, dando origen a una nueva dimensión de las relaciones internacionales conocida como "ciberdiplomacia". Para ALC, la ciberdiplomacia representa tanto oportunidades como desafíos por considerar, y el SELA reconoce la necesidad urgente de entender y adaptarse al nuevo paradigma diplomático. Este capítulo ofrece un panorama regional en torno a la ciberdiplomacia, a partir de una mirada sobre cómo los países están aprovechando las tecnologías digitales para promover sus intereses, fortalecer la integración y la convergencia regionales y enfrentar los desafíos emergentes en el ciberespacio.

Es importante destacar que la ciberdiplomacia no es simplemente una extensión de la diplomacia tradicional al ámbito digital, sino que representa un campo multidimensional que involucra aspectos de seguridad nacional, política exterior, economía digital y derechos humanos, entre otros. Para una región con una creciente dependencia de las TIC, la capacidad de navegar eficazmente en el ciberespacio se ha convertido en un imperativo estratégico. La ciberdiplomacia ofrece herramientas para fortalecer la cooperación regional, proteger la infraestructura crítica y promover una visión inclusiva y equitativa de la gobernanza digital.

Sin embargo, el camino hacia una convergencia regional en ciberdiplomacia está plagado de desafíos. Desde la brecha digital que aún persiste en algunas áreas hasta las amenazas cibernéticas transnacionales, que requieren respuestas coordinadas, ALC enfrentan obstáculos significativos. La falta de capacidades técnicas especializadas, la divergencia en las políticas nacionales de ciberseguridad y la ausencia de marcos normativos regionales cohesivos son solo algunos de los retos que requieren atención inmediata.

Ahora bien, para poder medir la brecha digital es importante considerar diferentes cuestiones. En ese sentido, el Banco Interamericano de Desarrollo (García Zeballos et al., 2023) ha elaborado un *Índice del Desarrollo*

de Banda Ancha (IDBA) teniendo en cuenta la existencia de políticas públicas y la visión estratégica de los países en la materia; la regulación estratégica; la infraestructura digital, y el nivel de capacitaciones y de aplicación. Por su parte, la Comisión Económica para América Latina y el Caribe (CEPAL) tiene un Observatorio Regional de Banda Ancha (ORBA) que ha identificado, entre otros datos, que, en la región, menos del 40 % de la población posee conocimientos básicos de informática (CEPAL, 2021).

Por otra parte, no debe perderse de vista que la discusión sobre la gobernanza de la red está politizada (Riordan, 2019), lo cual dificulta el desarrollo de las ideas. Tampoco debe olvidarse que internet funciona como una institución internacional de balance de poder geopolítico y que refleja dicha estructura (Riordan, 2019). El objetivo es salirse de discusiones locales o partidistas para centrarse en distintas experiencias y posibilidades.

A medida que avanzamos hacia una era cada vez más digitalizada es necesario que se trabaje conjuntamente en la región para desarrollar estrategias cohesivas que reflejen los valores, intereses y aspiraciones compartidos. Este capítulo pretende ser un primer paso para dicho diálogo y brinda una perspectiva para fortalecer la convergencia regional en el innovador y complejo mundo de la ciberdiplomacia.

América Latina y el Caribe, en contexto

Desde el siglo XV, ALC se transformó en una zona de extracción de recursos, como oro, plata, café y azúcar, para exportar a Europa, configurando una economía centrada en la exportación de materias primas. En el siglo XIX, muchos de estos países se independizaron de las potencias coloniales, aunque enfrentaron desafíos como la concentración de tierras y la dependencia de las exportaciones. Durante el siglo XX, la región vivió altibajos políticos y económicos, incluidos los periodos de crecimiento industrial y crisis financieras, y a pesar de las consolidaciones democráticas de las últimas décadas, persisten los desafíos relacionados con la desigualdad, la pobreza y la gobernabilidad.

Tabla 6

Ranking de países de América Latina y el Caribe según el índice IDBA 2021-2022

Lugar	País	Puntaje
1	Chile	5,75
2	Brasil	5,35
3	Costa Rica	5,29
4	Bahamas	5,15
5	Uruguay	5,15
6	Barbados	5,09
7	Argentina	4,96
8	México	4,76
9	Panamá	4,54
10	Jamaica	4,53
11	Perú	4,51
12	**Promedio ALC**	**4,48**
13	Colombia	4,45
14	Trinidad y Tobago	4,44
15	Belice	4,31
16	República Dominicana	4,27
17	Ecuador	4,22
18	Paraguay	4,07
19	Bolivia	4,01
20	Surinam	3,96
21	Venezuela	3,95
22	El Salvador	3,47
23	Honduras	3,45
24	Guyana	3,44
25	Guatemala	3,42
26	Nicaragua	3,29
27	Haití	1,96

Nota. Adaptado del Informe anual del Índice de Desarrollo de la Banda Ancha: brecha digital en América Latina y el Caribe. IDBA 2022, p. 28, por García Zeballos et al., 2023, BID. Disponible en: https://publications.iadb.org/es/informe-anual-del-indice-de-desarrollo-de-la-banda-ancha-brecha-digital-en-america-latina-y-el-0

Con una geografía que abarca desde las altas montañas de los Andes hasta las llanuras amazónicas, pasando por los ejes volcánicos y las paradisíacas playas caribeñas, la región posee una diversidad geográfica de amplias dimensiones. Esta variedad ha influenciado los patrones de migración, el desarrollo económico y los desafíos medioambientales, como la deforestación y el cambio climático. Por otra parte, alberga una mezcla vibrante de culturas, idiomas y tradiciones y, aunque cada país tiene su identidad única, existe una rica interconexión cultural que se refleja en la música, la gastronomía y las artes. Sin embargo, la desigualdad social persistente ha generado tensiones y movimientos sociales que buscan una mayor inclusión y justicia social. Las tensiones diplomáticas, las disputas territoriales y los intereses divergentes entre países han requerido una diplomacia activa y pragmática para construir puentes y fomentar la cooperación.

La política en la región se caracteriza por una diversidad de sistemas democráticos, movimientos y tensiones, por lo que la diplomacia regional ha jugado un papel crucial en la búsqueda de consensos y soluciones a problemas comunes, como el comercio, la migración y la seguridad. La región ha evolucionado en respuesta a los cambios geopolíticos globales y los desafíos regionales, de la mano de organismos e instituciones de trabajo mancomunado, en pos de fortalecer la integración regional, promover el desarrollo sostenible y enfrentar desafíos comunes. No debe olvidarse que la integración latinoamericana y caribeña se originó en la década de los cincuenta, durante el período de posguerra. A lo largo de los años, ha persistido y resistido las presiones geopolíticas, además de haber enfrentado los desafíos planteados por la globalización y la mundialización en la actualidad (SELA, 2023a). En estos términos generales, puede entenderse, entonces, cómo la ciberdiplomacia puede ayudar a la integración.

A pesar de los avances significativos en materia de conectividad en los últimos años, la región aún enfrenta desafíos en cuanto a la infraestructura tecnológica, ya que existen brechas digitales entre áreas urbanas y rurales, así como entre países. La falta de acceso a internet de alta velocidad y la limitada inversión en tecnologías emergentes, como la IA y la internet

de las cosas (IoT, por sus siglas en inglés), representan obstáculos para el desarrollo digital integral. Si bien la digitalización está transformando las economías de ALC, impulsando sectores como el comercio electrónico, las *fintech* y los servicios digitales, la transición hacia una economía digital también plantea dificultades en términos de la regulación, la protección de los datos y la ciberseguridad.

En ALC es imprescindible contar con políticas públicas adecuadas y de marcos normativos claros que permitan aprovechar las oportunidades y mitigar los riesgos asociados, máxime cuando la creciente interconexión digital ha aumentado la vulnerabilidad de la región a amenazas cibernéticas, como ciberataques, ciberespionaje y desinformación. La falta de capacidades especializadas en ciberseguridad, la ausencia de marcos normativos cohesivos y la dependencia de infraestructuras críticas vulnerables son preocupaciones urgentes que requieren atención. La cooperación regional en materia de ciberseguridad se presenta como un elemento clave para fortalecer la resiliencia y proteger los intereses nacionales y regionales. Aquí es donde la ciberdiplomacia adquiere un gran valor: la gobernanza del internet en ALC es un tema emergente que involucra múltiples actores, incluidos los Gobiernos, el sector privado, la sociedad civil y los organismos internacionales. La búsqueda de un equilibrio entre la regulación estatal y la libertad en línea, así como entre la protección de los derechos digitales y la promoción de una internet abierta, segura y accesible para todos, son desafíos cruciales en la agenda regional.

El continente enfrenta un panorama multifacético y, más allá de los avances significativos la región que ha registrado en calidad democrática y en integración regional, persisten problemáticas relacionadas con la desigualdad, la falta de infraestructura tecnológica y la tarea compleja de proveer ciberseguridad. La intersección entre la ciberdiplomacia y la gobernanza del internet se impone como un tópico crítico para navegar estos desafíos, y se requiere un enfoque colaborativo entre diversos actores para garantizar un desarrollo digital inclusivo, seguro y sostenible. La cooperación regional, la inversión en tecnología y la promoción de políticas públicas adecuadas

son esenciales para aprovechar las oportunidades y enfrentar los riesgos en el ámbito digital, y construir así un futuro más próspero y equitativo para todos los habitantes de la región.0.6

La pandemia de COVID-19 y la ciberdiplomacia en América Latina y el Caribe

La pandemia de la COVID-19 ha dejado un impacto profundo en la región. Desde principios del año 2020, afectó tanto el ámbito sanitario como el socioeconómico, situación que generó desafíos significativos para los sistemas de salud, la estabilidad económica y la cohesión social en varios países (SELA, 2023b). En lo que respecta a la salud pública, la rápida propagación del virus presionó intensamente los sistemas de atención médica y trajo aparejadas medidas de confinamiento y distanciamiento social para frenar su avance. Estas acciones, aunque necesarias para contener el virus, tuvieron grandes impactos socioeconómicos, como la pérdida de empleos, el cierre de negocios y perturbaciones en las cadenas de suministro.

En ese sentido, es esencial no perder de vista que las desigualdades preexistentes amplificaron las consecuencias de la pandemia, afectaron, de manera desproporcionada, a comunidades vulnerables, relevando la necesidad de fortalecer los sistemas de salud y de mejorar el acceso a la atención médica. La cooperación regional e internacional desempeñó un papel vital en la adquisición de suministros médicos y en el intercambio de información y de mejores prácticas. Además, cuando los efectos de la pandemia tendían a disminuir, el conflicto entre Rusia y Ucrania afectó las previsiones económicas globales y los pronósticos de recuperación, ya que impactó en áreas clave como el comercio mundial, el aumento de los costos de transporte internacional y la seguridad alimentaria (SELA, 2022a).

Desde una perspectiva económica, la región experimentó una contracción significativa debido a que se interrumpieron las actividades comerciales y cayó la demanda global. En un escenario en el que los países más dependientes de sectores como el turismo y la exportación de materias primas

enfrentaron mayores desafíos, la recuperación económica posterior mostró las marcadas diferencias entre naciones, las cuales estuvieron influenciadas por factores como la diversificación económica y la adaptabilidad a los cambios impuestos por la pandemia (SELA, 2023b).

Por otro lado, y en relación con los temas aquí tratados, la pandemia ha actuado como un catalizador para acelerar la digitalización y la modernización, ya que transformó el modo en que los Gobiernos, las empresas y los actores de la sociedad civil interactúan y se relacionan en el ciberespacio. Desde el enfoque de la ciberdiplomacia, este cambio ha planteado nuevos desafíos y oportunidades en términos de gobernanza digital, cooperación regional y diplomacia en el ciberespacio y ha inaugurado un nuevo contexto en el que se destaca la importancia de contar con infraestructuras digitales robustas y seguras. Los países de la región han reconocido la necesidad de invertir en el desarrollo de TIC y, consecuentemente, en la ciberseguridad para garantizar la continuidad de servicios esenciales, facilitar el trabajo remoto, la educación en línea y la prestación de servicios públicos digitales.

El camino acelerado hacia la digitalización ha impulsado iniciativas para fortalecer la infraestructura tecnológica y promover estándares de seguridad cibernética a nivel regional, lo que pone de manifiesto que el ejercicio de la ciberdiplomacia se hace cada vez más necesario. A partir de la pandemia y las medidas de confinamiento adoptadas para contener su avance, se ha incentivado la adopción de herramientas y plataformas digitales para la diplomacia y la cooperación internacional. Los mecanismos virtuales de diálogo y negociación se han vuelto más frecuentes, permitiendo a los países mantener relaciones diplomáticas, participar en foros internacionales y avanzar en agendas de cooperación en el ciberespacio. La adaptación a estos nuevos métodos ha requerido un enfoque proactivo para aprovechar las oportunidades que ofrece la digitalización en el ámbito diplomático.

Cooperación entre países para establecer regulaciones comunes

La ciberdiplomacia demanda una colaboración intergubernamental efectiva para abordar desafíos transfronterizos en el ciberespacio. ALC, con su

diversidad geográfica, política y económica, ha reconocido la necesidad de trabajar conjuntamente para establecer regulaciones comunes que promuevan un ciberespacio seguro, abierto y participativo. La colaboración cibernética internacional se presenta desde diversas perspectivas: se considera multilateral debido a que muchos esfuerzos conjuntos ocurren en foros regionales ya establecidos que tienen diferentes grados de alcance geográfico. Se entiende como multinivel porque existen iniciativas que abarcan toda la región, incluida América del Norte, junto con acuerdos específicos para ALC, así como programas más focalizados en subregiones como Sudamérica y Centroamérica (Vega, 2023).

En el contexto latinoamericano y caribeño, organismos como el SELA han sido plataformas clave para fomentar la cooperación regional en ciberseguridad y ciberdiplomacia. Sus iniciativas buscan promover estándares comunes, compartir mejores prácticas y fortalecer la capacidad técnica de los países miembros para hacer frente a amenazas cibernéticas emergentes.

Sin embargo, la experiencia latinoamericana y caribeña también evidencia desafíos significativos, como la disparidad en capacidades técnicas, la divergencia en marcos normativos nacionales y las tensiones geopolíticas entre algunos países. Estos factores han acentuado la necesidad de una diplomacia activa y pragmática para construir consensos y fomentar la confianza mutua en la región.

Al comparar ALC con otras regiones, como la Unión Europea (UE) o Asia-Pacífico, se observan diferentes enfoques y mecanismos de cooperación en ciberdiplomacia. Mientras que la UE ha avanzado en la armonización de regulaciones y políticas en materia de protección de datos y ciberseguridad a través del Reglamento General de Protección de Datos (RGPD) y la Estrategia de Ciberseguridad de la UE, Asia Pacífico ha adoptado enfoques más pragmáticos basados en la cooperación bilateral y multilateral, impulsados por iniciativas como el Diálogo ASEAN-Japón sobre Ciberseguridad. Por su parte, en los Estados Unidos de América, la cuestión de la protección de los datos ha estado en agenda desde el escándalo mediático

producido por las filtraciones de Edward Snowden (Riordan, 2019), el cual explica, en parte, la respuesta de la UE y de otros Estados ante la cuestión.

A pesar de las diferencias regionales, es evidente la necesidad global de establecer normas y principios comunes en ciberdiplomacia. La colaboración entre países y regiones, basada en el respeto mutuo, la transparencia y la confianza, se presenta como el camino a seguir para garantizar un ciberespacio inclusivo, resiliente y seguro a nivel global.

Más allá de las iniciativas regionales, es esencial destacar el papel de las organizaciones y los foros internacionales para promover la cooperación en ciberdiplomacia. Entidades como la ONU y la OEA han jugado un rol trascendental al facilitar el diálogo entre los Gobiernos y establecer directrices en áreas como la protección de infraestructuras críticas, la prevención de conflictos cibernéticos y la promoción de una gobernanza inclusiva y equitativa de internet.

En este contexto globalizado, los incidentes cibernéticos transfronterizos, como los ataques cibernéticos, el ciberespionaje y la desinformación, han reforzado la necesidad de una cooperación internacional más estrecha. La naturaleza interconectada del ciberespacio implica que ningún país puede abordar estos desafíos de manera aislada. Por lo tanto, la colaboración en ciberdiplomacia se ha convertido en una prioridad estratégica para fortalecer la seguridad, la estabilidad y la confianza en el ciberespacio a nivel global. Sin embargo, a diferencia de la postura de la OEA, que tiene un enfoque más orientado a la seguridad, distintas instituciones regionales como el Mercosur y la Alianza del Pacífico, en Suramérica, y el Sistema para la Integración Centroamericana (SICA), en Centroamérica, se enfocan, principalmente, en aspectos económicos y comerciales (Vega, 2023). Hace poco, los principales bloques regionales de integración han establecido plataformas dedicadas al ciberespacio, incluso dentro de sus respectivas agendas digitales institucionales, iniciativas que se centran en una perspectiva económica y privada y se enfocan en la utilización de las TIC y de la transformación digital para potenciar la gestión pública y la empresarial (Vega, 2023).

Como antecedente importante, a partir del año 2015, el SICA desarrolló la Estrategia Regional Digital (ERDI) para Centroamérica. En este marco, surgió la *Agenda Regional Digital 2022-2025* como un instrumento para fomentar su implementación. Esta incluye un área llamada Seguridad Digital, con el objetivo estratégico de fortalecer el marco jurídico regional, la ciberseguridad y la protección de la información de la población, así como coordinar acciones para prevenir y responder a incidentes cibernéticos. En la Agenda se detallan planes de acción bianuales, y en el periodo 2022-2023, el área de Seguridad Digital se centra en varias acciones en curso que incluyen la creación y la operación del Equipo de Respuesta ante Incidentes de Seguridad Informática Regional (CSIRTs-SICA, por sus siglas en inglés); el desarrollo de una guía regional de ciberseguridad; la realización de un encuentro regional de ciberseguridad; la formulación de una estrategia regional de seguridad digital y el establecimiento de un centro regional de ciberseguridad (Vega, 2023, p. 5).

En cuanto a herramientas y mecanismos específicos, los acuerdos bilaterales y multilaterales en ciberseguridad han ganado relevancia en los últimos años. Estos acuerdos permiten a los países compartir información, coordinar respuestas a incidentes cibernéticos y establecer protocolos de comunicación en caso de emergencias cibernéticas. Además, los centros de respuesta a incidentes cibernéticos regionales y nacionales[1] han facilitado la cooperación técnica y operativa entre países, mejorando la capacidad de respuesta y mitigación ante amenazas cibernéticas.

Desarrollo de normas regionales de ciberseguridad

La ciberseguridad se ha convertido en un pilar fundamental para garantizar la estabilidad, la confianza y el crecimiento sostenible en el entorno digital. En ALC, el desarrollo de normas de ciberseguridad se presenta como una necesidad imperativa para fortalecer la cooperación, mitigar

1 Registro de Direcciones de Internet para América Latina y Caribe (s. f.). CSIRTS de la región https://csirt.lacnic.net/csirts-de-la-region

riesgos y promover un ciberespacio seguro. Bustos Frati y Aguerre (2021) destacan los tres principales modelos que se han creado durante los últimos años para evaluar la seguridad en entidades públicas. Entre ellos, se encuentra el *Modelo de Madurez de Capacidad de Seguridad Cibernética,* desarrollado en la Universidad de Oxford por el BID junto con la OEA y el Centro de Construcción de Cibercapacidades de Oxford, que analiza aspectos como política, educación y tecnología. Otro de los modelos es el de la Unión Internacional de las Telecomunicaciones (UIT) que, de manera similar, evalúa el compromiso de los países con la ciberseguridad según pilares clave. De acuerdo con su versión 2018, ALC, después de África, es la región del mundo que muestra el menor grado de compromiso con la ciberseguridad (CEPAL, 2021). Finalmente, el último modelo de evaluación considerado es el *Índice de Preparación Cibernética 2.0*, del Instituto Potomac, apoyado por la OEA, que identifica indicadores específicos relacionados con la ciberseguridad.

Estos modelos ofrecen un inicio valioso para futuras investigaciones en el ámbito estatal y muestran claramente que, aunque ha habido avances en ciberseguridad en la región, aún persisten los desafíos (Bustos Frati y Aguerre, 2021), entre ellos, que muchos países carecen de estrategias específicas o de centros de control cibernético.

Por otro lado, hay estudios del sector privado, como el informe anual de ESET, que analiza incidentes de seguridad en empresas de la región y estrategias de protección. También es relevante mencionar colaboraciones entre organizaciones regionales y entidades estatales, por ejemplo, las iniciativas del Comité Interamericano contra el Terrorismo (CICTE), de la OEA, con organismos de Colombia. Estas colaboraciones muestran la importancia de la cooperación regional en ciberseguridad, ya que es fundamental tener una escala coherente para evaluar capacidades institucionales, pero también reconocer las particularidades y las estrategias de cada Estado (Bustos Frati y Aguerre, 2021).

A pesar de los avances, el desarrollo de normas regionales de ciberseguridad enfrenta desafíos significativos, como la disparidad en capacidades técnicas,

la diversidad de marcos normativos nacionales y las diferencias geopolíticas entre países. La búsqueda de la ciberseguridad en ALC resalta la importancia de la OEA en la creación de propuestas diplomáticas en este ámbito, puesto que el enfoque pionero de la región hacia la ciberseguridad se debe, en gran medida, a las acciones y propuestas impulsadas por este organismo (Vega, 2023). Estos factores requieren una diplomacia activa y pragmática para construir consensos, fomentar la confianza mutua y superar barreras en la armonización de regulaciones, además de representar oportunidades para fortalecer la cooperación técnica, compartir mejores prácticas y desarrollar capacidades especializadas a nivel regional.

El desarrollo de normas regionales de ciberseguridad no es un reto exclusivo de los Gobiernos, porque requiere la participación del sector privado, la sociedad civil, el sector académico, entre los actores más relevantes. La colaboración multisectorial con agentes diversos permite integrar diferentes perspectivas, aprovechar el conocimiento especializado y desarrollar soluciones innovadoras en ciberseguridad, así como facilitar la implementación efectiva de normas regionales y promover la adopción de mejores prácticas y estándares de seguridad en el ecosistema digital.

Al observar el panorama mundial, es evidente la interdependencia entre regiones en materia de ciberseguridad. La colaboración internacional, basada en el respeto mutuo y la cooperación, es clave para establecer normas y principios comunes que fortalezcan la seguridad cibernética a nivel global. En este sentido, la experiencia latinoamericana y caribeña en el desarrollo de normas regionales puede ofrecer lecciones valiosas y servir como modelo en la búsqueda de un ciberespacio más seguro, resiliente y confiable para todos.

Cabe mencionar que Vega (2023) distingue dos perspectivas de la ciberdiplomacia, a saber: a nivel hemisférico, se enfoca en la seguridad, con la promoción de la cooperación gradual; a nivel subregional, se aborda desde una óptica económica y de uso de las TIC que emerge en la agenda institucional. Ambas perspectivas, según este autor, destacan la ciberseguridad pero con énfasis distintos ya que, en el ámbito regional, se centra en la

ciberdelincuencia y la defensa, mientras que, en el subregional, se enfoca en aspectos técnicos y de protección de datos y en la integración económica. Aunque ALC ha avanzado de forma colaborativa en pos de lograr una mayor ciberseguridad, aún no alcanza la institucionalización de Europa, donde existen directrices claras y organismos específicos. En ese sentido, como se desprende de los datos del Observatorio de la Ciberseguridad en América Latina y el Caribe (2020), creación conjunta entre la OEA y el BID, la mayoría de los países de la región cuentan con una estrategia nacional de ciberseguridad o con, al menos, algún tipo de regulación o política pública sobre el tema, sin embargo, el nivel de desarrollo de cada país es muy dispar.

El desarrollo de normas regionales de ciberseguridad representa un paso importante para fortalecer la resiliencia cibernética y promover un ciberespacio seguro en ALC. A través de iniciativas regionales, colaboración multisectorial y cooperación internacional, la región puede avanzar hacia la creación de un marco normativo integral que proteja los intereses nacionales y promueva la confianza en el entorno digital.

Tabla 7

Adopción de estrategias nacionales de ciberseguridad en América Latina y el Caribe

País	Estrategia nacional de ciberseguridad	Año
Antigua y Barbuda	No	
Argentina	Sí	2017
Barbados	Sí	2013
Belice	Sí	2017
Bahamas	Sí	2014
Bolivia	Sí	2017
Brasil	Sí	2020
Chile	Sí	2017
Colombia	Sí	2016
Costa Rica	Sí	2017
Cuba	Sin datos	
Dominica	No	
República Dominicana	Sí	2018
Ecuador	En desarrollo	
El Salvador	No	
Granada	No	
Guatemala	Sí	2018
Guyana	Sí	2013
Haití	No	
Honduras	No	
Jamaica	Sí	2015
México	Sí	2017
Nicaragua	No	
Panamá	Sí	2013
Paraguay	Sí	2017
Perú	En desarrollo	
San Cristóbal y Nieves	No	
San Vicente y las Granadinas	No	
Santa Lucía	No	
Surinam	En desarrollo	
Trinidad y Tobago	Sí	2012
Uruguay	No	
Venezuela	No	

Nota. Elaboración propia sobre la base los datos de Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe, por el Observatorio de la Ciberseguridad en América Latina y el Caribe, 2020, BID y OEA.

CIBERSEGURIDAD Y POLÍTICA EXTERIOR

En el contexto actual, el ciberespacio se ha convertido en un componente básico de las relaciones internacionales y la política exterior de los países. ALC no es la excepción. De hecho, la región enfrenta desafíos y oportunidades únicas en el ámbito de la ciberseguridad y la ciberdiplomacia debido a su diversidad geopolítica, económica y social. La convergencia regional, que es uno de los objetivos principales del SELA, representa un escenario propicio para analizar cómo la intersección entre ciberseguridad y política exterior influye en la cooperación regional, la seguridad de cada país y las relaciones internacionales en un mundo cada vez más interconectado.

Este capítulo tiene como objetivo explorar la relación entre ciberseguridad y política exterior, situándose específicamente en el contexto de la región latinoamericana y caribeña. En el marco de una "definición amplia de la gobernanza de la ciberseguridad" (Bustos Frati y Aguerre, 2021, p. 4), las nociones de ciberseguridad y política exterior forman parte de los análisis de delitos informáticos y de la ciberdefensa.

Las amenazas cibernéticas emergentes, los esfuerzos regionales e internacionales para promover normas y principios para el ciberespacio, la cooperación regional en materia de ciberseguridad y el papel de la diplomacia digital en la promoción de los intereses nacionales y regionales, son los tópicos ineludibles que la realidad actual impone a todos los Estados y que moldean las discusiones sobre el futuro. Por ello, este capítulo no solo presenta los desafíos y las oportunidades que enfrentan los países de la región en lo que respecta a sus capacidades en ciberseguridad y su participación activa en el escenario internacional, sino que también ofrece insights y recomendaciones para fortalecer la cooperación regional, promover la seguridad cibernética y avanzar hacia una ciberdiplomacia inclusiva y equitativa.

Amenazas cibernéticas y su influencia

Las amenazas cibernéticas han surgido como un factor disruptivo en el panorama global e influyen sobre diversos aspectos de la política exterior, las normativas, la cooperación regional y las capacidades nacionales en el ci-

berespacio. Su naturaleza transnacional y evolutiva ha requerido respuestas adaptativas y colaborativas para mitigar sus impactos y riesgos asociados.

En el ámbito de la política exterior, los riesgos relacionados con el ciberespacio han reconfigurado las dinámicas tradicionales de las relaciones internacionales. Los ciberataques, el ciberespionaje y las operaciones de desinformación pueden ser utilizadas como herramientas de coerción, influencia y diplomacia encubierta entre Estados. Esta situación ha llevado a una reevaluación de las estrategias de política exterior y enfatiza la necesidad de promover la ciberseguridad como un elemento central de la agenda internacional y de fortalecer la capacidad de los Estados para proteger sus intereses nacionales en el ciberespacio.

En cuanto a las normas y los principios del ciberespacio, se han generado debates y tensiones sobre la elaboración de un marco normativo internacional que pueda regularlo y establecer parámetros comunes. La falta de consenso sobre las reglas de comportamiento responsable, la soberanía cibernética y los derechos digitales ha originado vacíos normativos que pueden ser explotados por actores maliciosos. Por ello, en este contexto, es imprescindible promover el diálogo internacional, la cooperación multilateral y la adopción de principios compartidos que reflejen los valores democráticos, los derechos humanos y un Estado de derecho en el ciberespacio.

Con respecto a la cooperación regional en ciberseguridad, se ha impulsado la creación de mecanismos de colaboración y coordinación entre países para enfrentar desafíos comunes. Los Estados están trabajando para construir redes de confianza, promover el intercambio de información, impulsar la formación del talento humano para estimular el desarrollo de capacidades regionales en ciberseguridad, esfuerzos que buscan fortalecer la resiliencia cibernética, promover la confianza mutua y establecer respuestas coordinadas a incidentes cibernéticos de gran envergadura que afecten la estabilidad y la seguridad regionales.

En el ámbito de las capacidades nacionales, los Estados han iniciado un camino de desarrollo de capacidades técnicas, operativas y estratégicas en ciberseguridad. Esto incluye la inversión en tecnologías avanzadas, la for-

mación de profesionales especializados, el fortalecimiento de infraestructuras críticas y la promoción de la cultura de ciberseguridad a nivel nacional. Además, como puede apreciarse a partir de los análisis del Observatorio de la Ciberseguridad en América Latina y el Caribe (2020), los Estados están adoptando políticas, estrategias y marcos normativos que promueven una aproximación integral y multidimensional a la ciberseguridad, considerando aspectos como la defensa, la inteligencia, la justicia, la diplomacia y la cooperación internacional.

Algunos de los peligros más prominentes relacionados con la red que han afectado a la región incluyen los ataques dirigidos a infraestructuras críticas, como los sistemas de energía y los servicios financieros y de salud. Además, se ha observado un aumento en campañas de desinformación y en la difusión de *fake news*, las cuales se sospecha que han podido influir en procesos electorales, socavando así la confianza pública en las instituciones democráticas. Por otro lado, los ransomwares (o secuestros de datos) que cifran datos y exigen pagos para su liberación, también han tenido un impacto significativo en empresas y entidades gubernamentales de varios países del continente.

Tabla 8

Tipos de amenazas cibernéticas en América Latina y el Caribe

Tipo de amenaza	Descripción	Ejemplos específicos	Impacto potencial
Ciberataques	Acciones maliciosas dirigidas a comprometer sistemas o datos.	Ataques a infraestructuras críticas: energía, finanzas, salud.	Interrupción de servicios, pérdida económica, daño reputacional.
Ciberespionaje	Obtención de información confidencial a través de actividades encubiertas.	Espionaje industrial, robo de información gubernamental.	Pérdida de propiedad intelectual, compromiso de la seguridad nacional.
Desinformación	Distribución de información falsa o engañosa para influir en opiniones o decisiones.	Campañas de desinformación durante procesos electorales, difusión de *fake news*.	Desconfianza pública, polarización social, daño a la democracia.
Ransomware	Software malicioso que bloquea el acceso a datos y exige un rescate para su liberación.	Ataques a empresas, entidades gubernamentales: cifrado de datos y demanda de pago.	Pérdida económica, interrupción de operaciones, daño reputacional.

Fuente: elaboración propia.

Intersección entre ciberseguridad y relaciones internacionales

Como ya se ha mencionado en este libro, la ciberseguridad y las relaciones internacionales se encuentran en una intersección crucial, lo cual refleja la naturaleza globalizada y digitalizada del mundo actual. Esta confluencia ha creado un escenario en el que las fronteras tradicionales se diluyen, y las acciones en el ciberespacio pueden tener repercusiones significativas en la estabilidad y la seguridad a nivel internacional.

Ejemplo de lo anterior es que las amenazas cibernéticas tienen la capacidad de trascender las fronteras nacionales y de afectar a Estados, organizaciones internacionales, infraestructuras críticas y entidades privadas en múltiples jurisdicciones. Esta naturaleza transnacional de los riesgos asociados a la red desafía las concepciones tradicionales de seguridad y exige respuestas cooperativas y coordinadas entre Estados para protegerse mutuamente contra las vulnerabilidades cibernéticas.

En este contexto, la diplomacia cibernética ha surgido como un instrumento clave para gestionar las tensiones y promover la cooperación en materia de ciberseguridad a nivel internacional. Los Estados están estableciendo mecanismos de diálogo y cooperación bilateral y multilateral para intercambiar información, compartir mejores prácticas y desarrollar normas y principios de comportamiento responsable en el ciberespacio. Estos esfuerzos buscan facilitar la coordinación y la respuesta conjunta a incidentes cibernéticos de gran envergadura, fortaleciendo así la seguridad y la estabilidad internacionales.

Además, el ciberespacio se ha convertido en un campo de batalla para la influencia y el poder entre Estados, donde las operaciones cibernéticas pueden ser utilizadas con el objetivo de proyectar poder, ejercer presión política, económica o militar y alcanzar objetivos estratégicos sin recurrir a conflictos armados convencionales. En este sentido, la capacidad de un Estado para proteger su infraestructura crítica y defenderse contra las amenazas cibernéticas se ha convertido en un elemento determinante de su posición y reputación en el escenario internacional, que redefine las dinámicas de poder y las relaciones entre actores globales.

Es también importante destacar que esta intersección entre la ciberseguridad y las relaciones internacionales plantea desafíos éticos y jurídicos fundamentales relacionados con la soberanía, la privacidad, los derechos humanos y el uso de la fuerza en el ciberespacio. Los Estados están trabajando activamente para desarrollar marcos normativos y legales que establezcan reglas claras y consensuadas a fin de regular las actividades cibernéticas, proteger los derechos y libertades fundamentales y promover un ciberespacio abierto, seguro y resiliente a nivel global.

Impacto en la seguridad regional

La intersección entre ciberseguridad y relaciones internacionales desempeña un papel vital y tangible en la configuración de la seguridad regional, especialmente en contextos geográficos y socioeconómicos específicos, como es el caso de ALC. En esta región, con una diversidad geopolítica, económica y social marcada, la interacción entre estos dos ámbitos se manifiesta en una serie de dimensiones complejas y variadas que abarcan desde esfuerzos de cooperación conjunta para fortalecer la ciberdefensa y proteger infraestructuras críticas hasta el surgimiento de tensiones y conflictos cibernéticos que pueden amplificar disputas preexistentes y generar nuevas áreas de fricción entre los países.

Además, la influencia de la ciberseguridad en las relaciones internacionales no solo se limita a aspectos técnicos u operativos, sino que también se extiende a cuestiones de política exterior, diplomacia digital y gobernanza cibernética, donde las decisiones y las acciones en el ciberespacio pueden tener efectos significativos en la estabilidad, la confianza y la cooperación regional.

Una de las manifestaciones más evidentes de esta intersección es el florecimiento de vulnerabilidades y amenazas cibernéticas compartidas. La creciente digitalización ha creado un escenario donde los ataques cibernéticos a infraestructuras críticas, sistemas financieros, Gobiernos y organizaciones regionales pueden generar repercusiones transfronterizas. Estos eventos pueden erosionar la estabilidad económica, política y social de múltiples naciones, lo que subraya la necesidad de una respuesta coordinada a nivel

regional. Ante estos desafíos, los países de la región están intensificando sus esfuerzos para fortalecer la cooperación en ciberseguridad.

A través de iniciativas regionales como las anteriormente mencionadas, se busca establecer mecanismos de diálogo, intercambiar información y desarrollar capacidades que contribuyan a construir un ciberespacio más seguro y resiliente. Sin embargo, a pesar de estos esfuerzos cooperativos, la interacción entre ciberseguridad y relaciones internacionales también puede generar tensiones. Las actividades cibernéticas maliciosas como el ciberespionaje o los ataques dirigidos, pueden ser utilizadas como herramientas para ejercer presión o influir en decisiones políticas, exacerbando las dinámicas de desconfianza entre Estados.

Adicionalmente, la interdependencia en el ciberespacio presenta desafíos para la gobernanza cibernética regional. Los Estados enfrentan la tarea compleja de desarrollar marcos normativos coherentes, promover la cooperación entre diferentes actores, proteger los derechos digitales fundamentales y fortalecer la resiliencia cibernética. Estos esfuerzos son fundamentales para gestionar eficazmente las amenazas, aprovechar las oportunidades y alcanzar una seguridad regional integral en el ciberespacio.

Organizaciones como la OEA han desempeñado un papel muy importante en la promoción de la ciberseguridad en la región. A través de su Programa de Ciberseguridad, este organismo ha facilitado el intercambio de mejores prácticas, la capacitación y la colaboración entre Estados miembros (Vega, 2023). Además, la creación de grupos de trabajo regionales ha permitido abordar desafíos comunes y establecer mecanismos de respuesta conjunta ante incidentes cibernéticos. En este sentido, la labor del SELA es vital para fortalecer la ciberseguridad regional a través de sus programas educativos y de cooperación destinados a facilitar el intercambio de conocimientos entre países miembros; evitar duplicidades y promover estrategias efectivas contra amenazas cibernéticas; impulsar la colaboración técnica para proteger infraestructuras críticas y capacitar a profesionales en políticas y tecnologías avanzadas. Asimismo, fomenta la armonización de normativas en áreas clave como la protección de datos y la ciberdefensa, estableciendo un marco normativo regional coherente y unificado.

Estrategias para fortalecer la ciberseguridad a nivel regional

En vista de la creciente interdependencia cibernética, fortalecer la ciberseguridad a nivel regional se convierte en una prioridad estratégica para garantizar la estabilidad, la confianza y el desarrollo sostenible de las naciones en un entorno digitalizado. Para lograrlo, es necesario adoptar un enfoque integral que abarque múltiples dimensiones y promueva la cooperación, la coordinación y la colaboración entre los países de la región.

Una de las estrategias clave consiste en **fomentar la cooperación regional en ciberseguridad a través del establecimiento de mecanismos de diálogo y colaboración**. Esto implica crear plataformas y espacios de intercambio de información, mejores prácticas y lecciones aprendidas entre Estados, organizaciones regionales, el sector privado y la sociedad civil. Tales mecanismos facilitan la construcción de una comunidad cibernética regional confiable y promueven la transparencia, la confianza mutua y la respuesta coordinada a incidentes cibernéticos de gran envergadura.

Para abordar estos desafíos, los países de ALC deben **fortalecer también la cooperación técnica y financiera en ciberseguridad**. La creación de un fondo regional dedicado a la ciberseguridad que facilite la inversión en tecnologías avanzadas, la capacitación especializada y el desarrollo de capacidades se presenta como un primer paso fundamental. Es necesario promover la participación activa del sector privado, la academia y la sociedad civil en iniciativas regionales, asegurando así una aproximación integral y colaborativa para construir un ciberespacio seguro y resiliente.

A partir de lo expuesto, se desprende la necesidad de **desarrollar capacidades nacionales y regionales en ciberseguridad a través de programas de formación, capacitación y fortalecimiento institucional**. Esto incluye el fomento de la investigación, el desarrollo e innovación en ciberseguridad, así como la creación de centros de excelencia, laboratorios de respuesta a incidentes y redes de expertos que contribuyan al fortalecimiento de las capacidades técnicas, operativas y estratégicas en la región.

Otra estrategia importante consiste en **promover la armonización y la cooperación en materia normativa y legal en ciberseguridad a nivel regional**.

Ello implica trabajar conjuntamente en la elaboración, adopción e implementación de marcos normativos y legales que establezcan reglas claras, consistentes y coordinadas en áreas como la protección de datos, los delitos cibernéticos, las infraestructuras críticas y la ciberdefensa, entre otros.

En ese sentido, es fundamental **fortalecer la resiliencia cibernética a nivel regional mediante la implementación de políticas, estrategias y medidas de seguridad que protejan las infraestructuras críticas, sistemas y redes contra amenazas informáticas emergentes**. Esto incluye la adopción de estándares de seguridad, buenas prácticas y tecnologías avanzadas para detectar y prevenir incidentes cibernéticos y dar respuesta ante ellos, así como impulsar la cultura de la ciberseguridad en todos los sectores y niveles de la sociedad.

Tabla 9

Estrategias y acciones propuestas con sus indicadores de resultado

Estrategias y acciones propuestas	Indicadores de resultados
Fomentar la cooperación regional	Número de plataformas de diálogo establecidas.
	Participación de países, organizaciones y sectores relevantes en mecanismos de cooperación.
	Incremento en el intercambio de información y mejores prácticas entre los países de la región.
Invertir en capacitación y desarrollo de capacidades	Número de programas de formación y capacitación implementados.
	Participación y certificación de profesionales y funcionarios en cursos especializados.
	Mejora en las capacidades técnicas, operativas y estratégicas en ciberseguridad.
Promover la participación del sector privado y la sociedad civil	Número de iniciativas y proyectos colaborativos establecidos con el sector privado y la sociedad civil.
	Participación y contribución en actividades y eventos regionales de ciberseguridad.
Desarrollar y armonizar marcos normativos y legales	Número de marcos normativos y legales armonizados y adoptados a nivel regional.
	Cumplimiento y aplicación efectiva de normativas y legislaciones en áreas clave de ciberseguridad.
Establecer fondos y mecanismos de financiamiento	Creación y financiamiento de fondos regionales de ciberseguridad.
	Inversión total en proyectos, tecnologías y capacidades de ciberseguridad a través de mecanismos de financiamiento regional.
Implementar políticas y medidas de seguridad cibernética	Adopción y aplicación de políticas, estrategias y medidas de seguridad cibernética en sectores críticos.
	Reducción en el número y el impacto de incidentes cibernéticos de gran envergadura a nivel regional.
	Mejora en la resiliencia y la respuesta ante amenazas cibernéticas emergentes.

Fuente: elaboración propia.

DESAFÍOS DE LA CIBERDIPLOMACIA EN MATERIA DE INTELIGENCIA Y DEFENSA

La interconexión global y la dependencia de las TIC han dado lugar a nuevos desafíos y vulnerabilidades que requieren respuestas estratégicas y cooperativas entre los actores estatales y no estatales. En este contexto, la ciberdiplomacia emerge como un campo interdisciplinario que busca articular políticas, normas y acciones para gestionar los riesgos y las oportunidades asociados con el ciberespacio. La ciberdefensa, entendida como la protección de sistemas, redes y datos contra amenazas cibernéticas, se sitúa en el centro de esta dinámica y adquiere una relevancia estratégica en las agendas de inteligencia y defensa de los Estados. Los incidentes cibernéticos, desde ciberataques sofisticados hasta operaciones de influencia y desinformación, pueden tener repercusiones significativas en la seguridad nacional, la estabilidad regional y las relaciones internacionales. Por lo tanto, la integración de la ciberdefensa en las estrategias de inteligencia y defensa se torna indispensable para garantizar la resiliencia, la seguridad y la soberanía en el ciberespacio.

En este capítulo, se exploran los desafíos específicos que enfrenta la ciberdiplomacia en materia de inteligencia y defensa y se analizan las amenazas emergentes, las vulnerabilidades sistémicas y las implicaciones en el contexto global y regional. A través de un enfoque analítico y reflexivo, se identifican tendencias clave y mecanismos de fortalecimiento para la cooperación internacional, la promoción de una gobernanza responsable y para mitigar los riesgos asociados con la ciberactividad maliciosa. Como sostienen Bustos Frati y Aguerre (2021), los ciberdelitos y la ciberdefensa son dos ámbitos de aplicación diferenciados dentro de una amplia definición sobre la gobernanza de la ciberseguridad, tema que fue abordado de manera más específica en el capítulo anterior.

Antes de profundizar en esta cuestión, es necesario recuperar algunas de las reflexiones sobre la red y el ciberespacio que ya se han mencionado en este manual. En ese sentido, es interesante rescatar el planteamiento de Riordan (2019) sobre el mundo digital como un mundo hobbesiano: al

considerar el ciberespacio a través del prisma de las ideas del filósofo inglés Thomas Hobbes sobre el "estado de naturaleza" y el "Leviatán", se lo puede comprender como un entorno anárquico donde diversos actores, desde los Estados hasta los individuos, compiten por recursos y seguridad sin una autoridad centralizada que regule sus acciones. Esta falta de regulación puede llevar a actividades maliciosas, como ciberataques y espionaje, y, al igual que Hobbes, propone un Leviatán para establecer el orden y superar el estado de naturaleza. En el ciberespacio, como también en el ámbito de las relaciones internacionales, surge la necesidad de algún tipo de autoridad o marco de gobernanza que pueda regular las actividades, garantizar la seguridad y resolver cuestiones de soberanía y jurisdicción. Dado este escenario, se plantea el valor de la ciberdiplomacia en tanto que posibilita acuerdos internacionales, normas de comportamiento y colaboraciones para abordar los desafíos y las oportunidades del ciberespacio de manera efectiva.

Al tratar estos temas, se busca contribuir al debate académico y político sobre la intersección entre ciberdiplomacia, inteligencia y defensa, ofreciendo insights para los tomadores de decisiones, emprendedores de políticas públicas, expertos en seguridad cibernética y los profesionales involucrados en la gestión de riesgos en el ciberespacio.

Ciberdefensa: conceptos básicos

La ciberdefensa se ha convertido en una pieza clave para garantizar la seguridad, la integridad y la disponibilidad de los sistemas de información y comunicación. Se refiere al conjunto de estrategias, políticas, técnicas y capacidades diseñadas para proteger los sistemas, redes y datos contra amenazas cibernéticas. Esto incluye la prevención y detección de incidentes cibernéticos que puedan comprometer la seguridad y la operatividad de las infraestructuras críticas y de las organizaciones y entidades gubernamentales, así como la respuesta y la recuperación ante estos.

En lo que respecta a los componentes de la ciberdefensa, es necesario tener en cuenta la prevención en términos de medidas proactivas como la activación de firewalls, sistemas de detección de intrusiones y políticas de seguridad para evitar vulnerabilidades y mitigar riesgos en los sistemas y

redes. Por otra parte, también es importante el monitoreo constante de la actividad cibernética para detectar patrones anómalos, comportamientos maliciosos y posibles amenazas que puedan afectar la integridad y la confidencialidad de la información.

Luego, es necesario dar una respuesta acorde a partir del desarrollo de planes de acción, protocolos de respuesta y capacidades de intervención rápida para neutralizar ciberataques, minimizar el impacto y restaurar la normalidad operativa en caso de incidentes cibernéticos. Por último, estos componentes estarían incompletos sin una recuperación y restauración de los sistemas, datos y servicios afectados por ciberataques que incluye la implementación de medidas de contingencia, backups y análisis forense para determinar el origen y el alcance de los incidentes.

Entre los principales objetivos que tiene la ciberdefensa pueden mencionarse los siguientes: i) garantizar la privacidad y confidencialidad de la información sensible y de los datos personales almacenados, procesados y transmitidos en los sistemas y redes; ii) asegurar la precisión, la consistencia y la fiabilidad de los datos, sistemas y servicios frente a manipulaciones, alteraciones y sabotajes cibernéticos y iii) garantizar la accesibilidad y la operatividad continua de los sistemas, redes y servicios, evitando interrupciones, denegaciones de servicio y degradaciones en su calidad.

La ciberdefensa, entonces, es un componente estratégico y operativo crucial para proteger la infraestructura crítica, salvaguardar la información sensible y garantizar la seguridad nacional en el ciberespacio. Al entender y aplicar sus conceptos básicos, pueden desarrollarse políticas, estrategias y capacidades efectivas para enfrentar los desafíos y las amenazas en el entorno digital. Por ello, es importante, en el plano de la ciberdefensa, ser capaz de adaptarse a las innovaciones tecnológicas, como la IA, el IoT y la computación en la nube, que amplían el perímetro de riesgo y complejidad en el ciberespacio. También es importante enfrentar amenazas emergentes, como ciberataques sofisticados, *ransomware*, ataques dirigidos y operaciones de influencia que requieren capacidades avanzadas de detección, atribución y respuesta. Para lograr superar estos desafíos, se hace necesario fortalecer la cooperación entre los sectores público y privado, así como a

nivel nacional e internacional, para compartir información, recursos y mejores prácticas en materia de ciberdefensa. Aquí el rol de la ciberdiplomacia vuelve a ser central, ya que permite mitigar el conflicto relacionado con ciberguerras, ciberespionaje, ciberterrorismo, uso de la información cibernética, etc. (Riordan, 2019).

Teniendo en cuenta lo expuesto, vale la pena aclarar que la ciberguerra se refiere a los conflictos y operaciones militares llevados a cabo en el ciberespacio con el objetivo de infligir daño, causar perturbaciones o lograr ventajas estratégicas en el ámbito nacional e internacional. En este contexto, los actores estatales emplean tácticas, técnicas y procedimientos cibernéticos para comprometer infraestructuras críticas, sistemas de defensa y redes de comunicación con el fin de desestabilizar adversarios, obtener información sensible o ganar superioridad en el campo de batalla digital. En ese sentido, el concepto hace referencia a un fenómeno que ocurre entre Estados o contra Estados (Riordan, 2019).

El ciberterrorismo se caracteriza por el uso de la tecnología cibernética para llevar a cabo actos de terrorismo, como ataques, sabotajes y acciones destructivas que tienen como finalidad causar pánico, generar desestabilización y provocar impactos socioeconómicos en la sociedad. Los grupos terroristas, extremistas y adversarios a distintos órdenes estatales utilizan el ciberespacio para difundir propaganda, reclutar seguidores, coordinar actividades y llevar a cabo operaciones cibernéticas dirigidas contra infraestructuras críticas, entidades gubernamentales y objetivos simbólicos, con el fin de promover su agenda ideológica, política o religiosa a nivel nacional e internacional. No necesariamente hace referencia a un ataque espectacular, sino que también y, principalmente, a actividades como difusión de propaganda o robo de dinero para financiamiento (Riordan, 2019).

El ciberespionaje, por su parte, se centra en obtener, de forma clandestina, información sensible, secretos comerciales, datos gubernamentales y otros tipos de información mediante actividades de vigilancia, infiltración y compromiso de sistemas informáticos y redes de comunicación. En otras palabras, implica introducirse en los sistemas informáticos de otros Estados para obtener datos (Riordan, 2019). Los actores involucrados, que pueden

ser Estados, organizaciones o individuos, utilizan técnicas avanzadas de hacking, malware y phishing para acceder, recopilar y explotar información estratégica, política, económica o militar de objetivos específicos, con el propósito de obtener ventajas competitivas, influir en decisiones políticas o apoyar operaciones encubiertas. Según Riordan (2019), solo puede haber ciberespionaje si hay un actor gubernamental involucrado en el ataque.

El uso de la información cibernética en contextos de conflictos armados se ha convertido en una herramienta estratégica y táctica para influir en la percepción pública, desinformar a adversarios y coordinar operaciones militares en el campo de batalla digital (Riordan, 2019). Los Estados y los actores involucrados emplean técnicas de guerra psicológica, desinformación y manipulación de información para crear narrativas, difundir propaganda y ejecutar operaciones de influencia que pueden tener repercusiones políticas, sociales y militares significativas. Así, la información cibernética se utiliza como un medio para alcanzar objetivos estratégicos, ganar ventajas competitivas y ejercer poder blando o coercitivo en el ámbito nacional e internacional.

Tabla 10

Tipos de ciberataques más comunes

Tipo de ciberataque	Descripción breve	Impacto principal
Ransomware	*Software* malicioso que bloquea el acceso a archivos o sistemas hasta que se pague un rescate.	Pérdida de datos, interrupción de operaciones.
Phishing	Intento de adquirir información personal mediante el engaño, generalmente, a través de correos electrónicos o sitios web falsificados.	Robo de información, fraude.
Malware	*Software* diseñado para dañar, alterar o robar información sin el consentimiento del usuario.	Daño a sistemas, robo de datos.
DDoS	Ataque de denegación de servicio que sobrecarga un sistema con tráfico, haciéndolo inaccesible para usuarios legítimos.	Interrupción de servicios, pérdida de ingresos.
Ciberespionaje	Acceso no autorizado a información sensible o secreta de organizaciones o Gobiernos con fines de espionaje.	Robo de información confidencial, espionaje.
Man-in-the-middle	Ataque donde un perpetrador intercepta y, posiblemente, altera la comunicación entre dos partes sin que ninguna se dé cuenta.	Intercepción de datos, manipulación de información.

Fuente: elaboración propia.

Desarrollo de capacidades de defensa a nivel regional a partir de la ciberdiplomacia

La ciberdiplomacia se ha posicionado como un instrumento estratégico para fomentar la cooperación, fortalecer la confianza y promover la estabilidad en el ciberespacio a nivel regional e internacional. En ALC, ofrece oportunidades significativas para desarrollar capacidades de defensa cibernética, mejorar la coordinación regional y enfrentar desafíos comunes en materia de ciberseguridad.

A través de la ciberdiplomacia, los países de la región pueden establecer mecanismos de cooperación, intercambiar información y colaborar técnicamente para desarrollar robustas competencias de seguridad en el ámbito digital. Esto incluye la creación de plataformas regionales, centros de operaciones conjuntas y programas de capacitación en ciberseguridad, con el objetivo de compartir mejores prácticas, recursos y conocimientos especializados entre los Estados miembros. También facilita el diálogo político y técnico entre los países de la región para promover la adopción de normas, principios y reglas de comportamiento responsable en el ciberespacio. Ello comprende la participación en iniciativas multilaterales, foros regionales y acuerdos bilaterales que establezcan estándares comunes, principios de soberanía y responsabilidad en la gestión y el uso del ciberespacio, lo cual contribuye a la construcción de un entorno cibernético seguro, confiable y resiliente.

Por otro lado, la ciberdiplomacia impulsa la formulación de políticas, estrategias y programas nacionales de ciberdefensa que se alineen con los objetivos, principios y compromisos regionales. Ello abarca la inversión en infraestructuras críticas, tecnologías emergentes y capacidades humanas en ciberseguridad, así como la colaboración con actores regionales, por ejemplo, organizaciones internacionales, el sector privado y la sociedad civil, para fortalecer la resiliencia, la innovación y la competitividad en el ámbito cibernético. Asimismo, facilita la preparación, coordinación y respuesta ante incidentes cibernéticos de gran escala que puedan afectar la seguridad, la estabilidad y la operatividad de la región. Esto se logra mediante el establecimiento de protocolos de comunicación, mecanismos de alerta tem-

prana y equipos de respuesta conjuntos que permitan una acción rápida, efectiva y coordinada entre los países afectados, minimicen el impacto y escalen la situación a nivel diplomático, en caso de ser necesario.

Además, a través del intercambio de información, evaluaciones de riesgo y buenas prácticas en ciberdefensa, se contribuye a construir un ambiente de confianza, transparencia y cooperación entre los países de ALC. Es fundamental la organización de talleres, seminarios y ejercicios conjuntos que promuevan el entendimiento mutuo, la colaboración estratégica y la consolidación de alianzas regionales en el ámbito cibernético, tareas en las que el SELA ha colaborado y proyecta continuar colaborando.

Colaboración entre países para enfrentar amenazas cibernéticas

Las amenazas cibernéticas representan desafíos multifacéticos que trascienden las fronteras nacionales y requieren respuestas coordinadas, cooperativas y estratégicas entre países, por lo que la colaboración internacional en el ámbito de la ciberseguridad se ha convertido en un elemento esencial para mitigar riesgos, fortalecer la resiliencia y garantizar la estabilidad en el ciberespacio.

La cooperación entre países facilita el intercambio oportuno y efectivo de información, inteligencia y datos relacionados con amenazas cibernéticas, tendencias emergentes y vulnerabilidades identificadas. Esto permite a los Estados miembros anticipar y detectar ciberataques, intrusiones y actividades maliciosas en sus sistemas y redes y responder de manera proactiva ante ellos, para mejorar así la capacidad de análisis, atribución y mitigación de riesgos a nivel nacional e internacional. También posibilita la coordinación de respuestas y operaciones conjuntas entre países para enfrentar amenazas cibernéticas de gran escala, sofisticación e impacto a partir del desarrollo de estrategias de respuesta, protocolos de acción y capacidades de intervención rápida a fin de neutralizar amenazas, minimizar el impacto y restaurar la normalidad operativa en el ciberespacio. De este modo, se promueven la seguridad, la estabilidad y la confianza entre los Estados afectados.

Es importante, además, el establecimiento de normas, principios y marcos regulatorios comunes en materia de ciberseguridad, gobernanza del cibe-

respacio y protección de infraestructuras críticas, lo cual se logra a partir de la participación en iniciativas multilaterales, foros regionales y acuerdos internacionales que impulsen estándares de conducta, responsabilidad compartida y cooperación estratégica entre Estados, organizaciones y actores relevantes en el ámbito cibernético.

Por otro lado, la formación, el desarrollo de capacidades y el fortalecimiento de competencias técnicas entre países para enfrentar amenazas cibernéticas son aspectos para considerar. Esto incluye la organización de talleres, seminarios, ejercicios conjuntos y programas de formación especializada que alienten la colaboración, el intercambio de experiencias y la transferencia de conocimientos en áreas críticas de ciberdefensa, investigación y desarrollo tecnológico en el ámbito digital.

La colaboración entre países contribuye a fomentar un ambiente de confianza, cooperación mutua y entendimiento estratégico en el ciberespacio a través de herramientas como el establecimiento de relaciones bilaterales, diálogos políticos y mecanismos de consulta. A través de ellas, se busca favorecer la transparencia, la comunicación y la colaboración entre Estados; fortalecer alianzas; construir consensos; y consolidar esfuerzos conjuntos para enfrentar amenazas cibernéticas a nivel global.

En el contexto específico de ALC, la colaboración entre países para enfrentar amenazas cibernéticas adquiere una relevancia particular debido a las características regionales, los desafíos compartidos y las oportunidades de cooperación en el ámbito de la ciberseguridad. Organizaciones como el SELA, la OEA y otros foros regionales han promovido el intercambio de experiencias, buenas prácticas y recursos entre países con la creación de redes de expertos, centros de respuesta a incidentes y programas de capacitación en ciberdefensa. De esta forma, el impulso al desarrollo de capacidades nacionales y regionales en ciberseguridad es una tarea que continúa hasta el presente y que fortalece la resiliencia, la innovación y la competitividad en el entorno digital. Esto incluye la implementación de estrategias nacionales de ciberseguridad, programas de formación especializada y proyectos de investigación colaborativa que aborden desafíos comunes, como el ciberespionaje, el ciberterrorismo y la protección de infraestructuras críticas en la región.

Por otro lado, la cooperación internacional propicia la armonización de normativas, marcos legales y políticas públicas en ciberseguridad entre países del continente. Tales acciones incluyen la adopción de estándares internacionales y de principios de soberanía digital y responsabilidad compartida que promuevan un enfoque integrado, coherente y colaborativo en la gestión y la gobernanza del ciberespacio y garanticen la protección de los derechos humanos, la privacidad y la libertad en la era digital. La cooperación internacional también contribuye a fortalecer la confianza, la cooperación mutua y la solidaridad en la región a partir de una perspectiva inclusiva, participativa y democrática de la ciberseguridad y del establecimiento de alianzas estratégicas y de mecanismos de consulta y plataformas de diálogo que fomentan la comunicación, la transparencia y la colaboración entre Estados, la sociedad civil, el sector privado y el académico para construir un ecosistema cibernético seguro, confiable y resiliente para todos los actores involucrados.

El papel de la inteligencia en la toma de decisiones ciberdiplomáticas

El papel de la inteligencia es fundamental para proporcionar información, análisis y evaluaciones que permitan a los tomadores de decisiones comprender las amenazas, oportunidades y riesgos asociados con el ciberespacio. La inteligencia cibernética, que incluye la monitorización de redes, sistemas y plataformas digitales, se encarga de recopilar datos relevantes sobre las capacidades, intenciones y actividades de los actores estatales y no estatales en el ciberespacio.

Una vez recopilada la información, los analistas de inteligencia la evalúan y analizan para comprender las tendencias, patrones y comportamientos en el ciberespacio, lo que les permite identificar amenazas emergentes, evaluar la capacidad de los adversarios y anticipar posibles escenarios de ciberataques o conflictos. Los informes de inteligencia proporcionan a los decisores políticos, diplomáticos y militares información sensible para desarrollar estrategias, políticas y acciones en el ámbito cibernético, como la identificación de objetivos estratégicos, la evaluación de riesgos y la formulación de respuestas proporcionadas y efectivas a las amenazas cibernéticas.

La inteligencia cibernética puede jugar un papel clave en la diplomacia preventiva, pues facilita la comunicación, los acuerdos y la cooperación entre países para mitigar tensiones, resolver disputas y evitar conflictos en el ciberespacio. Al proporcionar información objetiva y verificable, pueden establecerse canales de diálogo y mecanismos de confianza mutua entre los actores involucrados.

En caso de ciberataques, intrusiones o incidentes en línea de gran escala, la inteligencia cibernética es clave para gestionar la crisis, atribuir la responsabilidad y coordinar la respuesta nacional e internacional. Esto incluye identificar a los perpetradores, evaluar el impacto e implementar medidas de mitigación, recuperación y respuesta proporcional.

La inteligencia cibernética también facilita la cooperación internacional en la lucha contra el ciberdelito, el terrorismo cibernético y las amenazas cibernéticas transnacionales. A través del intercambio de información, análisis y mejores prácticas, pueden fortalecerse las alianzas, mejorar la coordinación y promover una respuesta colectiva y coordinada.

Figura 2

Conceptos relacionados con la utilización de la ciberdiplomacia en inteligencia y defensa

Fuente: elaboración propia.

CIBERDIPLOMACIA Y DERECHOS HUMANOS

Como se ha mencionado en capítulos precedentes, la ciberdiplomacia emerge como un campo estratégico fundamental para las relaciones internacionales, y más aún en regiones como ALC, donde se busca fortalecer la cooperación y el desarrollo sostenible. La interconexión global a través de las TIC ha generado oportunidades sin precedentes para el progreso económico, social y cultural, pero también plantea desafíos significativos en términos de seguridad, privacidad y —lo que interesa en este capítulo— protección de los derechos humanos.

Los derechos humanos, fundamentales para la dignidad, la libertad y el bienestar de todas las personas, constituyen el pilar central de las sociedades democráticas y justas. Estos derechos, consagrados en instrumentos y tratados internacionales, abarcan un amplio espectro de garantías fundamentales, incluidos el derecho a la vida, la libertad, la igualdad, la privacidad y la libertad de expresión que protegen a los individuos en contra de los poderes de los Estados nacionales. Ahora bien, en el contexto del mundo digital, los derechos humanos adquieren una relevancia especial, ya que se plantean nuevos desafíos para su protección y promoción.

El ciberespacio ofrece nuevas oportunidades para la participación política, pero también plantea retos en términos de fake news, propagandas en línea y ataques cibernéticos que pueden afectar los procesos democráticos. Otros problemas se relacionan con la brecha digital, entendida como la diferencia en el acceso y en el uso de las tecnologías, que puede exacerbar las desigualdades existentes y limitar el ejercicio de derechos fundamentales para grupos marginados o vulnerables.

La ciberdiplomacia, es decir, el uso de la diplomacia en el ciberespacio para promover intereses nacionales y globales se entrelaza inevitablemente con la protección y promoción de los derechos humanos en un entorno digital cada vez más complejo y dinámico. En este contexto, es imprescindible abordar cómo los Estados, las organizaciones regionales y los actores relevantes pueden colaborar de manera efectiva para garantizar que las políticas y prácticas en el ciberespacio se alineen con los principios fundamentales de los derechos humanos.

En ALC, la intersección entre ciberdiplomacia y derechos humanos se manifiesta en múltiples dimensiones, desde la ciberseguridad y la protección de datos personales hasta la libertad de expresión en línea y el acceso equitativo a la información. Este capítulo tiene como objetivo explorar dicha confluencia, con la convergencia regional en el horizonte, y proporcionar un análisis de los desafíos, oportunidades y mecanismos para fortalecer la cooperación regional en este importante ámbito. Así, se busca contribuir al desarrollo de estrategias políticas y normativas que promuevan una ciberdiplomacia inclusiva, transparente y orientada hacia el respeto irrestricto de los derechos humanos en la región.

Derecho internacional y ciberespacio

La aplicación del derecho internacional en el ciberespacio es un tema de debate y discusión entre los expertos y los organismos internacionales. Un hito significativo en este ámbito es el Convenio de Budapest sobre delitos cibernéticos, que busca establecer un marco legal para combatir infracciones, como el acceso ilícito a y la interferencia y el sabotaje de sistemas y datos informáticos. Este convenio, que entró en vigor en 2004, representa un esfuerzo inicial para adaptar el derecho internacional a los desafíos del ciberespacio, aunque su alcance y su aplicación pueden variar según los países.

El Manual de Tallinn (2013) es otro de los ejemplos de iniciativas que buscan establecer normas y principios para la conducta responsable de los Estados y otros actores en el ciberespacio.

Estos documentos ofrecen orientación sobre cuestiones como la ciberseguridad, la ciberdefensa y las ciberoperaciones, aunque su carácter no vinculante refleja la necesidad de un consenso más amplio sobre las normas y regulaciones en el ámbito internacional.

Por su parte, en el ámbito de la ONU, los expertos tienen diversas opiniones sobre cómo debe aplicarse el derecho internacional en el ciberespacio. Mientras algunos abogan por una regulación más estricta y vinculante, otros sostienen que el enfoque debe ser flexible y adaptarse a la naturaleza

Tabla 11

Lista de países de la región adheridos o invitados a la Convención de Budapest

País	Estatus	Año
Argentina	Estado parte	Ratificado en 2018
Brasil	Estado parte	Incorporado en 2022
Chile	Estado parte	Ratificado en 2017
Colombia	Estado parte	Ratificado en 2020
Costa Rica	Estado parte	Ratificado en 2017
República Dominicana	Estado parte	Ratificado en 2013
Guatemala	Estado invitado	-
México	Estado invitado	-
Panamá	Estado parte	Ratificado en 2014
Paraguay	Estado parte	Ratificado en 2018
Perú	Estado parte	Ratificado en 2019

Nota: Adaptado de Reporte Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe, por el Observatorio de la Ciberseguridad en América Latina y el Caribe, 2020, BID y OEA.

dinámica y transnacional de las amenazas cibernéticas. Estas discrepancias reflejan la complejidad de conciliar las normas tradicionales del derecho internacional con las realidades emergentes del ciberespacio. Sin embargo, el organismo sostiene que es imperativo asegurar la salvaguardia de los derechos humanos tanto en el ciberespacio como en entornos no digitales y destaca aspectos cruciales como el resguardo de la información personal y la confidencialidad, la gestión de la identidad digital, la aplicación de tecnologías de supervisión y la problemática de la violencia y del hostigamiento en línea. Estas temáticas suscitan una atención particular y demandan acciones concretas para garantizar un equilibrio justo y seguro en la intersección entre la sociedad y la tecnología.

En ese sentido, el documento elaborado por el Secretario General destinado a fortalecer la cooperación digital[2] propone una serie de acciones esenciales, tales como ubicar los derechos fundamentales en el núcleo de los marcos regulatorios y las legislaciones relacionadas con las tecnologías digitales; ofrecer una mayor guía sobre la aplicación de estándares de derechos humanos en la era digital; abordar las lagunas de protección que surgen debido a la constante evolución de las tecnologías digitales; desalentar la implementación generalizada de cortes de internet, así como el bloqueo y filtrado genérico de servicios, ya que se configura como una medida indispensable; establecer leyes nacionales basadas en los derechos humanos y prácticas que salvaguarden la privacidad de los datos; adoptar acciones empresariales claras y específicas para proteger los derechos de privacidad y otros derechos fundamentales; mejorar las garantías relacionadas con la identidad digital y cuidar a las personas de la vigilancia ilegal o innecesaria; elaborar leyes y enfoques basados en los derechos humanos para abordar el contenido en línea ilegal y perjudicial a fin de construir un entorno digital seguro y ético; establecer marcos de Gobierno de contenidos transparentes y responsables que defiendan la libertad de expresión, eviten prácticas excesivamente restrictivas y protejan a los más vulnerables para garantizar espacios en línea seguros; implementar directrices en todo el sistema de la ONU sobre la diligencia debida y las evaluaciones de impacto en derechos humanos en el uso de nuevas tecnologías para la protección de los derechos fundamentales en la era digital.

Por otra parte, existen debates sobre si el derecho internacional humanitario (DIH) puede aplicarse en el ciberespacio. Aunque el DIH fue diseñado, principalmente, para regular las hostilidades en un entorno físico, su aplicabilidad en el ciberespacio plantea desafíos y oportunidades, especialmente en lo que respecta a la distinción entre combatientes y civiles, la proporcionalidad en el uso de la fuerza y la protección de infraestructuras críticas.

Por otro lado, es vital reconocer que existen diferencias fundamentales entre el espacio físico y el ciberespacio que complican la aplicación directa del

2 United Nations (2020). Report of the Secretary-General. Roadmap for Digital Cooperation. UN. https://www.un.org/techenvoy/es/content/digital-human-rights

derecho internacional (SELA, 2022b). Estas diferencias incluyen cuestiones como la atribución de ataques cibernéticos, la neutralidad en la red y el control de armas cibernéticas, aspectos que no tienen equivalentes directos en el contexto físico y que requieren enfoques innovadores y adaptados.

La proliferación de actores no estatales y sucedáneos en el ciberespacio plantea desafíos adicionales para la aplicación del derecho internacional. El ciberespionaje, las operaciones encubiertas y las actividades maliciosas llevadas a cabo por estos actores exigen respuestas coordinadas y cooperativas a nivel global para garantizar la seguridad, la estabilidad y la protección de los derechos humanos.

Impacto de la ciberdiplomacia en los derechos humanos

El impacto de la ciberdiplomacia en los derechos humanos es un tema de creciente relevancia y complejidad en el contexto global actual. Si se tienen en cuenta derechos como el acceso a la información y la libertad de expresión, es mucho lo que puede decirse al respecto. A través de iniciativas diplomáticas en el ciberespacio, los Estados pueden colaborar para garantizar que las plataformas en línea sean accesibles y no estén sujetas a restricciones injustificadas que limiten el flujo libre de la información. Sin embargo, también existe el riesgo de que la ciberdiplomacia pueda utilizarse para justificar o perpetuar prácticas de censura y vigilancia digital, lo que podría socavar los derechos humanos en lugar de protegerlos.

En lo que respecta a la seguridad y a la privacidad en el mundo digital, la gobernanza de la red desempeña un papel estelar en la formulación de normas, principios y acuerdos internacionales relacionados con la ciberseguridad y la protección de datos personales. Al establecer marcos de cooperación y diálogo entre los Estados, se pueden desarrollar enfoques comunes para abordar amenazas cibernéticas transnacionales, como el ciberespionaje, el malware y los ataques informáticos. No obstante, es necesario que estos esfuerzos se realicen respetando los derechos humanos, a la par que se eviten prácticas que vulneren la privacidad y la integridad de las personas en línea.

Por otro lado, el desarrollo de la ciberdiplomacia en la región puede contribuir a promover la inclusión digital y, por ende, facilitar el ejercicio de derechos económicos y sociales como el acceso a la educación, al empleo y a los servicios públicos en línea. Al fomentar la cooperación regional e internacional en infraestructura tecnológica y capacidades digitales, pueden crearse oportunidades para reducir las brechas y garantizar que más personas se beneficien de las ventajas de la digitalización. No obstante, estos esfuerzos se deben realizar de manera equitativa a fin de garantizar que todas las personas tengan igualdad de acceso y oportunidades en el ciberespacio.

También puede influir en la gobernanza global del ciberespacio promoviendo modelos de participación ciudadana, transparencia y rendición de cuentas en la toma de decisiones relacionadas con la regulación y con el uso de las TIC. Al facilitar el diálogo multilateral y la cooperación entre diferentes actores, incluidos los Gobiernos, el sector privado, la sociedad civil y los expertos técnicos, pueden desarrollarse enfoques más inclusivos y democráticos para abordar los desafíos y las oportunidades del ciberespacio. Sin embargo, es menester que estos procesos se realicen de manera transparente y participativa a fin de garantizar que todas las voces sean escuchadas y consideradas en la formulación de políticas y estrategias en línea.

Protección de la privacidad en el ciberespacio

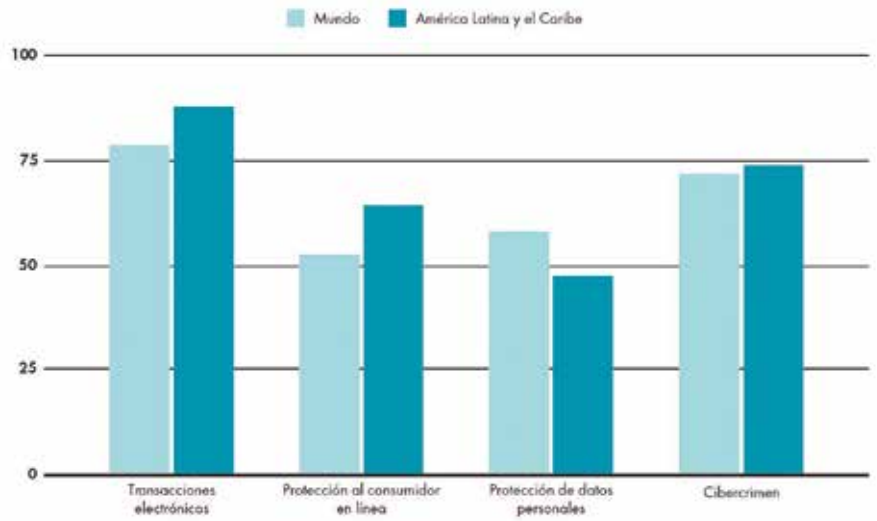
La protección de la privacidad en el ciberespacio se sitúa en el corazón de los derechos humanos, en particular, en el resguardo de la autonomía, la dignidad y las libertades fundamentales de las personas en el entorno digital. La privacidad no es simplemente un derecho técnico o legal, sino que también es un pilar central que sustenta una sociedad democrática, justa y equitativa, donde las personas pueden desarrollarse libremente sin temor a la vigilancia arbitraria o a la manipulación de su información personal.

La proliferación de las TIC, de las plataformas y de las redes sociales ha ampliado las posibilidades de interconexión y participación en el ciberespacio, pero también ha generado nuevos desafíos en términos de privacidad y derechos humanos. La recopilación masiva de datos, la vigilancia

digital y las prácticas de seguimiento en línea plantean interrogantes sobre la protección de datos personales y la integridad de la información en un contexto donde los Estados y los actores privados, dependiendo del caso, pueden ejercer un poder desproporcionado sobre los individuos. En este sentido, la regulación y la gobernanza del ciberespacio deben abordarse desde una perspectiva de derechos humanos a fin de garantizar que las políticas, prácticas y tecnologías implementadas respeten y protejan la privacidad y otros derechos fundamentales en línea. La adopción de marcos normativos robustos, como el Reglamento General de Protección de Datos (RGPD), en la UE, y las legislaciones nacionales en materia de protección de datos personales, representa un avance significativo en la armonización de la privacidad con los principios y valores de los derechos humanos que los países de ALC deben replicar. Entre los Estados de la región, son 16 los que cuentan con una ley específica sobre la protección de datos personales, y de ellos, 7 tienen leyes sectoriales, mientras que otros 10 carecen de legislación sobre el tema (CEPAL, 2021).

Figura 3

Comparativo de leyes relevantes para el comercio electrónico entre América Latina y el Caribe y el resto del mundo



Nota: Adaptado de Datos y hechos sobre la transformación digital, p. 27, por la CEPAL 2021, Documentos de proyectos (LC/TS.2021/20).

Asimismo, tanto la cooperación internacional como la regional son clave para fortalecer la protección de la privacidad en el ciberespacio al promover estándares comunes y mecanismos de rendición de cuentas que garanticen la implementación efectiva de los derechos humanos en todas las actividades y operaciones en línea. La colaboración entre los Estados, las organizaciones internacionales, la sociedad civil y el sector privado puede facilitar el intercambio de mejores prácticas, capacidades técnicas y recursos a los fines de abordar desafíos transnacionales y fomentar una cultura de privacidad basada en la dignidad humana. El rol de distintos organismos como el SELA es entonces fundamental para garantizar la cooperación y la convergencia. La ciberdiplomacia no debe perder de vista los derechos humanos en su perspectiva.

La ciberdiplomacia se presenta como un mecanismo facilitador para la construcción de consensos, normas y principios comunes que armonicen la innovación tecnológica con los derechos humanos en el ciberespacio. A través del diálogo multilateral, la negociación de acuerdos y la colaboración entre Estados, organizaciones internacionales y actores relevantes, la ciberdiplomacia puede contribuir a establecer marcos normativos robustos que salvaguarden la privacidad y protejan contra posibles abusos en línea. Es importante que la ciberdiplomacia y la diplomacia digital promuevan enfoques basados en los derechos humanos mediante la formulación de políticas y estrategias en el ciberespacio que garanticen que las medidas adoptadas sean proporcionadas, transparentes y estén sujetas a la rendición y revisión de cuentas. La cooperación internacional en materia de protección de datos, intercambio de mejores prácticas y capacitación en estándares de privacidad puede fortalecer la acción diplomática en la promoción de una cultura de privacidad respetuosa de la dignidad humana y de los principios democráticos. Además, la ciberdiplomacia puede facilitar la construcción de coaliciones y alianzas estratégicas entre Estados, la sociedad civil, el sector privado y las organizaciones internacionales para abordar desafíos emergentes en el ciberespacio, como la ciberseguridad, la vigilancia digital y la protección de datos personales. Al impulsar el diálogo inclusivo y la participación de diversos actores en la toma de decisiones, puede avanzarse hacia soluciones cooperativas que equilibren la innovación tecnológica con el respeto y con la protección de los derechos humanos en línea.

Desarrollo de políticas que equilibren la seguridad y los derechos individuales

En ALC, el desarrollo de políticas que equilibren la seguridad cibernética con el respeto de los derechos individuales representa un desafío serio para la construcción de sociedades democráticas, justas y equitativas en el entorno digital. Esta región, caracterizada por su diversidad cultural, socioeconómica y política, enfrenta retos específicos en términos de ciberseguridad, privacidad y protección de datos personales que requieren respuestas políticas integrales y basadas en los derechos humanos.

El equilibrio entre seguridad y derechos individuales en el ciberespacio implica la adopción de enfoques multidimensionales que consideren las necesidades y preocupaciones de diversos actores, incluidos los Gobiernos, la sociedad civil, el sector privado y las comunidades indígenas. En este contexto, es fundamental que las políticas y estrategias regionales y nacionales estén alineadas con los principios universales de los derechos humanos a fin de garantizar que las medidas adoptadas sean proporcionadas, necesarias y sujetas a rendición y revisión de cuentas.

Una de las dimensiones clave en el desarrollo de políticas equilibradas es la promoción de marcos normativos y regulatorios que armonicen la ciberseguridad con el respeto a la privacidad y la protección de los datos personales. La adopción de leyes sobre el tema, como la *Ley General de Protección de Datos Personales,* en Brasil, o la *Ley Federal de Protección de Datos Personales* en Posesión de los Particulares, en México, representa un avance significativo en la región para establecer estándares comunes y principios fundamentales en materia de privacidad y derechos humanos.

Asimismo, es necesario fortalecer una cooperación regional en ciberseguridad y protección de datos que promueva el intercambio de información, mejores prácticas y capacidades técnicas entre Estados miembros y organizaciones regionales, como el SELA. La colaboración multilateral puede facilitar la construcción de consensos, la implementación de iniciativas conjuntas y la elaboración de políticas públicas inclusivas que aborden desafíos transnacionales y regionales en el ciberespacio.

Por otro lado, hay que promover la participación activa y significativa de la sociedad civil, incluidas las comunidades indígenas, los grupos vulnerables y otros actores relevantes en la formulación, implementación y análisis de políticas y estrategias en el ámbito de la ciberseguridad y la protección de datos. Incluir y representar diversas voces y perspectivas puede enriquecer el debate público, garantizar la protección de derechos humanos y promover soluciones adaptadas a contextos locales y regionales específicos.

Se requiere, entonces, un enfoque integral, basado en los derechos humanos y centrado en la cooperación regional, la participación inclusiva y la armonización de marcos normativos. A través de la colaboración multilateral, la promoción de estándares comunes y la inclusión de diversas voces en el proceso político, es posible avanzar en la región hacia soluciones equitativas y sostenibles que respeten y protejan los derechos fundamentales en el ciberespacio.

Ciberdiplomacia, género y derechos

En tanto la ciberdiplomacia representa una oportunidad y un desafío para abordar cuestiones básicas de derechos humanos, es esencial considerar cómo esta actividad puede influir y ser influenciada por los derechos de las mujeres y de las diversidades. Sin embargo, antes de sumergirse en las potencialidades de la ciberdiplomacia en este ámbito, es imprescindible reconocer la brecha digital de género. Esta brecha no es más que el reflejo de las desigualdades existentes en cuanto al acceso, uso y control de la tecnología entre varones y mujeres, así como otras identidades de género y diversidades. Se trata de una desigualdad que limita la participación plena y equitativa en la sociedad digital, y obstaculiza la materialización de derechos fundamentales.

En este escenario, la ciberdiplomacia puede emplear herramientas digitales para promover activamente los derechos de las mujeres y de las diversidades. Las campañas en redes sociales se han mostrado eficaces para desafiar estereotipos de género, fomentar la igualdad, crear conciencia y movilizar a la sociedad civil. Además, la implementación de plataformas de denuncia en línea ofrece un espacio seguro donde mujeres y diversidades pueden infor-

mar violaciones a sus derechos, lo que genera respuestas rápidas y efectivas. Asimismo, la educación digital inclusiva es una herramienta indispensable en el diseño de programas de alfabetización que atiendan las necesidades específicas de estos grupos y fortalezcan capacidades y habilidades.

La incorporación de una perspectiva de género en la diplomacia digital podría contribuir al surgimiento de una corriente que tenga por propósito, mediante la participación activa de mujeres y diversidades en espacios de decisión, influir en las relaciones internacionales digitales. Para ello, es esencial forjar alianzas estratégicas entre los Estados, las organizaciones internacionales, la sociedad civil y el sector privado, es decir, buscar colaboraciones que permitan construir una agenda digital inclusiva, equitativa y con enfoque de género, y aborden, de manera integral, las necesidades y aspiraciones de las mujeres y de las diversidades.

No obstante, a pesar de los avances y de los esfuerzos, persisten desafíos significativos en la intersección entre ciberdiplomacia, género y derechos de las mujeres y de las diversidades. El aumento de la violencia de género en entornos digitales pone de manifiesto la urgencia de establecer políticas y mecanismos de protección robustos y efectivos. Asimismo, garantizar la igualdad de acceso y la participación en el espacio digital sigue siendo una meta pendiente. Sin embargo, en este panorama, también emergen oportunidades prometedoras ya que la colaboración regional y global, el desarrollo de capacidades y la promoción de políticas públicas inclusivas ofrecen caminos viables para avanzar hacia una ciberdiplomacia verdaderamente inclusiva y equitativa.

ECONOMÍA DIGITAL, TECHPLOMACIA Y MONEDAS DIGITALES

La economía digital se ha erigido como un pilar fundamental para el desarrollo y el crecimiento de las naciones, pues ofrece nuevas oportunidades en innovación, comercio e inclusión social. En este contexto, la techplomacia emerge como una herramienta para navegar las complejidades de la diplomacia en la era digital lo que permite a los países de la región fortalecer sus relaciones internacionales, promover sus intereses estratégicos y enfrentar desafíos globales, como la ciberseguridad y la gobernanza de internet (SELA, 2021).

Adicionalmente, el surgimiento de las monedas digitales y la tecnología blockchain plantea interrogantes y oportunidades sin precedentes para ALC en términos de inclusión financiera, eficiencia económica y soberanía monetaria. La adopción y regulación de estas nuevas formas de transacción y almacenamiento de valor requieren de un enfoque colaborativo y visionario que trascienda las fronteras nacionales y promueva la convergencia regional.

El enfoque en la ciberdiplomacia se centra en la aplicación de la diplomacia a los desafíos políticos y geopolíticos emergentes en el ciberespacio; va más allá del uso superficial de las redes sociales e internet: representa una disciplina en evolución constante que requiere una respuesta multilateral y cooperativa basada en el derecho internacional. Es un campo disciplinar emergente que requiere consolidar la ciberseguridad mundial y adoptar estrategias proporcionales a las amenazas del ciberespacio, caracterizado por fronteras difusas y actores con jurisdicciones no definidas.

Por otro lado, la techplomacia explora las interacciones entre los Estados y las grandes empresas tecnológicas, o big tech companies, las cuales destacan por su poder económico y geopolítico en el escenario global (SELA, 2023c). Es necesario abordar la regulación de estas empresas y su influencia en el ciberespacio, con hincapié en la importancia de trascender el uso de herramientas digitales con fines diplomáticos y adoptar estrategias políticas definidas en este ámbito (Riordan, 2019).

A nivel regional, países como Ecuador, Argentina, Brasil, Colombia, República Dominicana y México han incursionado en la ciberdiplomacia, mientras que, a nivel global, informes de organizaciones como el Banco Mundial y la Organización para la Cooperación y el Desarrollo Económicos (OCDE) resaltan el poder económico y geopolítico de las grandes empresas tecnológicas y plantean interrogantes sobre quién gobierna el ciberespacio y cómo abordar las complejidades jurídicas, fiscales y de responsabilidad asociadas.

Resulta, entonces, sumamente importante desarrollar capacidades en ciberdiplomacia y techplomacia para afrontar los desafíos emergentes en el ciberespacio, a la vez que se promueve la cooperación regional e internacional, la regulación efectiva de las empresas tecnológicas y la adopción de políticas públicas orientadas a fortalecer la gobernanza digital en beneficio de los países de la región (SELA, 2021). Este capítulo tiene como objetivo explorar la intersección entre la economía digital, la techplomacia y las monedas digitales en el contexto de ALC. Es por ello por lo que se da cuenta de los desafíos, oportunidades y perspectivas que estas transformaciones presentan para la región, así como las estrategias y políticas necesarias para impulsar una ciberdiplomacia efectiva y colaborativa que promueva la convergencia regional y el desarrollo sostenible en la era digital.

Vínculos entre la ciberdiplomacia y el desarrollo económico

La ciberdiplomacia se ha convertido en un instrumento vital que vincula estrechamente la diplomacia tradicional con las dinámicas económicas globales y juega un papel crucial en la promoción del desarrollo económico de las naciones. Uno de los principales ámbitos donde esta intersección se hace evidente es la facilitación del comercio digital, puesto que, a través de la negociación de acuerdos bilaterales y multilaterales, la ciberdiplomacia puede establecer normas y estándares que fomenten un ambiente propicio para el comercio electrónico transfronterizo; ello impulsa la integración económica regional y global, y crea condiciones más favorables para las empresas y emprendedores en el ámbito digital.

En este sentido, no debe perderse de vista que, en la búsqueda del crecimiento y de la integración, la diversificación productiva se convierte en

una estrategia clave para mejorar la participación en los mercados globales y promover el desarrollo económico de las naciones (SELA, 2023b). Esta diversificación puede lograrse a partir de un perfil detallado sobre las ventajas comparativas y de los posibles nichos productivos de las economías, cuestión sobre la cual el SELA ha avanzado desarrollando una metodología propia que examina las capacidades productivas de los países, habiendo considerado la evolución del factor trabajo, las exportaciones y la complejidad económica de los bienes producidos (SELA, 2023b). La ciberdiplomacia puede profundizar este proceso y ayudar a tender puentes entre países para la identificación y explotación de estos nichos.

La ciberdiplomacia, la techplomacia y las monedas digitales se han convertido en áreas fundamentales en la agenda internacional y su relevancia continúa creciendo en el contexto global actual (SELA, 2023c). Estas dimensiones no solo reflejan la evolución tecnológica y digital de la sociedad, sino que también determinan las relaciones entre naciones, empresas y ciudadanos, escenario en donde el papel del SELA adquiere un alcance significativo, ya que busca fortalecer la posición de ALC en estos ámbitos emergentes. Muestra de ello son las distintas acciones de capacitación que ha desarrollado en el área de la ciberdiplomacia y su relación con la techplomacia y con las monedas digitales.

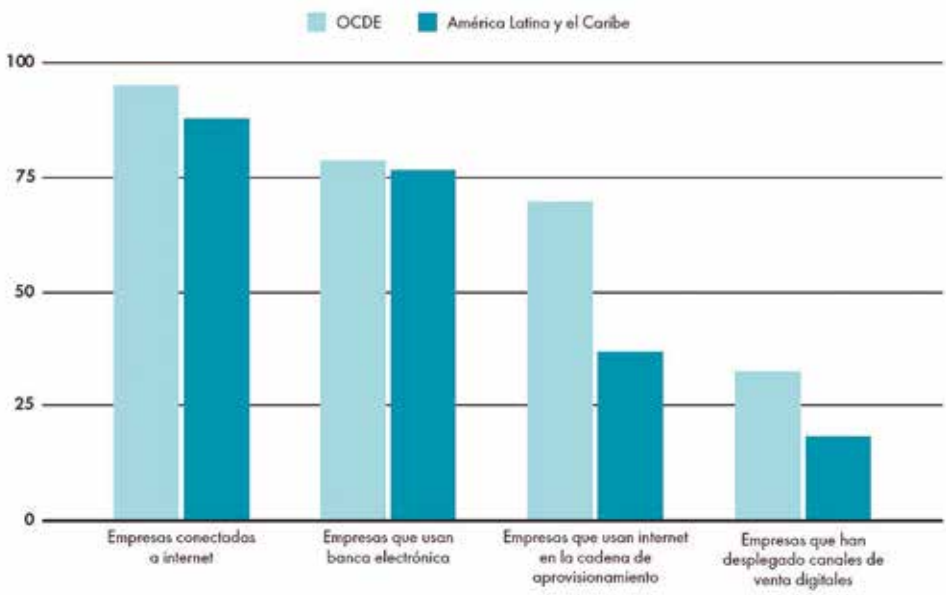
Por otro lado, la ciberdiplomacia desempeña un papel fundamental para atraer inversión extranjera directa e incentivar la cooperación internacional en sectores estratégicos de la economía digital, como la tecnología de la información y las telecomunicaciones. A través de la colaboración en proyectos de infraestructura digital, investigación y desarrollo, los países pueden impulsar iniciativas conjuntas que potencien el crecimiento económico, la competitividad y la innovación, a fin de generar empleo y riqueza en la economía digital.

En este contexto, la promoción de la innovación y el emprendimiento emerge como otra faceta clave de la relación entre la ciberdiplomacia y el desarrollo económico. Al facilitar la colaboración internacional en áreas como la educación, la formación técnica y la transferencia de tecnología se crea un ecosistema digital más dinámico y resiliente que fomenta la crea-

ción de startups y de soluciones innovadoras. Este impulso a la innovación contribuye a fortalecer la competitividad de las naciones en el escenario global y a generar un impacto positivo en la economía digital. El desafío que afronta la región es el de incorporar tecnologías digitales al proceso productivo, ya que, en comparación con otros países, aún queda camino por recorrer (CEPAL, 2021).

Figura 4

Digitalización de procesos productivos en OCDE y América Latina y el Caribe en 2018



Nota: Adaptado de Datos y hechos sobre la transformación digital (p. 21), por la CEPAL 2021, Documentos de proyectos (LC/TS.2021/20).

Por otro lado, la ciberdiplomacia también juega un papel significativo en la gobernanza del ciberespacio por cuanto colabora en la elaboración de políticas y regulaciones que garanticen un entorno digital seguro, confiable y abierto. Al establecer mecanismos de cooperación internacional en áreas como la ciberseguridad, la protección de infraestructuras críticas y la gestión de riesgos, pueden mitigarse amenazas y vulnerabilidades que podrían afectar la estabilidad económica y financiera de las naciones (SELA, 2022b).

Finalmente, es importante destacar que la ciberdiplomacia puede contribuir significativamente a reducir la brecha digital y promover la inclusión social al facilitar el acceso equitativo a las TIC. A través de iniciativas de cooperación regional e internacional, es posible implementar proyectos de infraestructura digital, capacitación y alfabetización tecnológicas que empoderen a comunidades y sectores vulnerables, lo cual impulsaría un desarrollo económico más inclusivo y sostenible en la comunidad global. La diplomacia digital permite a los países establecer diálogos, negociaciones y acuerdos en un entorno virtual, donde las fronteras físicas se difuminan. En este contexto, el SELA busca promover capacidades negociadoras en la gobernanza del ciberespacio para ALC, ya que su objetivo es que los países de la región participen activamente en la definición de normas, regulaciones y acuerdos internacionales que garanticen un uso seguro, equitativo y eficiente del ciberespacio, a la vez que se protegen los intereses regionales y se fomenta la cooperación multilateral.

Por su parte, la techplomacia se refiere a las relaciones y negociaciones entre Estados y las grandes empresas del sector tecnológico. Dada la influencia creciente de dichas entidades en la economía global y en la vida cotidiana

de las personas, es fundamental establecer un marco de cooperación y regulación. El SELA se posiciona como un actor clave en este ámbito al facilitar el diálogo entre los Estados miembros y las empresas tecnológicas en procura de un equilibrio entre los intereses comerciales y las necesidades de desarrollo, innovación y protección de los derechos digitales en la región.

Las monedas digitales, especialmente las criptomonedas, representan una revolución en el sistema financiero global y dada su capacidad para trans-

formar las transacciones financieras, la inversión y la política monetaria, su adopción y regulación son temas de debate en todo el mundo. El SELA (2023c) reconoce la importancia de abordar este fenómeno desde una perspectiva regional; por ello, promueve la investigación, la educación y la regulación de las monedas digitales en el continente con el objetivo de garantizar un entorno seguro, transparente y eficiente para las transacciones digitales, además de proteger a los usuarios y fomentar la inclusión financiera en la región.

Techplomacia: la promoción de la innovación y de la tecnología a través de la diplomacia

En el contexto actual, las plataformas tecnológicas y las redes sociales desempeñan un papel decisivo en diversos ámbitos como la democratización, las elecciones, las tendencias y las modas. Sin embargo, su impacto puede ser tanto positivo como negativo por lo que se requiere una regulación adecuada. En este sentido, áreas críticas como la gobernanza de internet, el cibercrimen y la ciberseguridad carecen de normas internacionales claras que guíen sus actividades, a pesar del avance acelerado de tecnologías como la IA, el aprendizaje automático, la robótica y el IoT, entre otras (Riordan, 2019).

Ante esta realidad, es imperativo que las cancillerías establezcan unidades especializadas en ciberdiplomacia para navegar de manera efectiva en el entorno virtual, utilizando herramientas diplomáticas apropiadas con el fin de proteger sus territorios contra posibles ataques cibernéticos. Además, la ausencia de fronteras claras en el ciberespacio requiere que los Estados creen unidades de ciberseguridad enfocadas en la defensa nacional, reconociendo este terreno como un dominio crítico que va más allá de los límites geográficos tradicionales.

En este contexto, la creación de un regulador internacional se presenta como una necesidad urgente, respaldada por instrumentos de ciberdiplomacia y techplomacia con el objetivo de establecer normas internacionales y promover un debate inclusivo entre actores públicos, privados, académicos y de la sociedad civil. Los países de ALC emergen como

actores clave en este diálogo internacional y ello representa una oportunidad única para la región de posicionarse como un puente estratégico entre Asia, Europa y Norteamérica.

Tanto en ALC como en la Unión Europea, se comparte el objetivo de garantizar un ciberespacio libre, seguro y con derechos fundamentales, aspecto que se pone de manifiesto en las estadísticas que revelan que, en la región, crece el porcentaje de la población usuaria de internet (CEPAL, 2021) lo que le otorga una voz relevante para exigir el establecimiento de normas y regulaciones en el ámbito digital. La gobernanza del ciberespacio representa un desafío crucial para el futuro del multilateralismo en el contexto de la globalización lo que requiere una adaptación y una reconceptualización del sistema internacional para asegurar un enfoque coherente y efectivo en el mundo cibernético (SELA, 2021).

La techplomacia emerge como un elemento clave en la intersección entre tecnología, política y diplomacia; ofrece un marco estratégico para promover la innovación y la tecnología a nivel internacional. Ha surgido como un concepto revolucionario desde que lo creara el Gobierno danés en 2017, y enfatiza la influencia de grandes empresas tecnológicas en los asuntos internacionales (Riordan y Torres Jarrín, 2020). Esta iniciativa ha llevado a la creación de "techembajadas" y a la designación de "techembajadores" en centros económicos y de poder, con lo que se reconoce a las big tech companies como actores internacionales equiparables a los Estados. Francia y Alemania siguieron esta iniciativa en 2018, aunque las propuestas francesa y alemana tienen focos diferentes y ninguna ha alcanzado el perfil del activo embajador danés.

La techplomacia complementa la diplomacia tradicional y reconoce a las empresas tecnológicas como actores geopolíticos (Riordan y Torres Jarrín, 2020). Además, realiza actividades de diplomacia pública para promover una mejor comprensión de su misión, incluidos la participación en conferencias y el lanzamiento de programas educativos, por lo que el rol del embajador tecnológico o techembajador se extiende más allá de una única ubicación física (Riordan y Torres Jarrín, 2020). El término "techplomacia" justamente da cuenta del objetivo que implica reunir información sobre

avances tecnológicos, discutir asuntos éticos y regulatorios con empresas tecnológicas y promover a un país como líder en tecnología. Las empresas tecnológicas, como las plataformas de redes sociales y motores de búsqueda, enfrentan desafíos para manejar la desinformación y garantizar la seguridad en línea, lo que incluye debates sobre cómo gestionar datos y cómo interactuar con Gobiernos y otras partes interesadas.

Esta evolución refleja el poder económico y geopolítico de las empresas en diversos ámbitos, desde lo político hasta lo cultural, contexto en el cual la diplomacia se convierte en una herramienta poderosa para facilitar colaboraciones bilaterales y multilaterales que impulsen el desarrollo tecnológico, la investigación y la innovación entre países y regiones.

El impacto de las empresas tecnológicas en la estabilidad geopolítica es innegable; su riqueza acumulada rivaliza con el PIB de numerosos países. Por ello, se destaca la necesidad de que los países de la región incorporen la techplomacia en su política exterior y establezcan relaciones internacionales con estas entidades para comprender y reglamentar su actividad en el ciberespacio, un dominio aún no regulado que requiere atención internacional. Con la proliferación de tecnologías como la 5G y la participación creciente de empresas tecnológicas no occidentales, como Huawei, en la definición de estándares industriales, se requiere una diplomacia tecnológica más estratégica (Riordan y Torres Jarrín, 2020). Las interacciones con empresas tecnológicas chinas, así como con otras en crecimiento, representan nuevos desafíos y oportunidades para la diplomacia en el siglo XXI.

En cuanto a las redes sociales, su influencia se extiende más allá de las fronteras nacionales: afectan aspectos sociales, culturales, económicos y políticos de los países y las relaciones internacionales. Aunque pueden servir como herramientas para promover la democracia, los derechos humanos y la paz, también presentan dificultades como la desinformación y la consolidación de poder por parte de grupos de interés.

La confianza es fundamental en las relaciones internacionales y la diplomacia multilateral funciona como un mecanismo determinante para garantizar la paz. Sin embargo, la brecha digital y la desigualdad social son factores

que pueden generar conflictos y tensiones por lo que es importante abordar estos desafíos mediante la diplomacia y la cooperación internacional.

La promoción de la innovación y la tecnología a través de la techplomacia se centra en el establecimiento de alianzas estratégicas, acuerdos de cooperación y programas conjuntos que fomenten el intercambio de conocimientos, mejores prácticas y recursos entre actores gubernamentales, académicos, empresariales y de la sociedad civil. Esta colaboración internacional puede abordar desafíos globales, como el cambio climático, la salud pública, la ciberseguridad y la inclusión digital, utilizando la tecnología como un catalizador para el desarrollo sostenible y la resiliencia global (Riordan, 2019).

En este sentido, los Estados pueden utilizar la diplomacia tecnológica para facilitar el acceso a recursos financieros, infraestructura, capacidades humanas y tecnológicas, a fin de promover la transferencia de tecnología y conocimiento en sectores prioritarios. Además, la techplomacia puede jugar un papel fundamental en la creación de ecosistemas de innovación robustos y competitivos e incentivar la inversión en investigación y desarrollo, startups tecnológicas y proyectos innovadores que generen empleo, crecimiento económico y soluciones novedosas a desafíos globales.

Por otro lado, la promoción de la tecnología a través de la diplomacia implica un enfoque proactivo en la formulación de políticas públicas, regulaciones y marcos normativos que faciliten la colaboración internacional, protejan los derechos de propiedad intelectual, promuevan la ética en la inteligencia artificial y garanticen un ciberespacio seguro, abierto y democrático. Además, es fundamental fortalecer la educación, la formación técnica y las capacidades digitales con el objeto de asegurar que los países y las regiones estén preparados para aprovechar las oportunidades y enfrentar los desafíos de la era digital.

Usos y regulaciones de monedas digitales y de criptomonedas

En el ámbito emergente de la ciberdiplomacia, las monedas digitales y las criptomonedas representan un fenómeno disruptivo que plantea desafíos

y oportunidades significativos para la gobernanza global y las relaciones internacionales. Sumado a ello, desde una perspectiva diplomática, estas tecnologías financieras descentralizadas han generado un nuevo conjunto de consideraciones en términos de seguridad cibernética, soberanía económica y cooperación internacional. Este surgimiento presenta implicaciones geopolíticas y desafía el dominio del dólar estadounidense como moneda de reserva, lo que ha llevado a discusiones sobre cómo las empresas tecnológicas y los Gobiernos pueden colaborar para abordar estos retos.

En primer lugar, las criptomonedas y las monedas digitales de bancos centrales (CBDC, por sus siglas en inglés) están reconfigurando el paisaje económico y geopolítico lo que requiere una respuesta diplomática coordinada (SELA, 2023c). La naturaleza transfronteriza y descentralizada de estas monedas desafía los marcos regulatorios convencionales y plantea preguntas fundamentales sobre la atribución de responsabilidades y la jurisdicción en el ciberespacio, contexto en el que la ciberdiplomacia se convierte en un mecanismo crucial para facilitar el diálogo internacional, promover la cooperación regulatoria y mitigar los riesgos asociados con el uso ilícito de criptomonedas.

En segundo lugar, la ciberdiplomacia también juega un papel vital en la promoción de usos legítimos y beneficiosos de las monedas digitales para el desarrollo económico y la inclusión financiera. A medida que los Estados exploran la implementación de las CBDC y de regulaciones específicas para criptomonedas, es fundamental que exista un marco que facilite la colaboración internacional lo que podría incluir la creación de normas y estándares internacionales, el intercambio de mejores prácticas y la construcción de alianzas estratégicas para abordar desafíos comunes, como el lavado de dinero, la evasión fiscal y la financiación del terrorismo.

También puede desempeñar un papel crucial en la mitigación de tensiones geopolíticas relacionadas con el uso y la regulación de monedas digitales. Dado que las criptomonedas pueden utilizarse como herramientas para evadir sanciones internacionales y eludir controles financieros, es esencial que los Estados trabajen conjuntamente a fin de desarrollar un enfoque diplomático coherente y efectivo. Esto podría implicar la coordinación en

foros multilaterales, como el G20, el FMI y las Naciones Unidas, así como el establecimiento de canales de comunicación directa entre actores clave en el espacio cibernético y financiero.

Por último, pero no menos importante, vale la pena mencionar el crecimiento de empresas que ofrecen un sinfín de servicios y productos financieros digitales. Las *fintech*, como se las denomina, desempeñan un papel transformador en el sector financiero global: introducen innovaciones que van desde pagos móviles hasta plataformas peer-to-peer. El crecimiento de estas empresas plantea desafíos y oportunidades únicas que requieren una respuesta diplomática adaptada, entre las que se destaca, en primer lugar, la ciberdiplomacia como facilitadora del diálogo entre reguladores y empresas *fintech* con el objeto de desarrollar marcos regulatorios equilibrados y promover la innovación mientras se mitigan riesgos para la ciberseguridad y la protección del consumidor. En segundo lugar, la cooperación internacional en cuanto factor esencial para abordar desafíos transfronterizos, como la ciberseguridad y el cumplimiento de regulaciones financieras, mediante el fomento de normas y estándares internacionales que promuevan un ecosistema fintech seguro y transparente. En última instancia, las fintech tienen el potencial de impulsar la inclusión financiera y el desarrollo económico, y la ciberdiplomacia puede desempeñar un papel vital en la promoción de políticas y estrategias colaborativas que faciliten el acceso a servicios financieros y propicien un crecimiento económico sostenible e inclusivo a nivel global.

Desafíos en la gobernanza de la economía digital a nivel regional

La gobernanza de la economía digital a nivel regional presenta una serie de desafíos complejos que requieren respuestas coordinadas y estratégicas por parte de los actores gubernamentales, empresariales y civiles (SELA, 2021). En un mundo cada vez más interconectado, donde las fronteras digitales son fluidas, pero los marcos regulatorios son inherentemente nacionales o regionales, surgen tensiones significativas que afectan tanto la competitividad económica como la cohesión social.

Uno de los desafíos más apremiantes es la disparidad en la adopción y regulación de tecnologías emergentes entre los países y las regiones. Mientras que

algunas economías regionales pueden estar a la vanguardia en áreas como la IA, el IoT y la blockchain, otras pueden quedarse rezagadas debido a limitaciones infraestructurales, regulatorias o económicas. Esta brecha digital no solo afecta la competitividad económica, sino que también puede exacerbar las desigualdades sociales y económicas dentro de los países y entre ellos.

Es necesario considerar también la protección de datos y la privacidad como áreas críticas que plantean desafíos significativos en la gobernanza regional de la economía digital, ya que, con la proliferación de plataformas en línea, servicios basados en datos y tecnologías de seguimiento, es fundamental establecer marcos regulatorios robustos que protejan los derechos individuales mientras se fomenta la innovación y la competitividad. Como se ha mencionado, los algoritmos, el big data y el análisis de datos personales implican una cuestión importante para las empresas que tienen negocios en la red y podrían ser regulados (Riordan, 2019). Sin embargo, la diversidad de enfoques regulatorios y culturales en diferentes regiones puede complicar los esfuerzos para desarrollar estándares comunes y mecanismos de cooperación efectivos.

Otro desafío importante se relaciona con la fiscalidad y la regulación de las actividades económicas en línea, dado que la naturaleza transfronteriza de la economía digital plantea problemas significativos en términos de cómo gravar las actividades económicas, regular las prácticas comerciales y proteger los derechos de los consumidores. A medida que las empresas digitales operan en múltiples jurisdicciones con diferentes regímenes fiscales y regulatorios se requiere una mayor cooperación regional e internacional para abordar la erosión fiscal, el lavado de dinero y otras prácticas económicas ilícitas.

Por otro lado, la ciberseguridad y la resiliencia de la infraestructura digital emergen como desafíos críticos que requieren una atención especial en la gobernanza de la región. Con el aumento de los ciberataques, las vulnerabilidades de la infraestructura crítica y las amenazas a la seguridad nacional, es imperativo que los países y regiones colaboren para fortalecer sus capacidades cibernéticas, compartir información y desarrollar mecanismos de respuesta conjunta.

INTELIGENCIA ARTIFICIAL Y DIPLOMACIA

En las últimas décadas, la intersección entre la tecnología y la diplomacia ha dado lugar a transformaciones significativas en la forma en que los Estados y las organizaciones internacionales abordan las relaciones entre países, la cooperación y la resolución de conflictos. En este contexto dinámico, la IA emerge como una herramienta poderosa que está redefiniendo los límites y posibilidades de la diplomacia —y de otras tantas cuestiones— en el siglo XXI. Según la Comisión Europea (2019) especializada en la temática, la IA comprende sistemas creados por humanos que operan con el propósito de alcanzar metas al procesar información, razonar y elegir acciones adecuadas. Es una disciplina que engloba métodos como el aprendizaje automático, la lógica computacional y la robótica y que se adapta a distintos entornos y situaciones. Se caracteriza por su capacidad para analizar grandes volúmenes de datos, automatizar procesos complejos y generar insights o perspectivas predictivas. Además, ofrece oportunidades sin precedentes para mejorar la eficiencia, la precisión y la relevancia de las iniciativas diplomáticas a nivel global.

A lo largo de este capítulo, se da cuenta del impacto y las implicaciones de la IA en el ámbito diplomático y se analizan sus aplicaciones prácticas, desafíos éticos y oportunidades para fortalecer la cooperación internacional. Esta tecnología se utiliza para facilitar el análisis de datos geopolíticos, optimizar la comunicación intercultural, simular escenarios complejos y automatizar tareas administrativas en el contexto diplomático. Por ello, se vuelve necesario examinar los desafíos éticos asociados con su uso, tales como la privacidad de datos, la transparencia algorítmica y el riesgo de sesgos algorítmicos, así como las estrategias para mitigar estos desafíos y promover un uso responsable en la diplomacia.

La IA ofrece grandes beneficios, pero también presenta riesgos de que su utilización tenga fines abusivos. Si bien están llevándose adelante diversas iniciativas por parte de organizaciones de la sociedad civil, empresas y Gobiernos para abordar los desafíos técnicos, éticos y sociales de la IA, la falta de colaboración global puede limitar su potencial positivo. Algunos

autores y actores proponen una nueva diplomacia tecnológica inclusiva que integre múltiples agentes para maximizar los beneficios de la IA (Feijóo et al., 2020; Bulnes e Higueras, 2023).

Diferentes actores internacionales están integrando la IA en su práctica diplomática y analizando lecciones aprendidas, mejores prácticas y áreas de oportunidad para fortalecer la colaboración y la cooperación en un mundo cada vez más interconectado y tecnológicamente avanzado. Las perspectivas de la IA en diplomacia, las innovaciones emergentes, las tendencias tecnológicas y su potencial transformador son insumos para abordar desafíos globales y promover un desarrollo sostenible y equitativo en la comunidad internacional (Muñiz, 2023).

Figura 5

Ecosistema digital

Nota: Adaptado de Cadenas de valor público y ecosistema digital, p. 49, por Campos Ríos, 2023, SELA.

Usos de la IA en la diplomacia

La revolución tecnológica impulsada por la IA ha permeado diversos sectores de la sociedad moderna y la diplomacia no es la excepción. La capacidad de esta tecnología para procesar, analizar y generar *insights*, a partir de grandes volúmenes de datos, ha abierto nuevas oportunidades con el propósito de fortalecer las relaciones internacionales, optimizar la toma de decisiones y abordar desafíos globales de manera más eficiente y efectiva (Muñiz, 2023).

La IA se refiere a la simulación de la inteligencia humana en máquinas o sistemas informáticos, es decir que se trata de una tecnología que permite que las máquinas realicen tareas que normalmente requerirían inteligencia humana como el aprendizaje, la percepción, el razonamiento, la resolución de problemas y la toma de decisiones. El desarrollo formal de la IA como campo de estudio se remonta a mediados del siglo XX, puntualmente, en 1956, cuando se llevó a cabo la Conferencia de Dartmouth, considerada el punto de partida oficial de la IA como disciplina académica (Torres Jarrín, 2021). A partir de entonces, la investigación en IA ha experimentado avances significativos, impulsados por la innovación tecnológica, el desarrollo de algoritmos y el aumento de la capacidad computacional.

En lo que respecta a sus usos, la IA puede impactar en áreas distintas, como la económica, la seguridad, la democracia y los derechos humanos (Bulnes e Higueras, 2023). Entre sus aplicaciones más prominentes se destaca el aprendizaje automático, que permite a las máquinas mejorar su rendimiento en tareas específicas a través de la experiencia. Los algoritmos de aprendizaje automático analizan datos, identifican patrones y aprenden a realizar tareas sin una programación explícita, como la clasificación de imágenes, la predicción de tendencias y la personalización de recomendaciones. El procesamiento del lenguaje natural (NLP, por sus siglas en inglés) es otra área clave de la IA que se centra en la interacción entre las computadoras y el lenguaje humano. Los sistemas de NLP permiten a las máquinas entender, interpretar y generar lenguaje humano de manera efectiva para facilitar aplicaciones como la traducción automática, el reconocimiento de voz y la generación de contenido.

Además, la visión por computadora utiliza algoritmos de IA para permitir que las máquinas procesen, analicen e interpreten imágenes y videos digitales, tecnología fundamental para aplicaciones como el reconocimiento facial, la detección de objetos, la monitorización de sistemas de seguridad y la realidad aumentada. Por su parte, los sistemas expertos son programas de IA diseñados para emular el conocimiento y la experiencia de una persona avezada en un dominio específico y que se sirven de reglas, heurísticas y bases de conocimiento para realizar tareas complejas, resolver problemas y ofrecer recomendaciones en áreas como la medicina, la ingeniería y la gestión empresarial.

La IA también impulsa avances en automatización y robótica, lo que permite el desarrollo de sistemas autónomos capaces de realizar tareas físicas y cognitivas en entornos complejos. Desde vehículos autónomos y drones hasta robots industriales y asistentes domésticos inteligentes, la IA está transformando la manera en que interactuamos con el mundo físico y con el digital.

Ahora bien, en lo que respecta a la diplomacia digital, que, como se ha visto, hace referencia a la utilización de distintas herramientas por parte de diplomáticos, una de las aplicaciones más destacadas de la IA es el análisis de datos (Bulnes e Higueras, 2023). Mediante algoritmos avanzados y técnicas de aprendizaje automático, la IA puede analizar grandes cantidades de información procedente de diversas fuentes, como noticias, informes y redes sociales, capacidad que les permite a los diplomáticos identificar tendencias emergentes, evaluar oportunidades de cooperación y anticipar posibles riesgos geopolíticos. Al procesar datos en tiempo real, la IA facilita la toma de decisiones basada en evidencia y contribuye a la formulación de políticas más informadas y contextualizadas.

En un mundo cada vez más globalizado, la comunicación efectiva entre diplomáticos de diferentes idiomas es esencial para promover el entendimiento mutuo y la cooperación internacional. La IA ha transformado el campo de la traducción automática desarrollando herramientas y plataformas capaces de traducir documentos, discursos y conversaciones en tiempo real, aportando soluciones tecnológicas que facilitan la comunicación inter-

cultural, reducen las barreras lingüísticas y fomentan el diálogo constructivo entre países y organizaciones internacionales.

La IA también ofrece herramientas poderosas para simular escenarios geopolíticos, analizar posibles consecuencias de políticas y facilitar la toma de decisiones informadas en el ámbito diplomático. A través de modelos computacionales y técnicas de simulación, los diplomáticos pueden evaluar el impacto potencial de diferentes acciones, anticipar resultados adversos y diseñar estrategias de mitigación. Estas capacidades de modelado permiten a los actores internacionales navegar en un entorno geopolítico complejo y dinámico, anticiparse a cambios, identificar oportunidades y promover soluciones colaborativas.

Tabla 12

Tabla sobre usos o aplicaciones de la IA en la diplomacia

Tipo de aplicación	Ejemplos de uso en diplomacia
Análisis de datos	Procesamiento de información de noticias e informes para identificar tendencias geopolíticas.
	Evaluación de datos económicos y sociales para informar políticas y estrategias internacionales.
Traducción automática	Traducción instantánea de discursos, documentos y comunicados entre diferentes idiomas en conferencias internacionales.
	Facilitación de la comunicación entre diplomáticos de distintos países y culturas en reuniones bilaterales o multilaterales.
Simulación de escenarios geopolíticos	Modelado y simulación de posibles consecuencias de políticas o decisiones en relaciones internacionales.
	Evaluación de riesgos y oportunidades en escenarios geopolíticos complejos mediante técnicas de modelado y simulación.
Reconocimiento facial	Uso de tecnologías de reconocimiento facial para la identificación de individuos en eventos diplomáticos o zonas seguras.
	Mejora de la seguridad en embajadas y consulados mediante sistemas de reconocimiento facial.
Procesamiento del lenguaje natural (NLP)	Análisis de discursos y comunicados para entender el tono, la intención y las preocupaciones de diferentes actores internacionales.
	Evaluación de la percepción pública y la opinión de los medios de comunicación en diferentes países sobre temas diplomáticos.

Fuente: elaboración propia.

Colaboración internacional y ciberdiplomacia

La colaboración internacional en la regulación de la red y la ciberdiplomacia emergen como pilares fundamentales para promover un orden mundial más cooperativo, inclusivo y resiliente. La rápida evolución de la IA ha reconfigurado la dinámica de las relaciones internacionales y ha ofrecido oportunidades sin precedentes para fortalecer la cooperación diplomática, fomentar el diálogo intercultural y abordar desafíos globales de manera más eficiente y efectiva.

La posibilidad de regular sobre los usos de la IA se presenta, entonces, como un imperativo estratégico para garantizar que las tecnologías emergentes sean utilizadas de manera ética, equitativa y sostenible en el escenario global. Los avances en la materia tienen el potencial de transformar sectores clave, como la salud, la educación, el medio ambiente y la seguridad, pero también plantean desafíos complejos relacionados con la privacidad, la seguridad y los derechos humanos. Por lo tanto, es imperativo que los países, las organizaciones internacionales y demás actores relevantes colaboren en la formulación de políticas, estándares y principios comunes que guíen el desarrollo y la aplicación de la IA de manera responsable.

De hecho, la Unión Europea ha avanzado en una serie de iniciativas para la regulación de la IA (Torres Jarrín, 2021) que los países de América Latina y del Caribe podrían evaluar. En diciembre de 2023, la UE -aprobó la Ley de Inteligencia Artificial, primera de su tipo que establece un marco detallado para supervisar y controlar su implementación y uso, especialmente en lo que respecta a modelos de alto impacto y a la "IA de propósito general", como ChatGPT. Uno de los aspectos más destacados de esta regulación es la exigencia de transparencia y responsabilidad por parte de las empresas desarrolladoras de esta tecnología, mientras que, para los modelos de IA con potencial impacto sistémico, se imponen requisitos más estrictos, que incluyen evaluaciones de riesgos, pruebas constantes y garantías de ciberseguridad. Esto asegura que las tecnologías de IA se utilicen de manera ética y responsable a fin de minimizar posibles amenazas a los derechos fundamentales y a la privacidad de los individuos.

La legislación también prohíbe activamente el uso de sistemas de IA que puedan comprometer los valores y derechos fundamentales de la UE, como sistemas de puntuación social, reconocimiento de emociones invasivo y vigilancia biométrica en espacios públicos sin salvaguardias adecuadas. Estas medidas reflejan el compromiso de la UE de proteger la privacidad, la libertad y la dignidad de sus ciudadanos en un mundo cada vez más digitalizado, por lo que, para garantizar el cumplimiento de estas regulaciones, se establecerá una Oficina de IA dentro de la Comisión Europea, encargada de supervisar, asesorar y aplicar las normativas. Además, se han establecido sanciones significativas para las empresas que no cumplan con las directrices; así se asegura la responsabilidad y el cumplimiento.

En este contexto, la ciberdiplomacia no solo se ha convertido en un campo emergente que utiliza herramientas digitales y plataformas en línea para facilitar el diálogo, la negociación y la resolución de conflictos entre Estados y actores no estatales, sino que también permite la discusión sobre la gobernanza de internet. La IA ofrece capacidades avanzadas para analizar datos, identificar patrones y generar perspectivas que pueden informar decisiones diplomáticas, facilitar la mediación de disputas y promover la construcción de consensos en temas de interés común. Las plataformas de diplomacia digital impulsadas por la IA, como los sistemas de análisis de tendencias geopolíticas, los simuladores de negociación y las herramientas de traducción automática, pueden ser utilizadas para mejorar la comunicación, reducir malentendidos y favorecer la cooperación dentro del comercio, la seguridad cibernética y la gobernanza de internet, entre otras áreas.

Sin embargo, es importante reconocer que la ciberdiplomacia y el uso de la IA en el ámbito internacional también presentan desafíos relacionados con la seguridad cibernética, la soberanía digital y la desigualdad tecnológica. La dependencia de plataformas digitales y algoritmos sofisticados puede generar vulnerabilidades, tensiones geopolíticas y brechas digitales que requieren una atención cuidadosa y coordinada entre los Estados. Además, la diversidad de enfoques, intereses y capacidades en el ámbito de la IA posiblemente cree desequilibrios de poder, inequidades y tensiones en la cooperación internacional, donde se destaca la necesidad de

promover un enfoque inclusivo, transparente y participativo en la gobernanza de la IA a nivel global.

La cooperación internacional y la ciberdiplomacia en la era de la IA ofrecen oportunidades significativas para fortalecer las relaciones diplomáticas, promover la paz y la seguridad internacionales, y abordar desafíos globales de manera colectiva, ya que "no se puede querer regular la IA sin regular el ciberespacio. La ciberdiplomacia como aplicación de la diplomacia a los problemas que se crean por causa de las tecnologías que surgen en el ciberespacio" (Torres Jarrín, 2021, p. 229). A través del diálogo constructivo, la colaboración estratégica y el compromiso ético, los Estados y los actores relevantes pueden aprovechar el potencial transformador de la IA para construir un orden mundial más justo, equitativo y sostenible, respetando los valores, derechos y principios fundamentales en la comunidad internacional del siglo XXI. Este esfuerzo no solo debe implicar la profundización del camino de convergencia de los países que componen ALC, sino que también debe tener en cuenta otros actores importantes, como los países de la Unión Europea, los Estados Unidos y China.

Desafíos y debates sobre sus usos

La integración de la IA en el ámbito de la diplomacia representa un avance tecnológico con potencial transformador, pero también conlleva desafíos éticos que demandan una cuidadosa reflexión y regulación. Una de las principales preocupaciones, que, como se ha visto, se repite en distintas cuestiones relacionadas con los usos de plataformas y redes, radica en la privacidad de datos, dado que la recopilación y el análisis de información sensible puede exponer a individuos y entidades a riesgos de vigilancia, discriminación y violaciones de la privacidad. Es imperativo establecer salvaguardias rigurosas que protejan la integridad y confidencialidad de los datos, y garanticen un equilibrio entre la seguridad y el respeto por los derechos fundamentales.

Por otra parte, la transparencia algorítmica emerge como un imperativo ético en el uso de IA en diplomacia. La opacidad en los procesos algorít-

micos puede generar desconfianza y suscitar interrogantes sobre la objetividad, la equidad y la responsabilidad en la toma de decisiones informadas por tecnologías de IA. Por tanto, promover un mayor nivel de transparencia que permita comprender y cuestionar los criterios y resultados de los sistemas algorítmicos se convierte en una necesidad para fortalecer la confianza pública y la legitimidad de las acciones diplomáticas.

Otro aspecto crítico que considerar es el riesgo de sesgos algorítmicos que pueden perpetuar o amplificar prejuicios y discriminaciones existentes en los datos y algoritmos utilizados. Como ya se ha mencionado, estos algoritmos pueden generar en las redes filtros burbuja o cámaras de eco que se repetirán en el uso de esta herramienta. La incorporación inadvertida de sesgos en modelos de IA puede influir en la percepción, la interpretación y la respuesta a situaciones internacionales, con lo cual se compromete la equidad, la objetividad y la eficacia de las iniciativas diplomáticas. Por lo tanto, es esencial realizar evaluaciones éticas y técnicas exhaustivas que identifiquen y mitiguen posibles sesgos a fin de asegurar que las decisiones informadas por la IA reflejen valores universales y principios democráticos.

Con el propósito de abordar estos desafíos éticos, es fundamental adoptar un enfoque integrado que combine marcos regulatorios robustos, una formación especializada en ética de la IA para diplomáticos y evaluaciones de impacto ético rigurosas. Estos mecanismos permitirán establecer directrices claras, capacitar a los actores relevantes y garantizar la implementación responsable de la IA en el ámbito diplomático, con prioridad en el bienestar humano, la justicia social y la cooperación internacional. Asimismo, es muy necesario promover el diálogo interdisciplinario, la colaboración entre países y la participación pública en la elaboración y aplicación de políticas de IA éticas, con el objeto de garantizar que las decisiones tecnológicas manifiesten valores compartidos, intereses comunes y aspiraciones colectivas en la comunidad global.

Perspectivas futuras

La intersección entre IA y diplomacia representa un paradigma en constante evolución que redefine el panorama internacional. Si bien la IA ha

permeado el ámbito diplomático, optimizando procesos, facilitando el diálogo intercultural y ofreciendo herramientas avanzadas para la toma de decisiones informadas, este avance tecnológico no está exento de desafíos éticos, técnicos y geopolíticos que requieren una atención meticulosa y una colaboración internacional estratégica.

Es evidente que la IA ha revolucionado la forma en que los diplomáticos analizan datos, comunican ideas y anticipan escenarios geopolíticos, y tiene aún mucho potencial para seguir haciéndolo. Su capacidad para procesar grandes volúmenes de información en tiempo real ha fortalecido la eficiencia y la eficacia de las iniciativas diplomáticas por cuanto promueve una cooperación más estrecha y una comprensión mutua entre los actores internacionales. Sin embargo, este progreso tecnológico viene acompañado de desafíos éticos significativos, como la privacidad de los datos, la transparencia de los algoritmos utilizados y el riesgo de sesgos discriminatorios, que requieren una regulación adecuada y un compromiso ético para garantizar un uso responsable de la IA en el escenario global.

En este sentido, es muy recomendable que los países, las organizaciones internacionales y otros actores relevantes colaboren activamente en la formulación de políticas, estándares y principios comunes que guíen el desarrollo y la aplicación de la IA de manera ética, inclusiva y sostenible. La implementación de marcos regulatorios robustos, la formación especializada en ética de la IA para diplomáticos y la realización de evaluaciones de impacto ético son pasos esenciales a fin de mitigar riesgos, promover la transparencia y garantizar que esta tecnología contribuya a construir un orden mundial más justo y equitativo.

Es fundamental también reconocer que la ciberdiplomacia y la colaboración internacional en la era de la IA requieren un enfoque multidimensional que integre la tecnología, la ética y la geopolítica. La promoción de un diálogo interdisciplinario, la participación pública y la cooperación estratégica son elementos clave para abordar desafíos complejos, como la seguridad cibernética, la soberanía en el mundo digital y la desigualdad tecnológica que pueden influir en la efectividad y la legitimidad de las iniciativas diplomáticas impulsadas por la IA.

Se puede anticipar que la IA continuará evolucionando y transformando el paisaje diplomático en los próximos años. La adopción de tecnologías emergentes, como el aprendizaje automático avanzado, el NLP y la visión por computadora, ofrecerá nuevas oportunidades para mejorar la comunicación, optimizar la toma de decisiones y brindar soluciones innovadoras a desafíos globales. Sin embargo, es imperativo mantener un enfoque centrado en el ser humano que priorice valores éticos, derechos fundamentales y principios democráticos en la implementación y regulación de la IA en el ámbito internacional.

La integración de la inteligencia artificial en la diplomacia representa un viaje hacia un futuro tecnológico prometedor, pero también plantea interrogantes y responsabilidades compartidas que requieren una reflexión profunda, una colaboración estratégica y un compromiso ético. Al enfrentar estos desafíos con firmeza, perspectiva y cooperación, la comunidad internacional puede aprovechar el potencial transformador de la IA con el propósito de construir un orden mundial más resiliente, inclusivo y sostenible en el siglo XXI que garantice que la tecnología sirva como una herramienta para promover la paz, la cooperación y el desarrollo humano integral en la comunidad global.

Embajador Clarems Endara Vera

Secretario Permanente del Sistema Económico Latinoamericano y del Caribe (SELA)

LA CIBERDIPLOMACIA Y EL DERECHO INTERNACIONAL

En lo que autores como Castells (2009) denominan la "era de la información", la ciberdiplomacia ha transformado las relaciones internacionales, pues utiliza plataformas digitales y aborda desafíos relacionados con la seguridad cibernética y la desinformación. Los términos "ciberdiplomacia", "diplomacia digital" e "e diplomacia" se entrelazan y se centran en las TIC, en las redes sociales y en aspectos más amplios, respectivamente, por lo que, a nivel regional, representan desafíos que incluyen brechas digitales y falta de normativas cohesivas. A su vez, se busca una colaboración multisecto-

rial para alcanzar soluciones innovadoras, además de que también resulta necesaria la cooperación regional en ciberseguridad ante amenazas compartidas. Por otro lado, la techplomacia emerge como medio para manejar las relaciones entre Estados y big tech companies, aunque requiere colaboración y regulación efectiva. En este contexto y ante todas estas cuestiones particulares, organismos como el SELA desempeñan un papel crucial en la promoción de la convergencia regional y el desarrollo sostenible.

Uno de los deberes de los Estados es resguardar los derechos de su población, entre ellos, el derecho a la privacidad el cual ha sido y es vulnerado de manera constante con el uso de las redes sociales, e inclusive mediante la influencia en los mercados.

La protección de los derechos humanos en el ciberespacio es imperativa, especialmente en temas de privacidad y libertad de expresión. Se ha enfatizado la necesidad de políticas públicas adaptativas y de cooperación regional para fortalecer la ciberdiplomacia y promover el bienestar colectivo en los países de la región. Ahora bien, también es imperativo comprender la intersección con el derecho internacional y adentrarse en ella al explorar algunas de las normas y acuerdos que buscan guiar el comportamiento de los Estados en el ciberespacio.

Al traer a la discusión el derecho internacional, se busca no solo reflexionar sobre el estado actual de la ciberdiplomacia en la región, sino también proyectar luces sobre los desafíos y las perspectivas. A medida que la tecnología avanza y la interconexión se profundiza, la interacción entre ciberdiplomacia y derecho internacional se vuelve cada vez más vital para forjar un camino hacia un futuro digital sostenible y seguro en ALC.

Desarrollo de normas y acuerdos internacionales en el ámbito cibernético

La ciberdiplomacia puede ser entendida como la cooperación internacional de los asuntos cibernéticos (Vega, 2023) y, bajo esta óptica, la diplomacia cibernética comprende el abordaje securitario de la problemática (cooperación en el ámbito de la ciberseguridad) como las iniciativas interestatales asociadas a la incorporación colaborativa de las tecnologías de la información y la comunicación en la economía.

La creciente interconexión global y la omnipresencia de la tecnología en todos los aspectos de la sociedad han impulsado la necesidad de establecer normas y acuerdos internacionales en el ámbito cibernético. Como explica Domínguez Bascoy (2014), en el ciberespacio existe consenso sobre la aplicabilidad de principios y normas preexistentes del derecho internacional, especialmente en relación con el uso de la fuerza y las ciberhostilidades durante conflictos armados. Sin embargo, la ausencia de reglas ad hoc no implica que los Estados puedan llevar a cabo ciberoperaciones sin restricciones, por lo que la regulación del ciberespacio busca asegurar que no sea una zona inmune al derecho y, sobre todo, al derecho internacional, aunque persiste la ausencia de una rama específica para el ciberespacio. La necesidad de adaptar normas existentes y el acuerdo sobre una interpretación amplia emergen como estrategias clave para abordar las complejidades legales en este ámbito (Domínguez Bascoy, 2014).

En este contexto, organismos internacionales como las Naciones Unidas y la OEA han liderado iniciativas para desarrollar principios que guíen el comportamiento de los Estados en el ciberespacio y que, a la vez, se fortalezcan las capacidades estatales, dado que solo así pueden generarse respuestas diplomáticas conjuntas.

Las respuestas diplomáticas concertadas o conjuntas en materia de ciberseguridad muestran un alto grado de asimetrías y enfoques, ya sean de carácter regional o interno, estas últimas, muy incipientes en la región, en comparación con el Viejo Mundo.

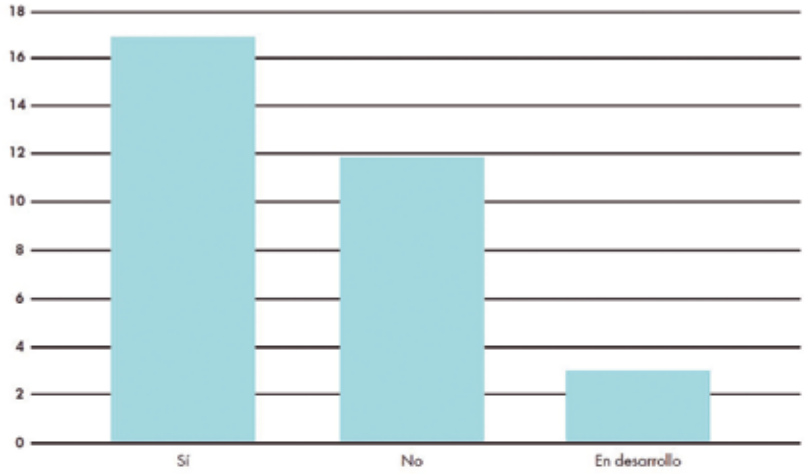
Las agendas en ciberseguridad de carácter nacional, regional y multilateral deberían tener como columna vertebral la cooperación interestatal, por la naturaleza transnacional de los riesgos y amenazas que se desarrollan en un área donde la normatividad es escasa, como es el ciberespacio. Esto requiere de amplios esfuerzos, pues inclusive la sola acción estatal es insuficiente. Por lo tanto, ampliar el espectro de colaboración transnacional precisa también de alianzas con organismos estatales y con los actores privados del ciberespacio, estos últimos, grandes actores en la gobernanza del ámbito digital.

La participación de los países latinoamericanos y caribeños en estos esfuerzos es fundamental para garantizar que las normas sean adaptadas a

las realidades regionales. A medida que se adentran en este proceso, surge la pregunta de cómo estos países han abordado tales iniciativas y qué tan proactivos han sido en la creación de estándares cibernéticos. Si bien existen proyectos de otras regiones, como en la Unión Europea, se hace necesario tener en cuenta las particularidades de los países de nuestras latitudes para llevar a cabo propuestas acordes. En términos generales, la respuesta de la región a los esfuerzos internacionales para establecer normas cibernéticas ha sido diversa: algunos países han adoptado un enfoque proactivo, participando activamente en la formulación de estándares y contribuyendo con sus perspectivas únicas, mientras que otros han optado por un enfoque más reactivo, ajustándose a las normas propuestas por los organismos internacionales. De acuerdo con los datos del Observatorio de la Ciberseguridad en América Latina y el Caribe (2020), 17 de los 33 países de la región (51,51 %) cuentan con una estrategia nacional sobre ciberseguridad y, en los restantes, en su mayoría, existe algún programa o interés sobre el tema.

Figura 6

Países de la región con una estrategia nacional sobre ciberseguridad



Nota: Elaboración propia con base en datos de Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe, por el Observatorio de la Ciberseguridad en América Latina y el Caribe, 2020, BID y OEA. Disponible en: https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

La aplicación de estas normas a las realidades regionales implica considerar diversos factores, desde el acceso a la digitalización, la diversidad cultural y económica, hasta las diferencias políticas. La capacidad técnica de los países, la coordinación efectiva entre ellos y la adaptación de los estándares a las realidades socioeconómicas particulares son elementos críticos en este proceso. La región enfrenta desafíos específicos en dicha transición, desde la brecha digital hasta la falta de capacidades técnicas especializadas. Sin embargo, también se presentan oportunidades, como la mejora de la seguridad cibernética, el fomento de la colaboración regional e, incluso, la posibilidad de facilitar la integración digital en ALC.

De cara al futuro, es esencial considerar las tendencias emergentes en el desarrollo de normas cibernéticas internacionales, oportunidades que la región puede aprovechar para fortalecer su posición estratégica en el ciberespacio a través de la propuesta de recomendaciones para abordar los desafíos y aprovechar al máximo las iniciativas globales, a fin de consolidar la posición del continente en este ámbito fundamental. Es necesario que la región desarrolle un papel activo en la creación de normas y acuerdos internacionales en el ciberespacio, subrayándose, además, la importancia de adaptar estas iniciativas a las realidades de ALC.

Sin embargo, es bueno resaltar lo avanzado y proyectar la capacidad colaborativa a fin de disminuir las asimetrías en cuanto a políticas nacionales y un enfoque necesario de la región. En el plano regional, es importante destacar los esfuerzos de la OEA, con una perspectiva de emergencia al considerar al ciberterrorismo como una amenaza. Ha logrado establecer como parte de su agenda la *Estrategia de Seguridad Cibernética* y ha delineado operativamente el *Programa de Seguridad Cibernética* con el propósito de ayudar a los países en desarrollo a mejorar sus capacidades técnicas y la formulación de sus políticas públicas al respecto. Bajo esta iniciativa y de manera colaborativa, también pudo establecerse el Observatorio de la Ciberseguridad en América Latina y el Caribe, sustentado metodológicamente en el *Modelo de Madurez de la Capacidad de Ciberseguridad*, que permite monitorizar el avance de los países en la región.

En el marco de la CELAC y sus características propias como organismo de diálogo político regional, también se logró su inclusión en las declaraciones presidenciales.

Con relación al Mercosur, a través del Grupo del Mercado Común, pudo establecerse el Grupo de Agenda Digital a fin de coordinar temas relativos a la economía digital de la subregión y abordar también temas como la confianza en el entorno en línea.

En la Declaración Especial sobre Ciberdelincuencia, realizada durante la LXI Cumbre de Presidentes del Mercosur del 6 de diciembre de 2022, se lee lo que sigue:

> … manifestaron su preocupación por el aumento de la tasa y la diversidad de los delitos cometidos en el mundo digital y en los riesgos por ello creados para la estabilidad de la infraestructura esencial de los Estados y las empresas y al bienestar de las personas.

Al mismo tiempo, destacaron lo siguiente:

> … la necesidad de mejorar la coordinación y la cooperación entre los Estados en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, entre otros medios prestando asistencia técnica entre los países para mejorar su legislación y sus marcos nacionales y reforzar la capacidad de sus autoridades nacionales para hacer frente al fenómeno de la ciberdelincuencia en todas sus formas, inclusive mediante la prevención, detección, investigación y enjuiciamiento. (Mercosur, 2022, p. 1)

Los países de la Alianza del Pacífico crearon el Grupo de Agenda Digital (GAD), el cual se guía a través de la *Hoja de Ruta del Mercado Digital Regional*, que pretende promover la seguridad de la información de los consumidores, la cooperación técnica y la adhesión al Convenio de Budapest. Además, tiene como objetivo fomentar escenarios de coordinación y convergencia entre los cuatro países que lo componen con el fin de mejorar las condiciones y el desarrollo de los negocios de la economía digital. Actualmente, el Grupo trabaja en el desarrollo de actividades específicas

basadas en cuatro pilares o ejes: economía digital, conectividad digital, Gobierno y ecosistema digitales.

En el marco del SICA, *SICA Digital* es una iniciativa estratégica promovida por la Secretaría General del organismo, orientada a mejorar la forma en que se opera y se genera valor para la población centroamericana. Su función es integrar la tecnología digital en todas las áreas funcionales del SICA y está conformado por diversos componentes que responden estratégicamente a las necesidades más apremiantes en el ente, a saber: coordinación, acuerdos, firma electrónica, cooperación regional, cooperación administrativa financiera y visibilidad.

Otros procesos de integración y otros organismos incluyen la temática en sus agendas, pero, al no emitir normas, solo son consideradas como recomendaciones de políticas públicas regionales. De todas formas, en ningún caso se logró que tuvieran un alcance regional, además de que la fuente de aquellas también apunta a objetivos diversos, aunque, generalmente, transcurren entre temas de seguridad y de facilitación del comercio.

Intersección entre el derecho internacional humanitario y la ciberdiplomacia

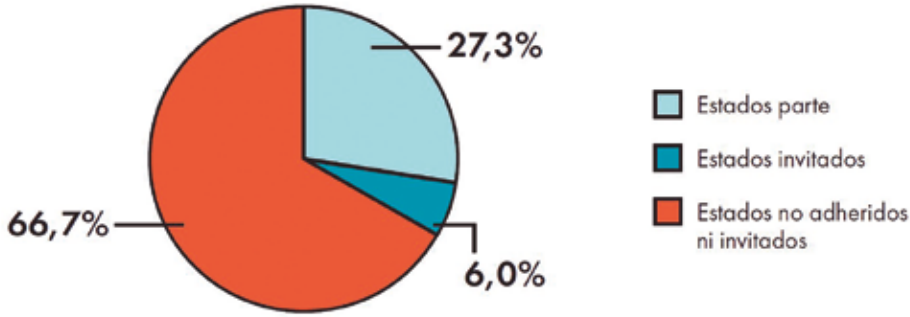
El avance vertiginoso de la ciberdiplomacia ha planteado interrogantes significativos sobre la relación entre este nuevo campo y el marco establecido por el derecho internacional. En la intersección entre ambos, emergen tensiones y continuidades que requieren un análisis detallado para comprender cómo estas dinámicas impactan en la toma de decisiones y en las relaciones entre Estados en el ámbito digital. Al ser una disciplina relativamente nueva, la ciberdiplomacia a menudo enfrenta tensiones con el derecho internacional existente ya que la falta de normas claras y consensuadas en el ciberespacio genera desafíos en la aplicación coherente de los principios legales. Las cuestiones de soberanía digital, el uso de armas en el mundo digital y la atribución de ciberataques son áreas donde las tensiones pueden ser especialmente evidentes y más aún cuando se encuentra en la gobernanza del ciberespacio una amplia participación de privados que van

delineando el comportamiento de los gobernantes al pretender enmarcarlas en las normas aplicables.

Como se ha mencionado en el capítulo específico sobre derechos humanos, el derecho internacional en el ciberespacio ha sido objeto de debate y discusión entre expertos y organismos internacionales. Uno de los hitos importantes es el Convenio de Budapest (2004), sobre delitos cibernéticos, que busca establecer un marco legal para combatir infracciones en sistemas y datos informáticos. Aunque este convenio representa un esfuerzo inicial para adaptar el derecho internacional a los desafíos del ciberespacio, su alcance y aplicación varía entre países. De los 33 países que conforman la región de ALC, 9 son parte de la Convención de Budapest (Argentina, Brasil, Chile, Colombia, Costa Rica, República Dominicana, Panamá, Paraguay y Perú); 2 fueron invitados (Guatemala y México) y el resto no ha adherido ni ha sido invitado a hacerlo.

Figura 7

Porcentaje de países de la región adheridos o invitados a la Convención de Budapest



Nota: Elaboración propia con base en los datos presentados en Reporte Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe, por el Observatorio de la Ciberseguridad en América Latina y el Caribe, 2020, BID y OEA.

La aplicación del derecho internacional humanitario en el ciberespacio plantea desafíos y oportunidades, especialmente en lo que respecta a la distinción entre actores estatales y civiles, la proporcionalidad en el uso de la fuerza y la protección de infraestructuras críticas. Las diferencias fundamentales entre el espacio físico y el ciberespacio, como la atribución de ataques cibernéticos y la proliferación de actores no estatales, requieren enfoques innovadores y adaptados para garantizar la seguridad, la estabilidad y la protección de los derechos humanos en línea. Por su parte, el Manual de Tallinn (2013) ofrece orientación sobre cuestiones de ciberseguridad y ciberdefensa, pero omite una considerable porción de ciberactividades. Entre ellas, se encuentran las ciberactividades que se desarrollan por debajo del umbral del "uso de la fuerza", de manera que excluye todo lo relacionado con la cibercriminalidad y demás actividades vinculadas a otras áreas del derecho internacional, como los derechos humanos o el derecho de las telecomunicaciones (Domínguez Bascoy, 2014). Por otro lado, su carácter no vinculante refleja la necesidad de un consenso más amplio en el ámbito internacional.

La atribución precisa de actividades cibernéticas a un Estado o a entidades específicas presenta desafíos y se convierte en un aspecto crucial del derecho internacional, que, en la búsqueda de establecer responsabilidades y consecuencias, se ve afectado por la naturaleza anónima y sofisticada de las operaciones en línea. La falta de mecanismos claros para atribuir responsabilidad puede generar tensiones y obstáculos para la rendición de cuentas.

A pesar de las tensiones, la ciberdiplomacia y el derecho internacional comparten un interés común en la cooperación de las naciones para abordar las amenazas en línea, entre las que se destacan la necesidad de protección de infraestructuras críticas, la prevención de ciberataques y la gestión de crisis digitales que requieren esfuerzos colaborativos entre Estados. En este sentido, la ciberdiplomacia puede actuar como un puente para fortalecer la aplicación colectiva de normas internacionales existentes y fomentar la creación de nuevas reglas para el ciberespacio.

La adaptación del derecho internacional al entorno digital es una necesidad imperiosa. A medida que la ciberdiplomacia moldea las interacciones entre Estados en el ciberespacio se abre la oportunidad de evolucionar y clarificar las normas existentes. La creación de instrumentos legales específicos para el ámbito digital puede reducir tensiones y proporcionar un marco más preciso a fin de abordar los desafíos emergentes..

El derecho internacional público en el ciberespacio

La diplomacia tradicional quedó superada por las nuevas circunstancias que traen, a su vez, nuevas formas de diplomacia por lo que establecer una relación entre Estados y organizaciones internacionales y otros sujetos y actores no estatales denota una alta complejidad. Los caminos hasta ahora recorridos indican que debe buscarse el marco normativo aplicable de acuerdo con la aparición del evento, vale decir que, para tipificar si un acto cibernético se enmarca en el derecho internacional, deben repasarse sus componentes, jurisdicción y efectos.

El derecho internacional influye en la ciberdiplomacia al proporcionar el marco legal para abordar cuestiones relacionadas con el ciberespacio, como ciberataques, ciberespionaje y ciberseguridad. La razón de ello es que la frecuencia y la sofisticación de los ciberataques han convertido la ciberseguridad en una prioridad global ya que, al examinar casos de este tipo de ataques en el ámbito internacional, se revela la magnitud de las amenazas que enfrentan los Estados y las organizaciones en la región. Diversos ciberataques, desde intrusiones en infraestructuras críticas hasta campañas de desinformación o *fake news*, han destacado la complejidad y la diversidad de las amenazas cibernéticas. Estos eventos requieren respuestas legales efectivas para garantizar la seguridad y la integridad de los sistemas en línea, lo cual entraña la aplicación de principios fundamentales. Organismos internacionales y Estados nacionales han trabajado en conjunto para desarrollar normativas y tratados que guíen la persecución de ciberdelincuentes. Estos esfuerzos buscan establecer un marco legal robusto para abordar estos ciberataques de manera coordinada y efectiva.

En el contexto cibernético, la atribución, es decir, la identificación precisa de los perpetradores de ciberataques presenta un desafío importante debido a la naturaleza anónima y en ocasiones sofisticada de estos. La región enfrenta la tarea de desarrollar capacidades técnicas y mecanismos de atribución eficaces para abordar esta dificultad.

La retorsión, o la respuesta proporcional a un ciberataque, es otro principio esencial en el ámbito cibernético. Sin embargo, determinar qué constituye una respuesta proporcional en el ciberespacio plantea interrogantes éticos y legales. Los límites de la retorsión en el ciberespacio son objeto de debate, ya que la respuesta debe ser efectiva sin desencadenar escaladas indeseadas.

La capacidad técnica limitada, la coordinación entre países y la adaptación de los marcos legales a la evolución de las amenazas cibernéticas son factores críticos y las estrategias regionales deben abordar estos desafíos para fortalecer la capacidad de respuesta legal ante los ciberataques. Resulta necesario que estas estrategias contengan recomendaciones destinadas a fortalecer la cooperación internacional y la capacidad de atribución, y que funcionen como insumo para políticas públicas, sumado a que las medidas legales esenciales deben ser identificadas y aplicadas para disuadir y prevenir futuros ciberataques. Es imperativo, entonces, considerar las tendencias emergentes en ciberseguridad y adaptar las respuestas legales en consecuencia, ya que la anticipación y adaptación a nuevas amenazas requerirán ajustes legales y estrategias innovadoras para garantizar una región segura de forma continua.

Si bien la cooperación internacional en ciberseguridad, derivada de la naturaleza transnacional de los riesgos y amenazas informáticos es una dimensión prioritaria de la ciberdiplomacia la aplicación de los principios generales del derecho internacional público en el ciberespacio también incluye **la soberanía territorial, la no intervención y el derecho a la legítima defensa. La soberanía territorial es un principio fundamental del derecho internacional que establece la autoridad exclusiva de un Estado sobre su territorio y en el ciberespacio, principio que se aplica a la jurisdicción y**

el control de las actividades en línea. La ciberdiplomacia, al gestionar las relaciones internacionales en el ciberespacio incluye el respeto a la soberanía de los Estados en este ámbito. Entre los retos que se le presentan, se encuentran, por ejemplo, las operaciones militares cibernéticas que desafían la noción tradicional de soberanía y jurisdicción, lo que requiere la adaptación de las normas internacionales existentes a este entorno.

En la práctica, la ciberdiplomacia se apoya en normas nucleares globales y en el derecho internacional para fomentar la capacidad y la seguridad en línea. La aplicación del derecho internacional al ciberespacio es un tema en evolución, ya que los Estados buscan establecer un marco jurídico que se adecúe a la relevancia creciente en ese medio.

La aplicación de los principios generales del derecho internacional público en el ciberespacio es esencial para regular las actividades que allí se realizan, proporcionar el andamiaje legal necesario para la diplomacia y abordar las complejidades y los desafíos que surgen en el ámbito digital, un aspecto fundamental en la ciberdiplomacia. Es por ello por lo que la evolución de este campo requiere la adaptación de los principios del derecho internacional a las nuevas realidades.

Mirando hacia el futuro

La ciberdiplomacia a menudo enfrenta tensiones con el derecho internacional existente, ya que la falta de normas claras y consensuadas en el ciberespacio genera desafíos en la aplicación coherente de los principios del derecho internacional. **Las cuestiones de soberanía digital, el uso de armas en este ámbito y la atribución de ciberataques son áreas en las que las tensiones pueden ser especialmente evidentes**.

La aplicación del derecho internacional humanitario en el ciberespacio exhibe desafíos y oportunidades, especialmente en lo que respecta a la distinción entre actores estatales y civiles, la proporcionalidad en el uso de la fuerza y la protección de infraestructuras críticas. Sin embargo, las diferencias fundamentales entre el espacio físico y el ciberespacio, como

la atribución de ataques cibernéticos y la proliferación de actores no estatales que llevan a cabo algunos de estos ataques, requieren enfoques que se adapten para garantizar la seguridad, la estabilidad y la protección de los derechos en la web.

A pesar de las tensiones, la ciberdiplomacia y el derecho internacional comparten un interés común en la cooperación internacional para abordar estos desafíos. La protección de infraestructuras críticas, la prevención de ciberataques y la gestión de crisis digitales requieren esfuerzos colaborativos entre Estados, y entre estos y los organismos internacionales interesados en el tema. En este sentido, la ciberdiplomacia puede actuar como un puente para fortalecer la aplicación colectiva de normas internacionales existentes y fomentar la creación de nuevas reglas. La adaptación del derecho internacional al entorno digital es una necesidad: a medida que la ciberdiplomacia moldea las interacciones entre Estados y actores de la sociedad civil en el ciberespacio, se abre la oportunidad de evolucionar y clarificar las normas existentes. Tanto es así que la creación de instrumentos legales específicos para el ámbito digital puede reducir tensiones y proporcionar un marco más preciso para abordar los desafíos emergentes. La ciberdiplomacia, al involucrar la negociación y la construcción de consensos, puede contribuir al desarrollo de normas compartidas, así como el establecimiento de acuerdos y tratados específicos para el ciberespacio puede proporcionar un marco más claro y detallado para abordar las cuestiones legales y diplomáticas que surgen en este entorno.

La participación de organismos internacionales como el SELA es esencial para gestionar las tensiones existentes ya que facilitan el diálogo, promueven la creación de políticas públicas regionales que podrían convertirse en normas y actúan como mediadores en conflictos cibernéticos lo que contribuye a la construcción de un marco más armonizado y efectivo. La ciberdiplomacia y el derecho internacional deben trabajar en conjunto para garantizar un futuro digital seguro y sostenible en ALC.

En particular, en el ámbito de ALC, debe tenerse conciencia de que el uso de la ciberdiplomacia va más allá de la expansión de las redes diplomáticas

en la esfera digital. Debe ser abordada como una política de Estado con definición de actores, objetivos y metas a corto y largo plazo. De allí la relevancia de desarrollar habilidades para aplicar el uso de las herramientas digitales con fines diplomáticos y actuar en la prevención, abordaje y solución de problemas que tienen lugar dentro del ciberespacio.

Las discusiones en la región aún no han trascendido el área de los intereses económicos, como la facilitación del comercio. Por ello, se requiere apalancar debates profundos desde los principales mecanismos de diálogo político y de integración de la región para generar una mayor capacidad institucional en los Gobiernos e incluir a la sociedad civil en las deliberaciones acerca del ejercicio pleno de la ciberseguridad regional.

POLÍTICAS PÚBLICAS PARA LA CIBERDIPLOMACIA

El presente capítulo contiene sugerencias de políticas públicas en ciberdiplomacia con un enfoque particular centrado en ALC. A través de un análisis de las tendencias globales, los desafíos regionales y las oportunidades emergentes, se proponen recomendaciones para fortalecer la posición de la región en el ámbito cibernético.

Se abordan temas clave como la gobernanza de internet, la protección de infraestructuras críticas, la gestión de incidentes cibernéticos, la diplomacia digital y la cooperación internacional en ciberseguridad. Cada uno de estos aspectos es examinado desde una perspectiva multidimensional considerando las implicancias políticas, económicas, sociales y tecnológicas en el desarrollo e implementación de políticas públicas efectivas. El objetivo es proporcionar a los tomadores de decisiones, académicos, expertos en ciberseguridad y demás actores relevantes una orientación para diseñar e implementar políticas públicas que promuevan la seguridad, la estabilidad y la cooperación en el ciberespacio.

Este capítulo aspira a contribuir al debate regional sobre la ciberdiplomacia y a impulsar la agenda política en ALC, a la vez que reconoce la importancia de adoptar un enfoque colaborativo, inclusivo y orientado hacia el futuro en la construcción de un ciberespacio seguro, abierto y globalmente conectado.

Consideraciones iniciales

La idea de Gobierno puede conceptualizarse como el lugar donde se toman decisiones o como un conjunto temporal de individuos que ocupan roles dentro de la administración estatal, encargados de dictaminar medidas específicas. Las políticas públicas representan justamente esas decisiones y acciones adoptadas por los Gobiernos para enfrentar retos, demandas o urgencias de una comunidad. Es decir, abarcan tanto lo que las naciones optan por ejecutar como lo que optan por omitir. Estas medidas pueden tener como objetivo combatir la pobreza, elevar el estándar educativo, pre-

servar el entorno, asegurar la equidad de género, impulsar la salud colectiva y atender múltiples aspectos que moldean el bienestar ciudadano.

Las políticas pueden enfocarse en diversos ámbitos, desde cuestiones económicas y educativas hasta ambientales y sanitarias. En el fondo, se trata de normativas, directrices, iniciativas y proyectos diseñados y puestos en marcha por la administración con el fin de orientar o regular la conducta de ciudadanos, colectivos o entidades. Es crucial reconocer la necesidad de mantener una perspectiva a largo plazo en la continuidad de estas políticas, especialmente ante desafíos regionales significativos, priorizando la estabilidad y las trayectorias históricas (Estévez, 2014).

Por otra parte, estas políticas sirven como herramientas para supervisar y dirigir las acciones y conductas dentro de la sociedad, desde la inspección industrial hasta la defensa del consumidor y la seguridad pública. Determinan, asimismo, la asignación de recursos estatales, tales como fondos para atender las exigencias y prioridades de la colectividad y decidir la financiación y ejecución de proyectos específicos.

Su objetivo fundamental radica en impulsar el bienestar colectivo, aunque no siempre se logre. Idealmente, buscan armonizar intereses diversos y garantizar una distribución equitativa de ventajas y responsabilidades. Asimismo, son fundamentales para el ejercicio democrático porque facilitan la participación ciudadana mediante mecanismos como elecciones y sondeos públicos y su estabilidad y duración son centrales. Se habla de políticas de Estado cuando perduran en el tiempo (Estévez, 2014).

Adicionalmente, las políticas públicas deben propiciar la creatividad y el crecimiento económico al establecer condiciones favorables para inversiones, investigaciones y emprendimientos, razón vital para que promuevan la competitividad y el desarrollo económico sostenible. Estas políticas desempeñan una función clave en la anticipación y el manejo de emergencias, como crisis naturales, brotes epidémicos o desafíos económicos, al establecer lineamientos y estrategias a fin de responder eficientemente. En esencia, son pilares para la administración efectiva y para el enfrentamiento de diversos retos sociales.

Estas temáticas problematizadas conforman el núcleo de las políticas públicas (Estévez, 2014), delinean el rol gubernamental en la sociedad y propician el progreso y el bienestar general. Por consiguiente, es imperativo considerar cómo integrar estas cuestiones en la agenda pública, así como su implementación, evaluación y seguimiento, a la vez que es necesario reconocer que a veces, más que resolver completamente problemas iniciales, se crean nuevos desafíos que requieren atención.

Figura 8

Modelo secuencial de políticas públicas

Nota: Elaboración propia con base en los desarrollos de Anderson (1975).

En la era contemporánea, la ciberdiplomacia emerge como una herramienta esencial para la interacción y la cooperación éntrelas naciones. El dinámico paisaje de la tecnología y la comunicación ha transformado las relaciones internacionales las cuales ahora demandan respuestas innovadoras y adaptadas a los desafíos del ciberespacio. En este contexto, ALC, con su rica diversidad cultural, económica y política, enfrenta imperativos regionales específicos que requieren una visión estratégica integrada.

El presente capítulo ofrece un conjunto de sugerencias de políticas públicas diseñadas para promover una ciberdiplomacia efectiva y cohesionada en la región. Estas recomendaciones se fundamentan en principios de colaboración, inclusión, innovación y adaptabilidad, esenciales para construir un espacio digital seguro, equitativo y próspero para todos los países involucrados.

La convergencia regional en ciberdiplomacia no es solo una aspiración, sino una necesidad imperante para garantizar el desarrollo sostenible, la seguridad y el bienestar de los ciudadanos en el siglo XXI.

Desafíos futuros y posibles escenarios

Con el progreso tecnológico y la creciente interconexión digital, surgen desafíos específicos que demandan una atención estratégica, entre cuyos retos más prominentes se encuentra la seguridad cibernética avanzada. A medida que la región se adentra en la era digital, enfrenta amenazas cibernéticas cada vez más sofisticadas, desde ataques informáticos hasta campañas de desinformación y de fake news, por lo que fortalecer las capacidades de defensa y establecer normativas regionales robustas se vuelve imprescindible para garantizar la integridad de las infraestructuras críticas y la protección de datos sensibles.

La interacción entre gobernanza digital y derechos humanos se convierte en un punto neurálgico y, aunque la innovación tecnológica ofrece oportunidades sin precedentes, también plantea dilemas éticos y prácticos. La región debe encontrar un equilibrio entre impulsar la digitalización y proteger derechos fundamentales, como la privacidad, la libertad de expresión y el acceso a la información, delicada balanza que se vuelve aún más importante en un contexto de creciente interdependencia digital y ciberespionaje. Aunque debe reconocerse que los avances tecnológicos permiten una mayor transparencia por parte de los Gobiernos, es necesario que los Estados se pongan de acuerdo, a través de negociaciones en el marco de la ciberdiplomacia, para establecer regulaciones acordes a la situación.

Otro aspecto esencial radica en la cooperación, tanto a nivel regional como internacional. ALC tiene el desafío de fortalecer mecanismos cooperación en ciberseguridad y ciberdiplomacia, cooperación que no se limita al ámbito regional sino que también implica establecer alianzas estratégicas con actores globales para abordar desafíos transnacionales. Al mismo tiempo, es necesario atender la brecha tecnológica y de habilidades que persiste en la región, situación en la que inversiones en infraestructura digital, investigación y desarrollo, junto con programas de capacitación en ciberseguridad, serán fundamentales para cerrar esta brecha y apalancar un desarrollo inclusivo. Aquí, tanto los Estados como distintas empresas de telecomunicaciones pueden invertir en la ampliación de la conectividad y obtener beneficios.

Teniendo en cuenta lo expuesto, se hace necesario enfatizar la necesidad de una gestión eficiente de datos, y se subraya el papel central de la información en la toma de decisiones informadas y la creación de valor público (Campos Ríos, 2023). Esta perspectiva es fundamental para la ciberdiplomacia en la que la recopilación, el análisis y el uso estratégico de los datos pueden mejorar las relaciones internacionales y la cooperación en el ciberespacio.

En este contexto, las políticas públicas de los Estados latinoamericanos y caribeños podrían centrarse en fortalecer las capacidades de análisis de datos y de la ciberinteligencia, a fin de promover la cooperación regional para enfrentar desafíos comunes en materia de ciberseguridad y diplomacia digital. Esto implicaría el desarrollo de plataformas y mecanismos de cooperación que faciliten el intercambio de información y mejores prácticas entre los países. Así se fortalecería la posición de la región en el escenario internacional.

Además, debe destacarse la importancia de la colaboración entre el sector público y el privado, una vía para impulsar la innovación y la competitividad (Campos Ríos, 2023). En relación con la ciberdiplomacia, esta podría traducirse en alianzas estratégicas entre Gobiernos, empresas de tecnología y organizaciones civiles para desarrollar capacidades avanzadas en áreas como la inteligencia artificial, la seguridad cibernética y la gobernanza de internet.

Por otro lado, al analizar el potencial de otros países que han presentado un favorable desarrollo en el ámbito digital, se pone de relieve la importancia de adoptar modelos exitosos y adaptarlos al contexto latinoamericano y caribeño (Campos Ríos, 2023). Esto implica invertir en infraestructura tecnológica, fortalecer la educación en ciencias de la computación y promover políticas de innovación que fomenten el desarrollo de *startups* y emprendimientos tecnológicos.

Al considerar los desafíos actuales y futuros, como la adaptación a los mundos inmersivos y las tecnologías emergentes (Campos Ríos, 2022), se subraya la necesidad de una visión prospectiva y estratégica en la formulación de políticas de ciberdiplomacia. Esto incluye la preparación para escenarios cambiantes, la anticipación de riesgos y oportunidades y la construcción de una agenda digital regional que refleje los intereses y los valores de ALC en el ámbito internacional.

En cuanto a los posibles escenarios, existe un espectro desde lo optimista hasta lo pesimista. En un escenario optimista, la región podría lograr consolidar una ciberdiplomacia efectiva centrada en el apoyo mutuo, la innovación y la defensa de los derechos, con estructuras de gobernanza digital robustas, lo que impulsaría un desarrollo sostenible en todos los niveles. Sin embargo, en un escenario más pesimista, si no se enfrentan adecuadamente los desafíos, la región podría sumergirse en vulnerabilidades crecientes, tensiones geopolíticas y retrocesos en la colaboración y confianza digitales.

Recomendaciones para la ciberdiplomacia del futuro

En el horizonte de la ciberdiplomacia, ALC se encuentra ante una oportunidad inigualable para consolidar estrategias y prácticas que garanticen una interacción digital segura, transparente y colaborativa entre naciones. Ante el vertiginoso ritmo de transformación tecnológica y las dinámicas geopolíticas en constante evolución, es imperativo diseñar e implementar políticas que se anticipen a los desafíos emergentes y potencien las oportunidades del ciberespacio. En este contexto, se proponen diversas líneas de acción para fortalecer la ciberdiplomacia en la región.

Primero y fundamentalmente, es esencial **promover una cooperación regional robusta**. La unión de esfuerzos entre países latinoamericanos y caribeños permitirá enfrentar de manera más efectiva las amenazas cibernéticas, compartir mejores prácticas y fortalecer capacidades. Establecer plataformas y mecanismos de diálogo constante entre los actores relevantes, como los Gobiernos, el sector privado, la academia y la sociedad civil, facilitará la construcción de una visión cohesiva y consensuada sobre cuestiones cibernéticas.

Para lograr dicho objetivo, una primera acción es fortalecer los mecanismos de diálogo y diplomacia entre los países o regiones involucradas. Establecer cumbres periódicas, reuniones ministeriales y grupos de trabajo especializados puede contribuir significativamente a abordar diferencias, construir confianza y robustecer relaciones bilaterales y multilaterales. Además del ámbito diplomático, es esencial fomentar iniciativas de inte-

gración económica que faciliten la cooperación comercial y la inversión entre los países miembros. La creación de zonas de libre comercio, uniones aduaneras o mercados comunes puede reducir barreras comerciales y promover el intercambio de bienes, servicios y conocimiento. En este contexto, la infraestructura mancomunada también desempeña un papel decisivo ya que desarrollar proyectos regionales de infraestructura no solo mejora la conectividad, sino que también impulsa el desarrollo económico y la integración regional.

Fortalecer las capacidades institucionales de organizaciones regionales y nacionales es fundamental para implementar políticas de cooperación eficaces. Ello implica formar funcionarios públicos, intercambiar mejores prácticas y coordinar esfuerzos en áreas prioritarias. También es importante promover valores democráticos, ya que la defensa del Estado de derecho y de los derechos humanos puede servir como una base sólida para construir confianza mutua y promover una cooperación regional basada en principios compartidos.

Ahora bien, no debe perderse de vista la importancia de involucrar activamente al sector privado, a las organizaciones no gubernamentales y a la sociedad civil en iniciativas de cooperación regional. Su aporte puede proporcionar recursos, conocimientos y experiencias diversificadas que complementen los esfuerzos de los Gobiernos y fortalezcan la colaboración regional en beneficio de todos los involucrados. En conjunto, estas políticas públicas pueden contribuir a construir una cooperación regional robusta, sostenible y beneficiosa para el desarrollo integral de la región.

En segundo lugar, se requiere **fortalecer las capacidades nacionales en ciberseguridad y ciberdiplomacia**. Esto implica invertir en formación especializada, investigación y desarrollo tecnológico, así como en infraestructuras resilientes. Los países deben priorizar la elaboración de políticas públicas que integren la seguridad cibernética en todos los niveles de la administración, desde el diseño hasta la implementación y evaluación de estrategias, haciendo hincapié en el desarrollo de un marco legal y normativo sólido que regule las actividades cibernéticas, proteja los derechos digitales y establezca responsabilidades claras para las entidades públicas y

privadas. Esta base legal proporciona el fundamento necesario para abordar ciberdelitos, proteger infraestructuras críticas y garantizar una respuesta efectiva ante incidentes cibernéticos.

Invertir en programas de capacitación y formación especializados es fundamental para desarrollar una fuerza laboral altamente calificada en áreas de ciberseguridad, ciberinteligencia y ciberdiplomacia. Esta formación especializada permite mantenerse al día con las últimas tendencias, técnicas y mejores prácticas en el ámbito cibernético porque prepara profesionales para enfrentar desafíos emergentes y proteger los intereses nacionales.

En paralelo, la colaboración entre las agencias gubernamentales, el sector privado, la sociedad civil y los organismos internacionales es crucial para compartir información, inteligencia y mejores prácticas. Establecer centros de excelencia y laboratorios de investigación en colaboración con instituciones académicas y tecnológicas puede impulsar la innovación, la investigación aplicada y el desarrollo de soluciones tecnológicas avanzadas en ciberseguridad y ciberdiplomacia.

Adicionalmente, es menester desarrollar estrategias integrales de gestión de riesgos cibernéticos y resiliencia para proteger infraestructuras críticas y sistemas de información clave. Esto implica identificar vulnerabilidades, evaluar riesgos e implementar medidas de protección adecuadas, así como establecer mecanismos de respuesta rápida ante incidentes cibernéticos para minimizar impactos y garantizar la continuidad operativa.

En el ámbito diplomático, resulta indispensable integrar la ciberseguridad en la agenda diplomática nacional e internacional para promover normas colectivas, construir confianza en el ciberespacio y abordar desafíos comunes. Participar activamente en foros internacionales, negociaciones de tratados y acuerdos, y establecer relaciones bilaterales y multilaterales puede fortalecer la posición del país en el escenario cibernético global y garantizar la protección de intereses nacionales.

Promover la toma de conciencia pública, educar a la sociedad civil y a los ciudadanos sobre los riesgos cibernéticos, los derechos digitales y las bue-

nas prácticas en seguridad informática es fundamental para construir una cultura de ciberseguridad y ciberresponsabilidad. **Involucrar a todos los actores relevantes** en iniciativas de sensibilización, educación y participación activa puede crear un entorno seguro, resiliente y confiable en el ciberespacio, ya que protege los intereses nacionales e impulsa la seguridad digital en beneficio de todos.

Otro objetivo clave es el de **fomentar la gobernanza digital inclusiva y participativa**. Garantizar la participación de diversos stakeholders en la formulación de políticas y regulaciones cibernéticas promoverá soluciones más equitativas y adaptadas a las necesidades y realidades regionales, para lo cual es necesario impulsar espacios de diálogo multiactor, consultas públicas y mecanismos de retroalimentación continua. Como se ha mencionado, no debe perderse de vista que la ciberdiplomacia implica la acción conjunta de actores diplomáticos y de otros actores como miembros de organizaciones de la sociedad civil, influencers, empresas, etc.

Es imprescindible, entonces, implementar políticas que garanticen el acceso a internet, a la educación digital y a las plataformas que faciliten la participación ciudadana en la toma de decisiones. Además, debe promoverse la transparencia gubernamental a través de datos abiertos, fortalecer la ciberseguridad y la privacidad de los datos de los ciudadanos e impulsar alianzas público-privadas para desarrollar soluciones innovadoras. Asimismo, es esencial invertir en infraestructura digital y promover una cultura digital responsable y ética que involucre a todos los sectores de la sociedad en el uso y en el aprovechamiento de las tecnologías de la información y la comunicación.

Por otro lado, es vital **establecer alianzas estratégicas a nivel internacional**. La colaboración con otros bloques regionales, organismos internacionales y actores globales permitirá a ALC posicionarse de manera más sólida en el escenario digital mundial. Estas alianzas pueden abarcar desde la cooperación técnica y operativa hasta la negociación de acuerdos y tratados internacionales en cuestiones cibernéticas, aspectos en los que el SELA ha comenzado un trabajo conjunto con cursos que fueron coordinados con el Instituto Europeo de Estudios Internacionales (IEEI). Reviste suma im-

portancia el hecho de promover la diplomacia digital y la cooperación multilateral entre los países, los organismos internacionales, el sector privado y la sociedad civil, mediante la creación de plataformas de diálogo y colaboración que faciliten el intercambio de mejores prácticas, conocimientos y recursos en áreas como tecnología, ciberseguridad, comercio electrónico y gobernanza de internet.

No solo es importante fortalecer los acuerdos bilaterales y regionales que fomenten la interoperabilidad y la armonización de normativas en el ámbito digital, sino que también deben impulsarse iniciativas conjuntas de investigación, desarrollo e innovación tecnológica que siembren el crecimiento económico sostenible, la inclusión digital y la resiliencia cibernética a nivel global. Estas alianzas estratégicas permitirán enfrentar desafíos comunes, construir confianza mutua y aprovechar las oportunidades que ofrece la era digital para el beneficio de todos los actores involucrados.

Finalmente, es esencial **promover una cultura digital responsable y ética**. Educar y concientizar a la población sobre los riesgos y las oportunidades del ciberespacio, así como fomentar prácticas responsables en el uso de tecnologías digitales, contribuirá a construir una sociedad más informada, resiliente y participativa. Esto implica campañas de sensibilización, programas educativos y acciones de capacitación dirigidos a diversos grupos etarios y sectores de la sociedad, más específicamente, actividades educativas desde temprana edad que enseñen habilidades digitales, alfabetización mediática y ética en línea. Además, es necesario establecer códigos de conducta y normas de comportamiento en el entorno digital que fomenten el respeto, la privacidad y la integridad en la comunicación y el uso de tecnologías.

Las organizaciones públicas, privadas y educativas deben colaborar en campañas de concienciación que destaquen la importancia de la responsabilidad digital, la protección de datos personales y el combate a la desinformación. Asimismo, es importante involucrar a la sociedad civil, a los líderes de opinión y a las figuras públicas en iniciativas que fomenten valores éticos y prácticas responsables en el uso de plataformas en línea. Estas acciones contribuirán a crear una cultura digital basada en la confianza, la transparencia y el respeto mutuo, en la que los ciudadanos puedan aprovechar las oportunidades del mundo cibernético de manera segura y ética.

Tabla 13

Resumen de objetivos, recomendaciones e indicadores

Objetivo	Políticas	Indicadores
Cooperación regional robusta	Promover plataformas de diálogo entre países.	Número de plataformas de diálogo establecidas.
	Fortalecer la cooperación entre los sectores público y privado.	Proyectos conjuntos entre los sectores público y privado.
Fortalecimiento de capacidades nacionales	Inversión en formación especializada.	Número de programas de formación implementados.
	Desarrollo de un marco legal robusto.	Evaluación de la efectividad del marco legal.
Inclusión de actores no estatales	Involucrar al sector privado y la sociedad civil en iniciativas.	Número de proyectos conjuntos con actores no estatales.
	Promover la participación en la formulación de políticas.	Número de consultas públicas y mecanismos de retroalimentación.
Gobernanza digital inclusiva	Garantizar la participación multiactor en políticas y regulaciones.	Número de stakeholders involucrados en políticas y regulaciones.
	Promover el acceso a internet y a la educación digital.	Porcentaje de población con acceso a internet.
Alianzas estratégicas internacionales	Colaboración con bloques regionales y organismos internacionales.	Número de acuerdos o tratados internacionales firmados.
	Participación en foros internacionales.	Participación en eventos y reuniones internacionales.
Cultura digital responsable	Educación y concienciación sobre riesgos y oportunidades del ciberespacio.	Número de campañas de sensibilización implementadas.
	Fomentar prácticas responsables en el uso de tecnologías digitales.	Porcentaje de ciudadanos con conocimiento sobre prácticas digitales.

Fuente: elaboración propia.

El rol del SELA

La ciberdiplomacia, enfocada en la regulación del ciberespacio, la ciberseguridad y la gobernanza digital, emerge como una herramienta en el contexto contemporáneo para crear un marco propicio a fin de mejorar aspectos como la economía digital o de la información. En relación con esto último, el crecimiento de sectores de la economía relacionados con lo digital y lo informático pueden ayudar a alcanzar objetivos fundamentales: el desarrollo, la recuperación, la integración y la convergencia en la región, pilares centrales del quehacer del SELA.

Al establecer marcos regulatorios claros y coherentes en ciberseguridad y protección de datos, puede generarse un ambiente favorable para la inversión y la innovación tecnológicas, ya que la confianza entre los actores económicos impulsa la competitividad regional y posiciona a la región en el escenario global como un actor relevante en el ámbito digital. En ese sentido, la ciberdiplomacia desempeña un papel fundamental en la protección de las infraestructuras críticas de los países.

A través de la cooperación en ciberseguridad, se fortalece la resiliencia de sectores clave como energía, salud, finanzas y transporte, protección que garantiza la estabilidad económica y la seguridad nacional y que mitiga riesgos y amenazas cibernéticas que podrían afectar tanto la integridad como el funcionamiento de estas infraestructuras vitales. En lo que respecta a la integración regional, la ciberdiplomacia puede promover la colaboración transfronteriza y el intercambio de información entre países de la región al facilitar la armonización de políticas, regulaciones y normas en ciberseguridad, lo que crea un marco unificado que fomente la confianza mutua y la cohesión regional. Asimismo, permite impulsar el desarrollo de capacidades y de talento digital a través de programas especializados de formación y capacitación.

En el ámbito del desarrollo, la ciberdiplomacia ayuda a los países miembros del SELA a fortalecer sus capacidades tecnológicas y digitales. A través de

la colaboración en ciberdiplomacia, se facilita el intercambio de conocimientos y mejores prácticas. Así se estimula la innovación y el crecimiento económicos que, junto con la promoción de políticas y marcos normativos coherentes en ciberseguridad, contribuyen a crear un ambiente propicio para la inversión en ciencia y tecnología, esenciales para el desarrollo sostenible de la región.

Por otra parte, la cooperación regional facilita la respuesta conjunta a amenazas cibernéticas, protegiendo infraestructuras críticas y asegurando la continuidad de operaciones en momentos de crisis. Esta colaboración fortalecida permite a los países miembros del SELA mitigar riesgos y recuperarse más rápidamente de incidentes o ataques cibernéticos, lo que garantiza la estabilidad y la seguridad de sus sistemas nacionales. En relación con la integración, la ciberdiplomacia promueve la cohesión regional a través del intercambio de información y experiencias en ciberseguridad. El SELA actúa, en este caso, como un puente para la colaboración técnica entre naciones facilitando la armonización de políticas, regulaciones y normas en áreas críticas como protección de datos, ciberdefensa y delitos cibernéticos. Esta integración regional en ciberseguridad crea un marco unificado que posibilita la cooperación transfronteriza y fortalece la confianza entre los países miembros. Allanando el camino para el diálogo y la colaboración, se establecen estándares y normativas regionales en ciberseguridad que garantizan un desarrollo tecnológico equitativo y sostenible. Esta convergencia en políticas y estrategias cibernéticas favorece la integración económica y social de la región, lo que impulsa una agenda común para enfrentar los retos digitales del presente.

En relación con las recomendaciones del apartado anterior, el SELA se constituye como un facilitador esencial para promover el diálogo regional entre los países miembros. Mediante la organización de cumbres, reuniones ministeriales y grupos de trabajo especializados, crea un espacio propicio para abordar de manera conjunta temas cibernéticos, compartir experiencias y mejores prácticas, y fortalecer la cooperación en áreas cruciales como la ciberseguridad y la gobernanza digital. El organismo también ofrece

apoyo técnico y asesoramiento para la formulación e implementación de políticas públicas relacionadas con la ciberseguridad y la ciberdiplomacia.

A través de sus investigaciones, análisis y proyectos de cooperación técnica, el SELA asiste a los países miembros en el desarrollo de marcos normativos coherentes, impulsar la integración económica y robustecer los mecanismos institucionales en el ámbito digital. Esto incluye la promoción de valores democráticos, el Estado de derecho y los derechos humanos en el ciberespacio, que son aspectos fundamentales para construir un entorno seguro, transparente y confiable.

En el ámbito del desarrollo de capacidades, el SELA juega un papel clave al seguir ofreciendo programas de capacitación especializados, seminarios y talleres en áreas prioritarias como la ciberseguridad, la ciberdiplomacia y las tecnologías digitales. Esta iniciativa contribuye a fortalecer las habilidades y competencias de funcionarios públicos, profesionales y otros actores relevantes en la región, a fin de prepararse para enfrentar los desafíos y aprovechar las oportunidades del ciberespacio de manera efectiva. Además, la coordinación de capacitaciones que cuentan con la participación de representantes de los países miembros promociona alianzas estratégicas a nivel regional e internacional, ya sea con otros bloques regionales, organismos internacionales, actores provenientes del sector privado y organizaciones de la sociedad civil. Estas alianzas hacen posible que la región se posicione de manera más sólida y cohesiva en el escenario digital global, impulse una agenda común y aproveche las convergencias regionales para promover el desarrollo sostenible en la era digital de la información.

EPÍLOGO

A modo de cierre, resulta pertinente reflexionar sobre los múltiples aspectos abordados y extraer conclusiones significativas que puedan orientar futuras investigaciones, políticas y prácticas en este campo emergente y dinámico. En los capítulos precedentes, se han abordado diversos temas que van desde la importancia y la potencialidad de la ciberdiplomacia en el contexto regional, pasando por el uso de nuevas plataformas digitales y redes sociales, hasta llegar a cuestiones críticas como la ciberseguridad, la defensa, los derechos humanos, la economía digital y la inteligencia artificial. Cada sección ha ofrecido conceptos y análisis que han permitido comprender mejor las complejidades y desafíos de la ciberdiplomacia en la región.

En la era de la información contemporánea, la intersección entre tecnología y diplomacia ha redefinido las prácticas tradicionales de las relaciones internacionales, ya que la emergencia de la diplomacia digital y la ciberdiplomacia han transformado la forma en que los Estados interactúan entre sí, comunican sus políticas y gestionan sus intereses en un entorno globalizado y altamente interconectado. Esto se da en un contexto en el que las plataformas y las redes sociales se han erigido como espacios cruciales donde se moldean percepciones, se construyen alianzas y se gestionan cuestiones a nivel global.

Si bien las herramientas digitales ofrecen nuevas vías para fortalecer la cooperación regional e internacional, también plantean preocupaciones relacionadas con la seguridad cibernética, la privacidad y la desinformación. La adaptación estratégica a este nuevo panorama requiere una comprensión profunda de las particularidades regionales, así como una visión proactiva para navegar por un paisaje en constante evolución. En este contexto dinámico, las estrategias efectivas de comunicación en redes sociales se convierten en un pilar fundamental para fortalecer la diplomacia y promover intereses nacionales en el escenario internacional. Si bien la segmentación del público objetivo, la definición de metas claras y la creación de contenido relevante son elementos esenciales para maximizar el impacto de la comunicación en plataformas digitales, es esencial reconocer y abordar los desa-

fíos inherentes, como la polarización y la dependencia de algoritmos que pueden influir en la percepción pública y las interacciones diplomáticas.

Como se ha mencionado, la ciberdiplomacia, la diplomacia digital y la e-diplomacia son términos interrelacionados pero con matices distintos en el ámbito de las relaciones internacionales y la tecnología. La ciberdiplomacia se centra en el uso estratégico de tecnologías cibernéticas e información para regular y proteger intereses nacionales en el ciberespacio, abordando aspectos como la ciberseguridad, la gobernanza digital y la relación con la economía digital. La diplomacia digital se enfoca, principalmente, en emplear plataformas y herramientas digitales, como redes sociales y aplicaciones de mensajería, para facilitar la comunicación y la cooperación entre Estados y actores internacionales y potenciar la transparencia de las prácticas diplomáticas tradicionales y su accesibilidad. En contraste, la e-diplomacia se presenta como un término más amplio que engloba tanto la diplomacia digital como otros aspectos que abarcan desde el intercambio de información hasta la colaboración en línea y se adapta a las transformaciones tecnológicas y geopolíticas.

El panorama regional refleja una serie de desafíos y oportunidades en el ámbito de la ciberseguridad, donde las amenazas, como los ataques a infraestructuras críticas y campañas de desinformación, representan riesgos significativos para la estabilidad y la seguridad. Aunque en la región se ha avanzado significativamente en áreas como la democracia y la integración regional, persisten desafíos críticos: desde la brecha digital hasta la falta de capacidades técnicas especializadas y la ausencia de marcos normativos regionales cohesivos. La ciberdiplomacia, tal como se presenta, aspira a abordar estos desafíos de manera integral, pues proporciona recomendaciones y estrategias adaptadas a las realidades y necesidades específicas de la región. En esta tarea, la cooperación entre países para establecer regulaciones comunes se destaca como un elemento clave.

A pesar de las disparidades en capacidades técnicas y de las tensiones geopolíticas, la región ha reconocido la importancia de trabajar conjuntamente para promover un ciberespacio seguro, abierto y colaborativo. Las lecciones aprendidas de otras regiones pueden servir de experiencia para ALC

porque ofrecen un modelo valioso en la búsqueda de soluciones conjuntas en ciberdiplomacia. El desarrollo de normas regionales de ciberseguridad también emerge como una necesidad imperativa para fortalecer la cooperación, mitigar riesgos y promover un ciberespacio seguro. Organismos como el SELA, la OEA y el BID han liderado esfuerzos para establecer estándares comunes, fomentar la cooperación técnica y facilitar el intercambio de información entre países miembros. La CELAC, por su parte, también se ha posicionado sobre el tema (Vega, 2023). Aunque enfrentan desafíos, la experiencia regional demuestra que la colaboración multisectorial, al involucrar al sector privado, a la sociedad civil y al sector académico, es esencial para desarrollar soluciones innovadoras y promover la adopción efectiva de normas regionales.

En un escenario global donde la intersección entre ciberseguridad y relaciones internacionales redefine las dinámicas de poder, influencia y cooperación, la ciberdiplomacia emerge como un instrumento indispensable para gestionar tensiones, promover normas compartidas y fortalecer la seguridad internacional. No obstante, este nuevo contexto también plantea desafíos éticos y jurídicos que requieren respuestas coherentes y consensuadas, puesto que, en el ámbito regional, la cooperación en ciberseguridad se presenta como un imperativo para abordar vulnerabilidades compartidas y construir un ciberespacio más seguro y resiliente. Con el propósito de avanzar hacia una ciberseguridad robusta a nivel regional, es fundamental adoptar un enfoque integral que promueva la cooperación técnica y financiera, fortalezca las capacidades nacionales, favorezca la armonización normativa y robustezca la resiliencia cibernética. Estas estrategias, junto con un compromiso renovado de los Estados, del sector privado, de la academia y de la sociedad civil, pueden contribuir a construir un ciberespacio que proteja los intereses, los derechos y las libertades de los países y de sus ciudadanos.

Ahora bien, la emergencia de la ciberdiplomacia como un campo estratégico para las relaciones internacionales se complementa con la necesidad imperativa de proteger y promover los derechos humanos en el ciberespacio, un entorno cada vez necesario para el desarrollo sostenible, la democracia y la inclusión en la región. En la actualidad digital, el almacena-

miento y uso masivo de datos generan inquietudes sobre la privacidad y la libertad de expresión, con plataformas digitales que facilitan la difusión de discursos dañinos y hasta violentos. Algunos Gobiernos restringen el acceso a internet y limitan la libertad de expresión, justificándolas como medidas contra el extremismo y emplean tácticas de vigilancia y desinformación contra defensores de derechos humanos y grupos vulnerables. A pesar de las preocupaciones que surgen sobre la discriminación y la parcialidad en sistemas basados en inteligencia artificial, el marco global de derechos humanos ofrece una guía para abordar estos problemas, situación que requiere colaboración entre los Gobiernos, las empresas, las organizaciones y los actores que defienden los derechos para asegurar que la digitalización respalde principios de transparencia, justicia y responsabilidad. Reviste suma importancia adoptar una estrategia que integre valores éticos y de derechos humano, y que asegure que la tecnología beneficie a las personas y no las perjudique.

Teniendo en cuenta los objetivos del SELA en relación con la integración regional y con el desarrollo económico, la techplomacia se presenta como un medio para navegar las relaciones entre los Estados y las grandes empresas tecnológicas. Es necesario fortalecer la posición de la región en estos ámbitos y promover la cooperación y la regulación efectiva, sobre todo, en un escenario en que las monedas digitales y las criptomonedas también se destacan por su potencial para transformar las transacciones financieras. En este contexto, son fundamentales la colaboración, la regulación y las políticas públicas orientadas a fortalecer la gobernanza digital y el desarrollo sostenible en la era digital. La mayoría de los esfuerzos de la región en materia de ciberdiplomacia se centran en la ciberseguridad, por lo cual la tarea del SELA (2023c) en el fortalecimiento y desarrollo de la relación con la economía digital y con las big tech companies es central.

Por su parte, el desarrollo de políticas públicas para el crecimiento de los países en materia de ciberdiplomacia es un serio desafío. Resulta cardinal reconocer que las políticas públicas no solo reflejan decisiones gubernamentales sino que también son instrumentos para sembrar el bienestar colectivo y la armonía entre naciones interconectadas digitalmente. La

cooperación regional se destaca como un pilar indispensable: aboga por diálogos constantes entre actores clave, como los Gobiernos, el sector privado, la academia y la sociedad civil.

Al reflexionar sobre el futuro de la ciberdiplomacia en el continente, se torna incuestionable la necesidad de adoptar un enfoque adaptativo, innovador y centrado en principios éticos y de derechos humanos. En este contexto dinámico, es crucial explorar y anticipar diversos escenarios futuros, desde perspectivas optimistas hasta desafíos más complejos, con el objetivo de orientar estratégicamente el desarrollo digital y cibernético de la región. Por ello, el papel del SELA adquiere una relevancia estratégica, ya que actúa como catalizador y facilitador de la convergencia regional, la cooperación técnica y el desarrollo sostenible. En última instancia, la visión para el futuro debe priorizar la construcción de un ciberespacio inclusivo, seguro y ético que respete y promueva los valores democráticos, los derechos humanos y el bienestar colectivo.

REFERENCIAS

Anderson, J. E. (1975). *Public Policymaking*. Holt Reinhart and Winston Inc. Disponible en: https://books.google.co.ve/books/about/Public_Policy_making.html?id=JxkXAAAAIAAJ&redir_esc=y

Barrinha, A. y Renard, T. (2017). *Cyber-diplomacy: the making of an international society in the digital age*. Global Affairs, 3(4-5), pp. 353-364. Disponible en: https://doi.org/10.1080/23340460.2017.1414924

Becerra, M. y Mastrini, G. (2017). *La concentración infocomunicacional en América Latina (2000-2015): nuevos medios y tecnologías, menos actores*. Universidad Nacional de Quilmes y Observacom. Disponible en: https://www.observacom.org/wp-content/uploads/2019/09/La-concentracio%CC%81n-infocomunicacional-en-Ame%CC%81rica-Latina-2000-2015.pdf

Bulnes, M. e Higueras, S. (2023). Apuntes sobre los impactos recíprocos entre diplomacia e inteligencia artificial. *Revista Política Internacional*, (134), pp. 29-43. Disponible en: https://revista.adp.edu.pe/index.php/RPI/article/view/86

Bustos Frati, G. y Aguerre, C. (2021). *Marco analítico para el análisis de políticas públicas sobre ciberseguridad en los países latinoamericanos*. Centro Latam Digital. Disponible en: https://centrolatam.digital/publicacion/marco-analitico-para-el-analisis-de-politicas-publicas-sobre-ciberseguridad-en-los-paises-latinoamericanos

Calvo, E. (2015). *Anatomía política de Twitter en Argentina: Tuiteando #Nisman*. Capital Intelectual. Disponible en: https://claveintelectual.com.ar/productos/anatomia-politica-de-twitter-en-argentina/

Calvo, E., y Aruguete, N. (2020). *Fake news, trolls y otros encantos. Cómo funcionan (para bien y para mal) las redes sociales*. Siglo XXI. Disponible en: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-49112020000200137

Campos Ríos, M. (2022). *El Estado en la era meta: del Estado inteligente al Estado inmersivo*. CLAD. Disponible en: https://clad.org/autor-maximiliano-campos/el-estado-en-la-era-meta-del-estado-inteligente-al-estado-inmersivo/

Campos Ríos, M. (2023). *Cadenas de valor público y ecosistema digital.* SELA. Disponible en: https://www.sela.org/es/centro-de-documentacion/base-de-datos-documental/bdd/91817/cadenas-de-valor-y-ecosistema-digital

Castells, M. (1995). *La ciudad informacional: tecnologías de la información, reestructuración económica y el proceso urbano-regional*. Alianza. Disponible en: https://e-tcs.org/wp-content/uploads/2017/03/Castells_19951.pdf

Castells, M. (2009). *Comunicación y poder*. Alianza Editorial. Disponible en: https://www.academia.edu/34150052/COMUNICACI%C3%93N_Y_PODER_Manuel_Castells

Comisión Económica para América Latina y el Caribe (2021). Datos y hechos sobre la transformación digital. *Documentos de proyectos (LC/TS.2021/20)*. CEPAL. Disponible en: https://repositorio.cepal.org/server/api/core/bitstreams/18590f39-d1e7-4370-b9d2-5769b1561422/content

Comisión Europea (2019). *A Definition of AI Main Capabilities and Disciplines*. Unión Europea. Disponible en: file:///C:/Users/cortuno/Downloads/ai_hleg_ai_definition_final_DF06F793-EA01-3573-16D2AC-D625E2BDB0_56341.pdf

Domínguez Bascoy, J. (2014). La ciberseguridad: aspectos jurídicos internacionales. *Revista Cursos de derecho internacional y relaciones internacionales de Vitoria-Gasteiz - Vitoria-Gasteizko nazioarteko zuzenbide eta nazioarteko herremanen ikastaroak*, 1, pp. 161 224.

Feijóo, C., Kwon, Y., Bauer, J. M, Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J. y Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, 44(6). Disponible en: https://doi.org/10.1016/j.telpol.2020.101988

García Zaballos, A., Iglesias Rodríguez, E., Puig Gabarró, P. y Dalio, M. (2023). I*nforme anual del Índice de Desarrollo de la Banda Ancha: brecha digital en América Latina y el Caribe*. Banco Interamericano de Desarrollo. Disponible en: https://publications.iadb.org/es/informe-anual-del-indice-de-desarrollo-de-la-banda-ancha-brecha-digital-en-america-latina-y-el-0

Estévez, A. M. (2014). Algunas características fundamentales de los estudios de políticas públicas. *Cuadernos de Polipub.org*, 13, pp. 3-19. Disponible en: DOI: 10.13140/2.1.1372.2886

Jenkins, H. (2006). Convergence Culture. *La cultura de la convergencia de los medios de comunicación*. Paidós. Disponible en: https://www.perio.unlp.edu.ar/sitios/wp-content/uploads/sites/7/2015/03/henry_jenkins-cultura-de-la-convergencia.pdf

Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books. Disponible en: https://www.hachettebookgroup.com/titles/lawrence-lessig/code/9780786721962/?lens=basic-books

Lessig, L. (2002). Las leyes del ciberespacio. THEMIS: *Revista de Derecho*, 44, pp. 171-179. Disponible en: file:///C:/Users/cortuno/Downloads/Dialnet-LasLeyesDelCiberespacio-5110282.pdf

Maldonado, T. (1998). *Crítica de la razón informática*. Paidós. Disponible en: https://monoskop.org/images/e/ef/Maldonado_Tomas_Critica_de_la_razon_informatica.pdf

Mazzucato, M. (2022). *El Estado emprendedor. Mitos en la oposición público vs. privado*. Taurus. Disponible en: https://books.google.co.ve/books/about/El_estado_emprendedor.html?id=WvSKEAAAQBAJ&redir_esc=y

Mercado Común del Sur (6 de diciembre de 2022). *Declaración especial sobre ciberdelincuencia*. LXI Cumbre de Presidentes del Mercosur. Montevideo, Uruguay. Disponible en: https://www.gov.br/mre/es/canales_servicio/prensa/notas-a-la-prensa/declaracion-especial-sobre-ciberdelincuencia

Muñiz, M. (2003). Diplomacia tecnológica para la era digital. Revista CIDOB d'Afers Internacionals, (134), pp. 91-102. Disponible en: DOI: doi.org/10.24241/rcai.2023.134.2.91

Observatorio de la Ciberseguridad en América Latina y el Caribe (2020). *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020*. BID y OEA. Disponible en: file:///C:/Users/cortuno/Downloads/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe%20(1).pdf

Pariser, E. (2017). *El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos*. Taurus. Disponible en: https://www.altamiralibros.com/libro/el-filtro-burbuja_23097

Peil, C. y Sparviero, S. (2017). Media Convergence Meets Deconvergence. En S. Sparviero, C. Peil y G. Balbi (eds.), *Media Convergence and Deconvergence*. IAMCR, AIECS, AIERI.

Pohle, J. y Thorsten, T. (2020). Digital *sovereignty. Internet Policy Review*, 9(4), pp. 1 19. Disponible en: https://doi.org/10.53857/OLMH2516

Riordan, S. (2019). *Cyberdiplomacy: Managing Security and Governance Online*. Polity Press.

Riordan, S. y Torres Jarrín, M. (2020). *Techplomacy and the Tech Ambassador*. European Institute of International Studies. Disponible en: https://books.google.co.ve/books/about/Cyberdiplomacy.html?id=XaySDwAAQBAJ&redir_esc=y

Rodríguez Gómez, A. A. (2015). *Diplomacia digital, ¿adaptación al mundo digital o nuevo modelo de diplomacia?* Opción, 31(2), pp. 915-937. Disponible en: https://www.redalyc.org/pdf/310/31045568050.pdf

Sistema Económico Latinoamericano y del Caribe (2021). *Cursos de Especialización sobre Ciberdiplomacia y Techplomacia. Informe* Final. SELA. Disponible en: https://www.sela.org/es/centro-de-documentacion/base-de-datos-documental/bdd/75178/ciberdiplomacia-y-techplomacia

Sistema Económico Latinoamericano y del Caribe (2022a). *Revista Convergencia. Agosto 2022*. 1(2). SELA. Disponible en: https://www.sela.org/es/centro-de-documentacion/base-de-datos-documental/bdd/84334/convergencia_2

Sistema Económico Latinoamericano y del Caribe (2022b). *Segunda edición de los Cursos de Especialización sobre Ciberdiplomacia y Techplomacia. Informe Final*. SELA. Disponible en: https://www.sela.org/es/centro-de-documentacion/base-de-datos-documental/bdd/80824/if-2da-edicion-curso-ciberdiplomacia-y-techplomacia-pdf

Sistema Económico Latinoamericano y del Caribe (2023a). *América Latina y el Caribe frente a los desafíos de la integración del siglo XXI*. SELA. Disponible en: https://www.sela.org/es/centro-de-documentacion/base-de-datos-documental/bdd/92644/alc-frente-a-los-desafios-de-la-integracion-del-siglo-xxi

Sistema Económico Latinoamericano y del Caribe (2023b). *Mapeo de nichos productivos en América Latina y el Caribe: experiencias y lecciones aprendidas*. SELA. Disponible en: https://www.sela.org/es/centro-de-documentacion/base-de-datos-documental/bdd/92642/mapeo-de-nichos-productivos

Sistema Económico Latinoamericano y del Caribe (2023c). *Tercera edición de los cursos de especialización en Ciberdiplomacia y la diplomacia de las monedas digitales. Informe de Relatoría*. SELA. Disponible en: https://www.sela.org/es/centro-de-documentacion/base-de-datos-documental/bdd/89742/tercera-edicion-de-los-cursos-de-especializacion-en-ciberdiplomacia-y-la-diplomacia-de-las-monedas-digitales

Srnicek, N. (2018). *Capitalismo de plataformas*. Caja Negra Editora. Disponible en: https://cajanegraeditora.com.ar/libros/capitalismo-de-plataformas-nick-srnicek/

Torres Jarrín, M. (2021). La UE y la gobernanza ética de la inteligencia artificial: inteligencia artificial y diplomacia. *Cuadernos Salmantinos de Filosofía*, 48, pp. 213-234. Disponible en https://doi.org/10.36576/ summa.144499

Van Cuilenburg, J. y McQuail, D. (2003). Media policy paradigm shifts: towards a new communications policy paradigm. *European Journal of Communication*, 18(2), pp. 181-207. Disponible en: https://doi.org/10.1177/0267323103018002002

Van Dijk, J., Poell, T. y de Wall, M. (2018). *The Platform Society: Public Values in a Connective World. Oxford University Press.* Disponible en: https://academic.oup.com/book/12378

Vega, J. M. (2023). Ciberdiplomacia en América Latina: niveles, enfoques y velocidades. *Real Instituto Elcano ARI*, 38, pp. 1-7. Disponible en: https://media.realinstitutoelcano.org/wp-content/uploads/2023/05/ari38-2023-vega-ciberdiplomacia-en-america-latina-niveles-enfoques-y-velocidades.pdf

SISTEMA ECONÓMICO
LATINOAMERICANO
Y DEL CARIBE

Más y mejor Integración

www.sela.org

@selainforma