FACULTAD DE CIENCIA POLITICA
Y RELACIONES INTERNACIONALES
UNIVERSIDAD NACIONAL DE ROSARIO

Universidad Nacional de Rosario

Facultad de Ciencia Política y Relaciones Internacionales

Licenciatura en Relaciones Internacionales

Tesina de Grado

"El Impacto de la Inteligencia Artificial en la Diplomacia: Innovación y Desafíos en la Era Digital"

Autora: Constanza Oliva

Email: constanza.oliva99@gmail.com

Directora: Paula Demarchi

Fecha: 17/09/2024

Índice:

Resumen **2**

Agradecimientos **3**

Introducción **4**

Marco Conceptual **12**

Capítulo 1: Diplomacia Digital e Inteligencia Artificial:

1.1 Impacto de la utilización de la inteligencia artificial en la toma de decisiones diplomáticas, eficiencia operacional y comunicación personalizada **17**

1.2 El papel de la inteligencia artificial en la redefinición de las estrategias y tácticas diplomáticas modernas **24**

Capítulo 2: Ciberseguridad

2.1 Beneficios de la inteligencia artificial en la detección y prevención de ciberamenazas en la diplomacia digital **32**

2.2 Desafíos asociados con los ciberataques y el espionaje, y estrategias de mitigación y protección para los Estados **38**

Capítulo 3: Acceso a los datos y Ëtica

3.1 La influencia de la disparidad en el acceso y uso de la inteligencia artificial en las relaciones internacionales **45**

3.2 Consideraciones éticas en el desarrollo y uso de la inteligencia artificial **52**

Reflexiones finales **58**

Referencias bibliográficas **62**

Resumen

La presente tesina examinará cómo la diplomacia digital está siendo afectada por la creciente aparición de la inteligencia artificial (IA) en el escenario global. El estudio se centrará en tres áreas clave: la toma de decisiones diplomáticas, la ciberseguridad, y la equidad en el acceso y uso de la IA. La investigación exhibirá cómo la IA no solo tiene el potencial de mejorar de manera significativa la eficiencia y efectividad de las interacciones diplomáticas, sino que también puede optimizar el análisis de datos y fortalecer la capacidad de los diplomáticos para gestionar crisis y anticipar escenarios complejos. Sin embargo, estos beneficios dependerán de la implementación de estrictas medidas de seguridad y de mejores prácticas en la protección de la información y la infraestructura digital.

Además, se abordarán los desafíos éticos y estratégicos que surgen con la adopción de la IA en la diplomacia. Entre ellos, se encuentran preocupaciones sobre la privacidad de la información diplomática, el riesgo de sesgo algorítmico en la toma de decisiones y la falta de transparencia en los sistemas automatizados. También se destacará la creciente disparidad entre Estados en cuanto a su capacidad para acceder y utilizar la IA, lo cual podría intensificar las desigualdades existentes en el poder y la influencia internacional. La investigación, por tanto, ofrecerá un análisis exhaustivo de las oportunidades y riesgos que plantea la IA para la diplomacia en un mundo cada vez más digitalizado e interconectado.

Palabras clave: Diplomacia digital, inteligencia artificial, toma de decisiones, ciberseguridad, ética, poder blando.

Agradecimientos

En primer lugar, quisiera agradecerle a Paula, cuya dedicación, organización y responsabilidad han sido fundamentales para que este proyecto se haga realidad. Gracias por guiarme con tanta paciencia y entusiasmo a lo largo de este camino.

Quisiera agradecerle a mi familia. A mi mamá y a mi papá, que me apoyaron y me enseñaron el valor del esfuerzo y el compromiso. A Delfina, por ser mi impulso cuando más lo necesitaba. A Francisco, por escucharme estudiar y brindarme aliento. A Ignacio, que desde la distancia siempre estuvo acompañándome. Y a Luciano, por estar en los momentos clave, dándome el apoyo y el empuje necesario para seguir adelante.

A mis amigas de la primaria, que han estado conmigo incondicionalmente desde que somos pequeñas, acompañándome en cada paso de mi vida.

A los amigos que hice en mi recorrido por la fcpolit, quienes han sido un sostén esencial en estos años y nadie más que ellos entienden lo que es este logro. En especial a Abraham y Celina, quienes me han acompañado desde mis primeros días en la facultad hasta este último momento, convirtiéndose en personas indispensables en mi vida.

A Lu, quien, aunque llegó en el último tramo de la facultad, se convirtió en un pilar fundamental para mí. Gracias por las largas noches de estudio, por quedarte conmigo, escucharme, leerme cuando estaba agotada, y por compartir esta última etapa con tanto amor y paciencia.

A She, el amor de mi vida, cuya sola existencia ilumina mis días y llena mi vida de alegría.

Finalmente, a la universidad pública, y en especial a la Fcpolit, que, aunque representó un gran desafío, también me brindó aprendizajes invaluables y de una calidad excepcional.

Introducción

Las nuevas tecnologías han estado señalando novedosos rumbos para todo tipo de acciones institucionales y diplomáticas desde el comienzo del siglo XXI. Diversos actores pueden avanzar por el camino digital con costes muy razonables, y así, alcanzar públicos segmentados en función de las características y demandas de cada audiencia. Las autoridades utilizan los canales digitales para difundir la propaganda oficial y reforzar la influencia y el control de la población.

A lo largo de los años, la sociedad ha experimentado constantes avances tecnológicos que han transformado diversos ámbitos, incluida la diplomacia. Es fundamental reconocer que la diplomacia digital ha evolucionado con cada nuevo descubrimiento tecnológico, adaptándose y aprovechando los beneficios potenciales que ofrecen estas innovaciones para optimizar sus prácticas y estrategias.

No obstante, el paso de la diplomacia tradicional a la diplomacia digital representa una transformación profunda que trasciende la simple incorporación de herramientas tecnológicas. Este cambio implica una reconfiguración integral del enfoque diplomático, donde la inmediatez, la interactividad y el acceso a grandes volúmenes de información en tiempo real redefinen las prácticas de comunicación y negociación en el ámbito internacional. La diplomacia digital no solo introduce nuevas plataformas y medios, sino que también modifica la dinámica del poder y la influencia, al facilitar una participación más directa y una mayor capacidad de respuesta ante los acontecimientos globales. Esta transformación estructural refleja un enfoque diplomático más ágil y adaptable, preparado para enfrentar los desafíos de un mundo cada vez más interconectado y complejo.

En la diplomacia digital, ya no basta con comunicar, los diplomáticos deben procesar la información de la Red, analizar *big data* y construir estrategias digitales. Las interacciones diplomáticas se ven influidas y transformadas por plataformas digitales y algoritmos de inteligencia artificial (IA). La diplomacia digital exige no sólo informar, sino también interactuar y conversar con los ciudadanos de otros países y del país en el cual están localizados. Nuevas alianzas y complicidades necesitan ser establecidas con gobiernos y sociedades civiles a través de la Red. Esto obliga a ajustar las estructuras

diplomáticas bajo una premisa básica: integrar la diplomacia digital en las labores del diplomático.

La diplomacia digital ha recorrido un largo camino desde sus inicios con los mails y los primeros sitios web hasta convertirse en un componente sumamente importante de las políticas exteriores modernas, enriquecida por tecnologías avanzadas como la IA y el análisis de datos.

Esta diplomacia comienza a emerger con la llegada de Internet y el correo electrónico, herramientas que empezaron a ser utilizadas por los ministerios de relaciones exteriores y las embajadas para mejorar la comunicación interna y externa. Durante esta etapa inicial, el uso de las tecnologías de la información y la comunicación (TIC) en la diplomacia era principalmente funcional, enfocado en la eficiencia y la gestión (Bjola y Holmes, 2015).

El surgimiento de las redes sociales y otras plataformas digitales transformó la manera en que los Estados y las organizaciones internacionales se relacionan con el público. Las embajadas y los diplomáticos comenzaron a utilizar herramientas como Twitter (actualmente X), Facebook (actualmente Meta) y blogs para gestionar la percepción pública de sus países en tiempo real. (Manor, 2019)

Además, es importante considerar que, debido a la pandemia de COVID-19, muchas actividades que tradicionalmente se realizaban de forma presencial tuvieron que adaptarse rápidamente a una modalidad digital. La diplomacia no fue una excepción a este cambio, experimentando una transición forzada hacia plataformas digitales para mantener la continuidad de sus operaciones y relaciones internacionales.

La diplomacia digital se vuelve más sofisticada y estratégica, integrándose plenamente en las políticas exteriores de muchos países. Los gobiernos empezaron a reconocer el alcance de las redes sociales no solo para la comunicación, sino también para la influencia y la promoción de sus intereses nacionales en el extranjero. (Hocking et al., 2012)

La integración de la IA y el análisis de *big data* en la diplomacia digital representa la fase más reciente de su evolución. La IA se utiliza para analizar grandes volúmenes de datos y proporcionar conocimientos que pueden informar la toma de

decisiones diplomáticas. Herramientas avanzadas permiten a los diplomáticos monitorear tendencias globales, gestionar crisis y anticipar desarrollos (Bjola, 2018).

Esta integración plantea una serie de desafíos y dilemas éticos, incluyendo preocupaciones sobre la privacidad, la seguridad, el sesgo algorítmico y la falta de transparencia en el proceso de toma de decisiones. La IA en la diplomacia digital está generando tanto oportunidades como desafíos. Aunque la IA puede mejorar la eficiencia y efectividad de las interacciones diplomáticas, también plantea riesgos significativos en términos de ciberseguridad y manejo de datos sensibles. Además, existe una disparidad en la capacidad de los estados para adoptar estas tecnologías, lo que puede exacerbar las desigualdades internacionales y afectar las relaciones diplomáticas.

Ahora, la comunicación ha pasado a ser bidireccional y personalizada. Las Cancillerías y los diplomáticos buscan crear experiencias diplomáticas centradas en los intereses, necesidades y patrones de uso de los usuarios de la tecnología.

En este contexto y siguiendo esta línea de ideas es que nos preguntamos: ¿Cómo la diplomacia digital se ve impactada por la IA, y cuáles son los beneficios y desafíos asociados con su implementación en términos de ciberseguridad, gestión de datos y equidad entre los estados?

En relación con lo explicado anteriormente, el objetivo que conduce esta investigación es lograr analizar cómo la IA impacta en la diplomacia digital, identificando las oportunidades y desafíos que presenta su implementación, con los enfoques previamente mencionados. De este objetivo general se desprenden los siguientes objetivos específicos: examinar cómo la IA puede optimizar la gestión y análisis de datos en la diplomacia, analizar cómo esta herramienta puede ser empleada para detectar, prevenir, mitigar o deteriorar la ciberseguridad en la diplomacia digital y explorar cómo la disparidad en el acceso y uso de la IA puede influir en las relaciones internacionales.

A modo de hipótesis, el presente trabajo sostiene que la IA tiene el potencial de convertirse en una parte troncal de la diplomacia en el futuro, mejorando significativamente la eficiencia y efectividad de las interacciones diplomáticas, siempre y cuando se desarrollen y apliquen adecuadas medidas de seguridad y mejores prácticas

para proteger la integridad de la información diplomática en un entorno digital. Podemos optimizar la gestión y el análisis de datos, mejorando la precisión y rapidez en la toma de decisiones, así como la capacidad de los diplomáticos para interactuar y comunicarse con diversas audiencias. Asimismo, con las estrategias adecuadas, es factible asegurar que los beneficios de la diplomacia digital sean accesibles para todos los estados, independientemente de su nivel de desarrollo tecnológico.

La transición de la diplomacia tradicional a la digital es un tema que ha cobrado relevancia en el campo de las relaciones internacionales. Para referirnos a la diplomacia digital, también conocida como ciberdiplomacia, diplomacia electrónica o e-diplomacia, utilizaremos el concepto de Bjola (2015) que hace referencia al uso de tecnologías de la información y comunicación para alcanzar objetivos diplomáticos. Desde el comienzo del siglo XXI, podemos observar cómo ha cambiado la manera en que los estados y las instituciones diplomáticas se comunican y operan. La diplomacia digital incluye una variedad de prácticas, como el uso de redes sociales para la comunicación pública, la creación de plataformas digitales para la colaboración internacional, y la implementación de sistemas de gestión de datos para la toma de decisiones informadas.

Este campo ha sido estudiado por una variedad de autores de diferentes partes del mundo, quienes han explorado sus implicaciones y aplicaciones en diversos contextos. Entre los autores destacados se encuentran Corneliu Bjola (2015), que ha trabajado extensamente en la teoría y práctica de la diplomacia digital; Ilan Manor (2019), que ha investigado el impacto de las redes sociales en la diplomacia; Jan Melissen (2005), conocido por su trabajo en diplomacia pública y digital; Joseph S. Nye (2011), que ha examinado el poder blando en el contexto de la diplomacia digital; Alexander L. Vuving (2013), que ha aportado perspectivas sobre la ciberseguridad y la diplomacia; y Shaun Riordan (2019), que ha analizado las transformaciones en las prácticas diplomáticas debido a las tecnologías digitales. Estos autores ofrecen una visión amplia y diversa de cómo la diplomacia digital está redefiniendo las relaciones internacionales en la era moderna.

La tecnología ha avanzado hasta el punto en que la IA está al alcance de todos, y esto ha impactado significativamente en la diplomacia digital. La IA se define como la capacidad de una máquina para imitar la inteligencia humana, mediante el aprendizaje, razonamiento y la auto-corrección. Según Russell y Norvig (2019), la IA implica el

desarrollo de algoritmos y sistemas capaces de realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de patrones, el procesamiento del lenguaje natural y la toma de decisiones autónoma. Mitchell (2019) destaca que la IA no solo busca replicar la inteligencia humana, sino también ampliar sus capacidades a través del procesamiento de grandes volúmenes de datos y la automatización de procesos complejos.

Koekelberg (2020) añade que la IA abarca diversas disciplinas, incluyendo el aprendizaje automático, la visión por computadora y la robótica, cada una contribuyendo a la creación de sistemas más inteligentes y eficientes. Esta tecnología tiene un impacto significativo en múltiples áreas, desde la economía y la medicina hasta la seguridad y la diplomacia, planteando tanto oportunidades como desafíos éticos y sociales. En resumen, la IA representa un avance tecnológico que no solo busca emular la inteligencia humana, sino también potenciar y aplicarla a una variedad de contextos prácticos y teóricos.

Este campo ha sido estudiado por una variedad de autores de diferentes partes del mundo, quienes han explorado sus implicaciones y aplicaciones en diversos contextos. Entre los autores destacados se encuentran, ya mencionados anteriormente, Stuart Russell y Peter Norvig (2019), cuyas obras como "Artificial Intelligence: A Modern Approach" son fundamentales en el estudio de la IA; Melanie Mitchell (2019), que ha explorado las implicaciones de la IA en diversos contextos; Mark Koekelberg (2020), conocido por su trabajo en ética de la tecnología y la IA; Yann LeCun (2015), pionero en el desarrollo de redes neuronales y aprendizaje profundo; Andrew Ng (2017), un líder en el campo del aprendizaje automático y la IA aplicada; Fei-Fei Li (2019), que ha trabajado extensamente en visión por computadora; y Nick Bostrom (2014), que ha investigado los impactos futuros y los riesgos existenciales de la IA, entre otros.

Para contextualizar el recorte temporal, es esencial entender el concepto de era digital. Castells (2010) describe el área digital como un ámbito que engloba tecnologías, disciplinas, y actividades relacionadas con el uso de medios digitales, desde el desarrollo de software y la gestión de redes sociales, hasta el análisis de datos y la ciberseguridad. Este campo comenzó a tomar forma con la digitalización y la informática en la segunda mitad del siglo XX, adquiriendo mayor relevancia con el

auge de internet a partir de los años 90 y la expansión de la tecnología móvil y la economía digital en el siglo XXI.

Asimismo, la IA comenzó a desarrollarse como un campo formal de estudio y tecnología en la década de 1950. Este período marca el inicio de la IA como una disciplina, con trabajos pioneros de científicos como Alan Turing, John McCarthy, Marvin Minsky, y otros que sentaron las bases para lo que hoy conocemos como IA. Su impacto en la diplomacia se ha hecho más notable a partir de la década de 2010, cuando las tecnologías de IA, como el aprendizaje automático, la minería de datos y el procesamiento del lenguaje natural, comenzaron a ser aplicadas en áreas como la diplomacia digital, la gestión de conflictos, la ciberseguridad y la propaganda. Este período coincide con el auge del big data, la computación en la nube, y el aumento del poder computacional. Por ello, en esta tesina se tomarán ejemplos y bibliografía desde 2010 hasta agosto del 2024.

En línea con lo planteado, es de suma envergadura poder analizar el contexto actual de la diplomacia digital y la gran influencia que posee la IA sobre la misma, ya que cada vez vivimos en un mundo más globalizado e interconectado, donde ambas están en una etapa crucial de desarrollo y adopción. Observaremos cómo los Estados ponen en juego su capacidad para llevar a cabo acciones de diplomacia digital para influenciar a otros Estados, regiones e individuos para verse favorecidos. Es una de las herramientas de *soft power* más utilizadas en la actualidad, crece a un ritmo acelerado y está incidiendo en grandes cambios de la sociedad, es por eso mismo que los diplomáticos deben poder entender cómo explotar al máximo sus beneficios. Este análisis es crucial debido a que la IA tiene el potencial de transformar la diplomacia, la seguridad y la defensa de un país cuando se utiliza adecuadamente, al contribuir significativamente a la labor de los funcionarios diplomáticos.

Este estudio puede considerarse una contribución significativa tanto para los individuos, Estados, organizaciones internacionales que están abocados a la diplomacia, como para la sociedad civil que se encuentra interpelada frente a la toma de decisiones. Asimismo, los resultados obtenidos serán de gran utilidad y relevancia para la gestión pública. Al explorar cómo la IA puede ser utilizada para mejorar la toma de decisiones diplomáticas, mi investigación proporciona un análisis crucial de las herramientas

tecnológicas que permiten a los diplomáticos analizar grandes volúmenes de datos, identificar patrones en tiempo real y prever posibles conflictos o alianzas.

De esta manera, mi trabajo facilita la toma de decisiones en el ámbito diplomático al ofrecer una comprensión más profunda de cómo la IA puede optimizar procesos clave como la negociación, la gestión de crisis y la comunicación internacional. Al proporcionar modelos y ejemplos prácticos de la aplicación de IA en escenarios diplomáticos, mi tesina no solo destaca su importancia teórica, sino que también expone estrategias concretas, lo que permitirá a los profesionales del área comprender la importancia de aggiornarse a la actualidad ya que podrán tomar decisiones más informadas, rápidas y precisas en un entorno cada vez más complejo y dinámico. Este estudio enriquecerá mucho el ámbito académico, no solo a las relaciones internacionales, sino también a la ciencia política, comunicación social, sociología, etc.

Se adoptará una estrategia metodológica que permita una comprensión integral del tema, con el objetivo de construir un marco conceptual sólido que sirva como base para la investigación. La investigación se llevará a cabo utilizando un enfoque cualitativo, considerado el método más adecuado para abordar el problema planteado ya que contribuye a la obtención de evidencia empírica a través de la observación de datos, su interpretación y análisis. Dado los objetivos de este trabajo y los recursos disponibles, las técnicas de recopilación de información se basarán en la revisión de fuentes primarias y secundarias. Esto incluirá una revisión exhaustiva de la bibliografía existente sobre diplomacia digital, IA, ciberseguridad y ética en el uso de la IA. Analizar artículos académicos, libros, informes de organizaciones internacionales y estudios de caso relevantes e identificar las principales teorías, conceptos y debates actuales en el campo. A lo largo de este estudio se expondrán ejemplos concretos de la implementación de la IA en la diplomacia digital para identificar patrones, beneficios y desafíos.

A fin de dar respuesta al problema de investigación, esta tesina se estructura en tres capítulos principales, cada uno de los cuales aborda un aspecto clave de la relación entre la IA y la diplomacia. En el primer capítulo, se explora la manera en la que la IA afectará tanto a la toma de decisiones diplomáticas, eficiencia operacional y comunicación personalizada como redefinirá de las estrategias y tácticas diplomáticas modernas. El segundo capítulo se centra en la ciberseguridad, analizando cómo la IA

está siendo utilizada para detectar y prevenir ciberamenazas en la diplomacia digital, así como los desafíos que esta tecnología plantea. Finalmente, el tercer capítulo aborda el peso de la disparidad en el acceso y uso de la herramienta, sumado a las implicancias éticas, examinando cómo estas cuestiones están influyendo en las relaciones internacionales y en el equilibrio de poder global.

A lo largo de este trabajo, se argumentará que la IA, si bien ofrece oportunidades significativas para mejorar la diplomacia, también plantea desafíos éticos y estratégicos que deben ser abordados con seriedad. Al final, se espera que esta tesina proporcione una visión comprensiva y crítica sobre el papel de la IA en la diplomacia moderna, y ofrezca recomendaciones para su implementación efectiva y responsable.

Marco Conceptual

La diplomacia es un proceso fundamental en las relaciones internacionales que implica la negociación, el diálogo y la resolución de conflictos entre actores estatales y no estatales en la arena mundial. Tradicionalmente, se ha entendido como el arte y la práctica de representar los intereses nacionales en el escenario internacional a través de canales formales e informales de comunicación, con el objetivo de alcanzar objetivos políticos, económicos, sociales y de seguridad (Berridge, 2015).

Desde su concepción clásica hasta la actualidad, la diplomacia ha experimentado una serie de transformaciones significativas, influenciadas por cambios en la estructura del sistema internacional, avances tecnológicos y la evolución de las relaciones internacionales. En sus inicios, la diplomacia se centraba principalmente en las interacciones entre estados soberanos y se caracterizaba por ser una actividad elitista y secreta, donde los diplomáticos representaban los intereses de sus gobiernos en la corte de otros estados (Holbraad, 2006).

La diplomacia se ha ido evolucionando con el fin de poder adaptarse mejor a los cambios coyunturales ya que han surgido en este último tiempo nuevos actores internacionales y nuevas tecnologías que están transformando los métodos tradicionales de diplomacia, evidenciando el dinamismo y la evolución que experimenta el Sistema Internacional. A partir de esto, debemos observar que actores logran posicionarse de manera favorable en esta reestructuración de los escenarios políticos, económicos, sociales y culturales que configuran el nuevo contexto mundial. Con el tiempo, la diplomacia se ha ido desarrollando hacia una práctica más inclusiva y multidimensional, que abarca no solo las relaciones entre estados, sino también las interacciones con actores no estatales.

Según Holmes (2001), este cambio se ha visto impulsado por la globalización, que ha aumentado la interconexión y la interdependencia entre países, así como por la aparición de nuevos desafíos transnacionales, como el cambio climático, el terrorismo y la ciberseguridad.

En la era contemporánea, la diplomacia se ha diversificado para incluir una amplia gama de actividades y herramientas, como la diplomacia pública, la diplomacia

digital, la diplomacia económica y la diplomacia científica. Estos enfoques reflejan la necesidad de adaptarse a un entorno internacional cada vez más complejo y dinámico, donde las fronteras entre lo nacional y lo internacional se vuelven cada vez más difusas (Ferguson, 2016).

Para Bjola, (2018) la diplomacia digital se entiende como al uso de tecnologías para apoyar los objetivos diplomáticos. Es probable que la diplomacia digital logre penetrar la esencia diplomática, esto será posible si los altos funcionarios entienden la aceleración tecnológica como una oportunidad de adaptación proactiva, basada en el ecosistema y enfocada en la red. La diplomacia digital no solo implica transmitir información como era antes, sino también implica escuchar y responder a las preocupaciones y necesidades del público al cual se busca cooptar por medio de nuevas tecnologías.

Dentro de las nuevas herramientas, podemos observar como la IA se ha convertido en una fuerza transformadora en una amplia gama de campos, incluyendo la medicina, la educación, el comercio, la seguridad y las relaciones internacionales. En el contexto de la diplomacia, la IA está siendo utilizada para mejorar la eficiencia y la efectividad de las actividades diplomáticas, proporcionando nuevas herramientas y capacidades para analizar grandes volúmenes de datos, predecir tendencias y comportamientos, y automatizar procesos diplomáticos (Melissen, 2005).

La IA se refiere al desarrollo de sistemas informáticos que pueden realizar tareas que normalmente requieren la inteligencia humana, como el aprendizaje, la percepción, el razonamiento y la toma de decisiones. A diferencia de los sistemas tradicionales de software, los sistemas de IA son capaces de aprender de la experiencia y adaptarse a nuevas situaciones sin intervención humana directa (Russell & Norvig, 2019). La IA ha evolucionado significativamente desde sus inicios, pasando de simples sistemas de reglas a complejos algoritmos de aprendizaje automático y redes neuronales profundas que pueden procesar y analizar grandes volúmenes de datos en tiempo real.

La integración de la IA en la diplomacia digital está dando lugar a lo que se conoce como "diplomacia digital inteligente", que aprovecha las capacidades de la IA para mejorar la toma de decisiones, aumentar la eficiencia y la eficacia de la

comunicación, y fortalecer la capacidad de los actores diplomáticos para adaptarse a un entorno internacional en constante cambio (Wagner, 2019).

Además, la aplicación de la IA en la diplomacia digital incluye varias áreas clave: análisis de datos, comunicación personalizada y automatización de tareas rutinarias. Por ejemplo, los algoritmos de IA pueden analizar grandes conjuntos de datos para identificar tendencias y patrones que informen la toma de decisiones diplomáticas. Además, la IA permite una comunicación más personalizada y efectiva con diferentes públicos a través de canales digitales, adaptando los mensajes en función de las preferencias y comportamientos de los usuarios (Bjola & Holmes, 2015).

No obstante, la IA puede traer consecuencias negativas en el sistema internacional, ya que si bien la implementación de la misma en ciberseguridad puede mejorar la detección y prevención de amenazas, también introduce nuevos riesgos y desafíos que deben ser gestionados cuidadosamente. La ciberseguridad es fundamental en la diplomacia digital debido a la creciente amenaza de ciberataques y espionaje. Según la página oficial de IBM, un ciberataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital. Los actores de amenazas lanzan ciberataques por todo tipo de motivos, desde pequeños robos hasta actos de guerra. Utilizan diversas tácticas para obtener acceso no autorizado a sus sistemas de destino.

La ciberseguridad se refiere a las prácticas y tecnologías diseñadas para proteger las redes, dispositivos y datos de ataques, daños o acceso no autorizado. En el contexto de la diplomacia digital, la ciberseguridad es crucial para proteger la integridad y confidencialidad de la información diplomática. La creciente dependencia de las tecnologías digitales en la diplomacia ha aumentado la vulnerabilidad de los sistemas diplomáticos a ciberataques y espionaje (Gompert, Cevallos, & Libicki, 2014).

La integración de la IA en la ciberseguridad diplomática incluye varias estrategias, como el uso de algoritmos de aprendizaje automático para la detección de anomalías, la implementación de sistemas autónomos para la respuesta a incidentes y el desarrollo de modelos predictivos para anticipar ataques futuros. Sin embargo, también existen riesgos asociados, como la posibilidad de que los sistemas de IA sean

manipulados por atacantes o que introduzcan sesgos en la detección y respuesta a amenazas (Russell & Norvig, 2019).

Por otro lado, existen otra serie de desafíos y dilemas éticos, incluyendo preocupaciones sobre la privacidad, la seguridad, el sesgo algorítmico y la falta de transparencia en el proceso de toma de decisiones (Jobin et al., 2019). Por lo tanto, es fundamental que los actores diplomáticos trabajen en colaboración con expertos en IA y en ética para desarrollar marcos regulatorios y normativos que garanticen un uso responsable y ético de estas tecnologías en el ámbito diplomático (Buchanan et al., 2020).

Además, debemos analizar que el impacto que tendrá la IA irá variando dependiendo de muchos factores ya que existen desigualdades tecnológicas que pueden afectar las relaciones internacionales y el equilibrio de poder global. La capacidad de un estado para adoptar y utilizar la IA en su diplomacia puede depender de su nivel de desarrollo tecnológico, recursos y políticas de innovación (van Dijk, 2020).

Una de las mayores barreras para la adopción de la IA en la diplomacia es la disparidad en el acceso a la tecnología entre diferentes estados. Mientras que algunos países tienen los recursos para desarrollar y utilizar tecnologías avanzadas, otros carecen de las infraestructuras necesarias. Hocking et al. (2012) advierten que esta desigualdad puede exacerbar las diferencias de poder y recursos a nivel internacional, afectando la equidad y justicia en las relaciones diplomáticas.

Kurbalija (2016) sugiere que es fundamental desarrollar estrategias para asegurar que los beneficios de la diplomacia digital sean accesibles para todos los estados, independientemente de su nivel de desarrollo tecnológico. Esto puede incluir iniciativas de cooperación internacional, transferencia de tecnología, capacitación, etc.

La ética de la IA se ocupa de los principios y valores que deben guiar el desarrollo y uso de la IA. En la diplomacia digital, las preocupaciones éticas incluyen la privacidad, el sesgo algorítmico, la transparencia y la rendición de cuentas. Las teorías éticas en este ámbito abogan por un uso responsable y justo de la IA, asegurando que las tecnologías no perpetúen desigualdades ni violen los derechos humanos (Floridi, 2016).

Dentro de las implicaciones éticas, Jobin, Ienca, y Vayena (2019) subrayan la importancia de la transparencia y la responsabilidad en el desarrollo y uso de la IA. Los diplomáticos deben asegurarse de que las decisiones basadas en IA sean explicables y justas, evitando sesgos y discriminación.

La privacidad es otra preocupación ética importante. La recopilación y análisis de grandes volúmenes de datos personales por parte de sistemas de IA pueden invadir la privacidad de los individuos, lo que es especialmente preocupante en contextos diplomáticos donde la información sensible es común. Nye (2011) argumenta que es esencial establecer regulaciones y políticas claras para proteger la privacidad y los derechos humanos en el uso de la IA en la diplomacia.

Capítulo 1: Diplomacia Digital e Inteligencia Artificial

1.1 Impacto de la utilización de la IA en la toma de decisiones diplomáticas, eficiencia operacional y comunicación personalizada

En un entorno donde la información es poder, la implementación de la IA en la diplomacia digital no solo mejora la capacidad de respuesta ante situaciones críticas, sino que también facilita un enfoque más proactivo y estratégico en la gestión de relaciones internacionales.

En este contexto, la IA transforma el proceso de toma de decisiones diplomáticas al mejorar la capacidad para analizar grandes conjuntos de datos de manera eficiente, lo que permite una evaluación más precisa de las posibles consecuencias de cada acción. Como observa Allison (1971), la complejidad inherente a las decisiones en política internacional exige la consideración de múltiples factores interrelacionados. La IA, al agilizar este proceso de análisis y al prever diversos escenarios, facilita el diseño de estrategias diplomáticas más flexibles y eficaces, proporcionando una herramienta poderosa para navegar los retos del entorno global actual.

Las estrategias diplomáticas tradicionales se han basado en la experiencia y el juicio humano, pero la incorporación de la IA introduce un enfoque más *data-driven*. El término "*data-driven*" se refiere a una perspectiva en la toma de decisiones y estrategias que se basa en el análisis y la interpretación de datos. Según Davenport y Harris (2007), este tipo de toma de decisiones se centra en el uso sistemático para guiar las resoluciones estratégicas y operativas en las organizaciones que les permite obtener una visión más clara y precisa de sus operaciones, aumentando la capacidad de respuesta ante cambios en el entorno.

Un caso destacado es la estrategia de Alemania para la gestión de sus relaciones internacionales en el contexto de la crisis de refugiados. Este país ha integrado sistemas de IA para comprender y evaluar datos provenientes de agencias de refugiados, informes de inteligencia y redes sociales. Estos sistemas permitieron identificar patrones

y tendencias emergentes en los flujos migratorios y ajustar las políticas de refugio y ayuda humanitaria en consecuencia (Müller, 2019).

Según Russell y Norvig (2019), el campo del Análisis de la Decisión estudia la aplicación de la teoría de la decisión en problemas actuales. Este campo se utiliza para ayudar a tomar determinaciones razonables en dominios relevantes en los que están en juego intereses importantes, como son el mundo empresarial, gubernamental y legislativo, la estrategia militar, el diagnóstico médico y la salud pública, el diseño en la ingeniería y la gestión de recursos. El proceso incluye un estudio cuidadoso de todas las acciones posibles y sus consecuencias, así como las preferencias planteadas en cada resultado. En la terminología de este campo es habitual distinguir entre el sujeto decisor, que establece preferencias entre los resultados, y el analista de las resoluciones que enumera las acciones y resultados posibles y obtiene preferencias del sujeto para determinar el mejor curso de la acción.

Este análisis se emplea para asegurar que los procesos automáticos operen conforme a las expectativas deseadas. La percepción, en este contexto, proporciona a los agentes de IA la información necesaria sobre el entorno en el que se desenvuelven, mejorando su capacidad de respuesta y adaptación a las cambiantes condiciones del entorno digital. Tal como los sistemas de IA utilizados por empresas como Facebook y Twitter analizan patrones de comportamiento de los usuarios para optimizar la entrega de contenido y mejorar la experiencia del usuario (Smith, 2020).

Sin embargo, no solo las empresas hacen uso de esta tecnología, sino que existen muchos Estados que sacan provecho de estas herramientas, como Japón, que la utiliza para gestionar mejor sus relaciones comerciales internacionales, especialmente en la negociación de tratados de libre comercio. Utilizando análisis predictivo basado en IA, el país anticipó las reacciones de sus socios comerciales a diferentes propuestas, lo que le permite negociar acuerdos más favorables. Además, ayuda a identificar nuevas oportunidades de mercado en función de tendencias económicas globales, fortaleciendo la posición de Japón en el comercio internacional (Yamamoto, 2018).

En las negociaciones internacionales, existen aplicaciones que permiten una mejor adaptación frente a los desafíos actuales a nivel global, posicionando a los Estados en una ventaja competitiva dentro del complejo entorno internacional

ayudándoles a conseguir mayor influencia. Tal como hace la Unión Europea (UE), la Comisión Europea ha implementado sistemas de IA para apoyar las negociaciones comerciales internacionales. La IA se utilizó para analizar documentos complejos y grandes cantidades de datos históricos, estos sistemas simularon diferentes escenarios y predijeron los posibles resultados de las negociaciones, facilitando así una mejor preparación y elección de una manera más informada (European Commission, 2020).

Hoy en día, una enorme cuota de influencia le pertenece a aquel grupo de empresas como Google, Tiktok, Facebook, convirtiéndose en actores de gran envergadura debido a su poder de acción dentro del sistema internacional. Un claro ejemplo es Twitter, Arrosa Soares (2017) con su texto de "Twiplomacia en América Latina" hace alusión a que Twitter es la nueva forma de hacer diplomacia, de forma más directa, transparente y participativa. Ya no basta con que los políticos den lecciones, sino que tienen que responder las cuestiones formuladas por los usuarios y seguidores, en un entorno digital que abrió el escenario internacional a nuevos actores. El uso de Twitter como una herramienta diplomática encaja perfectamente con el nuevo sentido de empoderamiento político que ha acompañado el auge de los medios sociales. Tiene dos grandes efectos positivos en política exterior: fomenta un intercambio fructífero de ideas entre creadores de políticas y sociedad civil y mejora la capacidad de los diplomáticos para recoger información, al igual que para anticipar, analizar y gestionar sucesos y las posibles reacciones ante los mismos.

La utilización de la IA en conjunto con las redes sociales se ha convertido en una fuente inestimable de información, permitiendo la recopilación y análisis de una inmensurable cantidad de datos. Estos datos actúan como predictores conductuales, ofreciendo una representación detallada y precisa de las preferencias y comportamientos de los usuarios. A través del análisis de datos, es posible segmentar a los usuarios y ofrecerles contenido y servicios personalizados que se ajusten a sus necesidades y deseos específicos (Russell & Norvig, 2019).

Debemos tener en cuenta que en la actualidad existen diversos actores con gran influencia; el poder no se encuentra exclusivamente en los Estados. Strange (1996) argumenta que la globalización y la creciente interdependencia económica han erosionado la capacidad de los Estados para controlar sus propias economías y, por extensión, su alcance en la arena internacional. Según esta autora, el poder estructural,

que incluye la capacidad de los Estados para moldear los entornos políticos, económicos y sociales, se ha visto significativamente debilitado. Las instituciones financieras internacionales, las corporaciones multinacionales y otros actores no estatales han ganado prominencia, reduciendo la influencia de los Estados.

Además, Strange (1996) subraya cómo los avances tecnológicos y la liberalización de los mercados financieros han acelerado este proceso de pérdida de control. La movilidad del capital y la velocidad de las transacciones financieras internacionales han desafiado la soberanía estatal, dificultando la capacidad de los gobiernos para implementar políticas económicas independientes y efectivas. Esta transformación ha llevado a una redistribución del poder en la economía política global, donde los Estados ya no son los únicos actores dominantes.

En este contexto, la IA emerge como un nuevo factor que podría exacerbar esta tendencia. La capacidad de la IA para transformar sectores enteros de la economía y de influir en la geopolítica global añade una capa adicional de complejidad a la pérdida de influencia estatal. Los Estados que no logren adaptarse rápidamente a estos cambios tecnológicos corren el riesgo de quedar rezagados, tanto económica como políticamente. La influencia de la IA en el orden mundial refuerza las observaciones de Strange sobre la naturaleza cambiante del poder en el sistema internacional, destacando la necesidad de reevaluar las estrategias de los Estados para mantener su relevancia y autoridad en un entorno global cada vez más dominado por actores no estatales y avances tecnológicos disruptivos.

Desde una perspectiva operativa, el incremento en el número de actores que utilizan la IA, tanto a nivel interno como externo, podría llevar a un aumento en la cantidad de oficinas diplomáticas, ya sea en formato físico o virtual. No obstante, cabe aclarar que este crecimiento en la cantidad de entidades diplomáticas no necesariamente se traducirá en una mejora en la calidad de sus actividades diplomáticas, tanto en las prácticas tradicionales como en aquellas emergentes, como resultado de la aplicación de tecnologías de IA.

Es crucial que los gobiernos no solo se centren en aumentar la cantidad de oficinas diplomáticas potenciadas por IA, sino también en garantizar que estas tecnologías se utilicen responsablemente. La adopción de IA debe ir acompañada de una

formación adecuada para los diplomáticos y la implementación de estándares internacionales que aseguren la calidad y la coherencia de las actividades diplomáticas. De lo contrario, corremos el riesgo de que la IA, en lugar de mejorar la diplomacia, contribuya a la fragmentación y la ineficacia de los esfuerzos diplomáticos globales (Allan, 2018).

Una actividad consular rutinaria, como las solicitudes de visa, difícilmente necesitará modelos predictivos respaldados por algoritmos sofisticados para lograr sus objetivos, pero podría beneficiarse de técnicas de descubrimiento de datos para ayudar con su análisis descriptivo. Al mismo tiempo, las funciones diplomáticas como las negociaciones diplomáticas estarían mejor servidas por simulaciones impulsadas por IA o procesamiento de eventos complejos para navegar y gestionar las incertidumbres políticas utilizando análisis prescriptivos. (Bjola, 2020).

Un ejemplo notable es el uso de IA por parte del Ministerio de Relaciones Exteriores de Japón. En 2019, El país lanzó un sistema basado en IA llamado "*Sakura*," destinado a asistir a los ciudadanos japoneses en el extranjero con servicios consulares a través de un chatbot que responde a consultas frecuentes y proporciona información vital. Este sistema ha mejorado significativamente la eficiencia y rapidez de los servicios consulares, permitiendo una respuesta más ágil en situaciones de emergencia (Ministry of Foreign Affairs of Japan, 2019).

La IA puede ayudar a mejorar la comunicación entre gobiernos y públicos extranjeros al reducir las barreras lingüísticas entre países, mejorar la seguridad de las misiones diplomáticas mediante tecnologías de reconocimiento de imágenes y clasificación de información, y apoyar operaciones humanitarias internacionales al monitorear elecciones, asistir en operaciones de mantenimiento de la paz y asegurar que los desembolsos de ayuda financiera no sean mal utilizados mediante la detección de anomalías (Bjola, 2020).

Hoy en día los datos se han convertido en el "nuevo petróleo", donde la recopilación de datos se asemeja a una “carrera armamentista”, en la que no solo se trata de obtener información, sino de saber cómo utilizarla de manera efectiva. La capacidad de clasificar a las personas en diferentes categorías permite enviar mensajes específicos a través de correos electrónicos, publicidad y redes sociales, con el objetivo de influir

psicológicamente en grupos determinados (Kaiser, 2019). La IA facilita la personalización de la comunicación diplomática, adaptando los mensajes y la interacción con diferentes audiencias (Manor, 2019)

La personalización de contenidos está estrechamente vinculada con la microsegmentación del público. El *big data* facilita la especialización de los temas mediante el análisis de las audiencias en función de variables como edad, género, ocupación e intereses, dirigidos a grupos específicos dentro de su público objetivo. Los resultados serán óptimos si los datos recogidos son de alta calidad y, en particular, si han sido proporcionados por los propios usuarios. Esto garantiza que la información sea precisa y relevante, lo que a su vez mejora la eficacia de las estrategias de comunicación.

Podemos observar cómo de manera progresiva, la utilización estratégica de los medios digitales en los procesos electorales se ha convertido en una práctica cada vez más común. Este fenómeno ha dado lugar a una dinámica innovadora, transformando la naturaleza de las estrategias políticas. Los profesionales emergentes en este campo han desarrollado tácticas con una lógica distinta a la que predominaba en los medios masivos tradicionales (Shmargad & Sanchez, 2022).

Mientras que la publicidad tradicional se ha centrado en construir marcas y proporcionar pruebas sociales, hoy en día, con el masivo acceso a internet, existe una mayor capacidad de cooptación y manipulación de comportamientos. Este nuevo panorama digital ofrece tanto oportunidades como desafíos (Kaiser, 2019).

Según Bjola, se espera que la influencia de las tecnologías digitales en la diplomacia pública maximice el interés en aprender. A medida que el volumen de interacciones basadas en datos sigue creciendo a un ritmo exponencial, uno puede hacerse escuchar aprendiendo profesionalmente cómo separar las “señales” del “ruido” de fondo y ajustando proactivamente su mensaje para garantizar la máxima visibilidad en el espacio en línea, en tiempo real. Hacerse escuchar requeriría, por extensión, una mejor comprensión de los marcos cognitivos y los matices emocionales que permiten a las audiencias conectarse significativamente con un mensaje particular. Hacerse seguir implicaría conexiones a nivel micro con la audiencia basadas en intereses y preferencias individuales.

Esta evolución ha permitido la creación de campañas aprovechando el vasto potencial de los datos y las tecnologías digitales para captar y movilizar a los electores. Así, se ha consolidado una nueva era en la comunicación política, caracterizada por la interactividad, la personalización y la rapidez en la difusión de mensajes, lo que ha transformado significativamente la dinámica electoral global.

Para que la personalización de contenidos y la segmentación precisa de audiencias sean realmente receptivas, es fundamental que haya una buena calidad de datos. Al vincular la información requerida, las organizaciones pueden desarrollar campañas que no solo lleguen a su público objetivo, sino que también resuenen de manera significativa con cada grupo.

La campaña presidencial de Barack Obama en 2008 es un ejemplo destacado de la utilización estratégica de los medios digitales en los procesos electorales. Esta campaña se resalta por su innovador uso de internet y las redes sociales para movilizar y conectar con los votantes de una manera sin precedentes. Utilizaron plataformas como Facebook, Twitter y YouTube para difundir mensajes, organizar eventos y recaudar fondos, lo que permitió una gran participación y un alcance masivo. Además, la campaña empleó técnicas avanzadas de análisis de datos y micro-segmentación para personalizar mensajes y optimizar las estrategias de comunicación, como en el *targeting*. Como señalan Kotler, Kartajaya y Setiawan (2017), el targeting digital se refiere a la práctica de dirigir mensajes y contenidos específicos a un público particular basado en datos demográficos, comportamentales y de interés. Permite a las empresas dirigir sus mensajes de manera más precisa a segmentos específicos de consumidores, logrando una mejor llegada en las campañas publicitarias. Esta estrategia permite a las empresas y campañas políticas personalizar sus mensajes para maximizar la relevancia y efectividad.

La campaña de Obama utilizó herramientas de análisis de datos para entender mejor las preferencias y comportamientos de los votantes. Esto incluía el uso de software de análisis de datos para identificar segmentos específicos de la población que posiblemente serían más receptivos a ciertos mensajes. La estrategia se basó en la creación de contenido viral y en la interacción directa con los votantes a través de medios digitales, lo que aumentó significativamente la participación y el compromiso de los ciudadanos. Además, estableció un precedente para futuras campañas políticas,

demostrando cómo el uso estratégico de los medios digitales puede transformar la dinámica electoral (Plouffe, 2009).

Los medios masivos son clave para posicionar agendas públicas, pero también para promover carreras políticas personales. En la disputa por los poderes públicos, la estrategia mediática que adoptaran los competidores podría ser clave en su triunfo (Castells, 2010).

En conclusión, la integración de la IA en el entorno diplomático ha traído consigo nuevas herramientas que abren las puertas a posibilidades de optimizar y mejorar tanto para la toma de decisiones como para la eficiencia operativa y comunicación personalizada. Sin embargo, esto no significa que puede ser utilizada de manera beneficiosa en cualquier momento, sino que debemos aprender a utilizarla propiamente y en circunstancias adecuadas. La tecnología debe adaptarse a las necesidades diplomáticas, permitiendo a los Estados aprovechar sus beneficios sin comprometer los principios diplomáticos. Además, la integración de la IA en la diplomacia puede otorgar un papel más visible y significativo a los diplomáticos, al proporcionarles herramientas avanzadas para el análisis de datos y la previsión de escenarios, lo que podría mejorar la toma de decisiones y la formulación de políticas (Johnson, 2021). En última instancia, el reto radica en equilibrar el uso de la IA con la necesidad de mantener un enfoque humano y estratégico en la diplomacia.

1.2 El papel de la IA en la redefinición de las estrategias y tácticas diplomáticas modernas

Dentro de la gran distinción entre poder duro y poder blando, el poder blando ha adquirido una relevancia significativa en la diplomacia moderna. A diferencia del poder duro, que se basa en la coerción y la fuerza, el poder blando se centra en la influencia y persuasión a través de medios no coercitivos, como la cultura, los valores y la comunicación estratégica (Nye, 2004). Hoy en día, el poder blando ofrece a los Estados la posibilidad de impactar psicológicamente a audiencias internacionales de manera más sutil pero efectiva. Esta capacidad psicológica permite que las estrategias diplomáticas se diseñen para moldear percepciones, fomentar relaciones positivas y promover intereses nacionales sin recurrir a la presión directa.

La IA juega un papel crucial en la potenciación del poder blando al permitir un análisis más detallado de las audiencias y el diseño de estrategias altamente personalizadas. Según Miranda (2017), el poder blando se basa en la capacidad de un actor para atraer y persuadir a otros, logrando así modificar su comportamiento en situaciones específicas. La concreción de iniciativas y acciones en el ámbito internacional refleja el nivel de influencia política de un país, que puede ser importante, moderado o nulo. En este contexto, la IA se convierte en una herramienta esencial para aumentar dicha influencia al permitir una adaptación más precisa de las estrategias diplomáticas, optimizando el impacto y la eficacia de las políticas en función de los objetivos geopolíticos de un Estado.

Los países que lideran en materia de IA pueden emplear estas tecnologías para fortalecer su poder blando y duro, aumentando su influencia en la escena internacional. La capacidad de desarrollar y utilizar tecnologías avanzadas de IA puede traducirse en ventajas estratégicas en áreas como la ciberseguridad, la inteligencia militar y la diplomacia digital. En contraste, los países con acceso limitado a la IA pueden encontrar difícil mantener la soberanía digital y proteger sus intereses nacionales en un mundo cada vez más interconectado y dependiente de la tecnología (Kostka & Gkritzali, 2020).

Corea del Sur es un excelente ejemplo de cómo un país que lidera en IA puede hacer uso de estas tecnologías para fortalecer su poder blando y duro, aumentando su influencia en la escena internacional. Por un lado, ha utilizado su avance en IA para promover su cultura y educación a nivel global. A través de la exportación de su tecnología y el establecimiento de centros de investigación en IA en países aliados, Corea del Sur ha incrementado su presencia cultural y educativa en el extranjero. La creación de "Korean Cultural Centers" y "K-pop AI Music" han ayudado a proyectar la cultura surcoreana en el escenario global, fomentando un efecto de poder blando significativo (Kim, 2021).

El país también ha sido proactivo en la creación de plataformas y foros internacionales para discutir el futuro de la IA. Corea del Sur ha organizado y participado en conferencias globales sobre IA, ofreciendo sus avances tecnológicos y su experiencia para colaborar en la formulación de normas y políticas internacionales. Estas acciones han mejorado su reputación como líder en innovación y cooperación global (Choi & Lee, 2022).

Por el otro lado, en términos de poder duro, Corea del Sur ha integrado la IA en sus sistemas de defensa y seguridad nacional. El país ha desarrollado tecnologías avanzadas de IA para la vigilancia y la ciberseguridad, lo que le permite mejorar sus capacidades militares y de inteligencia. El uso de IA en sistemas de misiles y en la vigilancia fronteriza ha fortalecido su capacidad de respuesta y defensa (Lee & Kim, 2020).

Además, la inversión en IA ha permitido a Corea del Sur competir de manera más efectiva con otras potencias tecnológicas, como China y Estados Unidos. Su habilidad para desarrollar y aplicar tecnologías avanzadas de IA ha generado una ventaja estratégica en sectores clave como la tecnología militar y la infraestructura crítica (Park, 2021).

En la diplomacia digital, la IA se ha convertido en una herramienta indispensable no solo para aumentar la influencia de un país, sino también para dotar a los altos funcionarios de la capacidad de evaluar de manera más precisa el impacto de sus políticas, anticipar crisis y seguir de cerca las tendencias globales. En un entorno internacional caracterizado por su alta complejidad y dinamismo, la capacidad de responder de forma ágil y eficaz es fundamental para mantener una posición competitiva en el escenario global. La IA, con su capacidad predictiva, permite anticipar movimientos geopolíticos y económicos, lo que no solo facilita la creación de estrategias mejor informadas, sino que también ofrece la posibilidad de medir con mayor exactitud el impacto de las políticas implementadas.

China ha sido pionera en la utilización de sistemas avanzados de IA para evaluar una amplia gama de datos provenientes de diversas fuentes, tales como redes sociales, medios de comunicación, indicadores económicos y movimientos del mercado financiero. Estos sistemas permiten al gobierno chino prever tendencias y eventos geopolíticos y económicos con una anticipación significativa, lo que les otorga una ventaja estratégica en la formulación de políticas. Un proyecto destacado en este ámbito es el desarrollado por el Centro de Investigación en Inteligencia Artificial de la Universidad de Tsinghua. Este centro ha implementado modelos predictivos basados en *machine learning* y análisis de *big data* que son capaces de identificar patrones complejos y prever cambios en la política internacional, flujos comerciales y movimientos en el mercado financiero (Wang et al., 2020).

La capacidad de anticipación proporcionada por estos modelos ha sido crucial para China en varios aspectos clave de su política exterior. En la gestión de inversiones extranjeras, estos modelos han permitido al gobierno chino identificar mercados emergentes y sectores estratégicos para invertir, minimizando los riesgos y maximizando los beneficios. Asi como, mediante el uso de algoritmos avanzados, China ha podido adaptar su narrativa diplomática para alinearse mejor con las preocupaciones y valores de audiencias específicas en África, América Latina y el sudeste asiático, fortaleciendo así sus lazos con estas regiones y aumentando su influencia global. Este enfoque no solo ha mejorado la imagen de China en el extranjero, sino que también ha permitido al país construir alianzas estratégicas más sólidas y duraderas (Zhang & Li, 2020).

En cuanto al manejo de crisis, los sistemas de IA también pueden ser de gran ayuda estratégica para los funcionarios diplomáticos, proporcionando un análisis descriptivo más detallado y la capacidad de identificar posibles escenarios futuros con mayor claridad. Estos sistemas pueden simular diversas situaciones, ofreciendo una visión más amplia y detallada de las posibles ramificaciones de diferentes acciones. Sin embargo, presenta un desafío adicional debido a su inherentemente alto nivel de incertidumbre y la necesidad de rendir cuentas rápidamente. Como señala Bjola (2020), este ámbito requiere una evaluación continua de riesgos y una adaptación constante a nuevas informaciones, lo que limita el potencial de la IA para ofrecer soluciones definitivas en situaciones de crisis.

Asimismo, podemos observar en Estonia, donde la IA se ha integrado en la diplomacia pública y la gestión de crisis. El Ministerio de Asuntos Exteriores de este país ha adoptado soluciones de IA para monitorear las redes sociales y el flujo de información, identificando rápidamente desinformación y propaganda hostil. Estas capacidades permiten a Estonia reaccionar ante crisis informativas y mejorar la comunicación pública. La utilización de IA en este contexto ha fortalecido la capacidad del Estado para gestionar crisis diplomáticas y ha optimizado su estrategia de comunicación externa (Ministry of Foreign Affairs of Estonia, 2020).

Además, la implementación de IA en el análisis de redes sociales tiene implicaciones significativas para la diplomacia y la gestión de crisis. Los gobiernos y organizaciones internacionales utilizan IA para monitorear conversaciones y tendencias

en redes sociales, permitiendo una detección temprana de conflictos potenciales y desinformación. Esta capacidad de respuesta rápida y precisa es esencial para gestionar crisis diplomáticas y mantener la estabilidad política. La información obtenida a través de IA y redes sociales permite a los diplomáticos y responsables de políticas anticipar y mitigar riesgos, así como formular mejores estrategias (Johnson, 2021).

Por otro lado, la utilización de algoritmos de IA en la monitorización de medios sociales ha permitido a los diplomáticos identificar temas emergentes y opiniones públicas relevantes, mejorando así la capacidad de respuesta diplomática. Un ejemplo destacado es el caso de Israel, donde el Ministerio de Asuntos Exteriores ha implementado herramientas de IA para analizar y monitorear las conversaciones en redes sociales sobre temas relacionados con la seguridad y las relaciones internacionales. Esta tecnología ha permitido al país anticipar reacciones internacionales ante decisiones políticas y ajustar su estrategia diplomática en consecuencia, mejorando su capacidad para gestionar crisis y mantener una imagen positiva en el escenario global (Cohen, 2019).

La implementación de estas tecnologías transforma la manera en que se gestionan las relaciones internacionales; este cambio refleja una dependencia creciente en las tecnologías avanzadas que comienzan a tener los diversos Estados para gestionar y anticipar eventos, optimizando así las estrategias en diversos campos. Por lo tanto, el uso de IA en la formulación de políticas y estrategias no solo es una tendencia en alza, sino una necesidad en un mundo cada vez más interconectado y complejo.

De la misma manera en que se aprovechaban nuevas estrategias para consolidar comunidades virtuales que ayudarán a posicionar y socializar ciertos mensajes, también comenzaron a surgir tácticas en las que de manera deliberada se hacía uso de la desinformación (Shu et al., 2020). En otras palabras, "f*ake news*", el término se refiere a noticias falsas o información engañosa que se presenta como noticia legítima con el objetivo de influir en la opinión pública o engañar a las personas. Según Allcott y Gentzkow (2017), las *fake news* son artículos de noticias que son intencionalmente y verificablemente falsos, y que posiblemente inducían a error a los lectores. Este fenómeno ha ganado prominencia con la proliferación de las redes sociales y el acceso generalizado a plataformas digitales, lo que facilita la difusión rápida y amplia de información falsa. Podemos observar un ejemplo en las elecciones presidenciales de

Estados Unidos en 2020, la propagación de *fake news* en redes sociales se convirtió en un desafío significativo para la integridad del proceso electoral. En respuesta a esta problemática, varias organizaciones y plataformas tecnológicas emplearon IA para identificar y mitigar la difusión de desinformación.

Un estudio destacable sobre este tema es el realizado por Kleinberg, Roth, y Zhang (2020), publicado por la Cornell University. Éste se centra en el uso de técnicas avanzadas de aprendizaje automático para rastrear y analizar la propagación de noticias falsas en Twitter durante el periodo electoral. El equipo de investigación implementó algoritmos de IA diseñados para detectar patrones de difusión que indican la presencia de información engañosa. Estos algoritmos fueron entrenados para identificar características específicas asociadas con *fake news*, como el uso de lenguaje sensacionalista, la falta de fuentes confiables y la rápida viralización de contenidos.

La investigación demostró cómo la IA permite a los equipos de verificación de hechos y a las plataformas de redes sociales identificar rápidamente contenido falso o engañoso. Los algoritmos no solo detectaron noticias falsas, sino que también ayudaron a rastrear la forma en que estas noticias se difundían a través de diferentes redes y usuarios, proporcionando una visión integral de las dinámicas de desinformación.

Además, el estudio mostró que la implementación de IA no solo facilitó la detección de noticias falsas, sino que también permitió una respuesta más rápida para contrarrestar la desinformación antes de que pudiera afectar gravemente la opinión pública y el proceso electoral. Esto incluyó la eliminación de publicaciones engañosas, la advertencia a los usuarios sobre la información falsa y la promoción de contenido verificado y preciso.

Mediante el uso de algoritmos avanzados y técnicas de análisis de datos, los diplomáticos pueden identificar y entender mejor los valores, intereses y comportamientos de sus audiencias. Esto facilita la creación de mensajes y campañas que resuenen profundamente con los públicos internacionales, logrando un impacto psicológico que puede ser decisivo en la formación de alianzas y en la influencia de políticas extranjeras (Floridi, 2016).

No obstante, la capacidad de segmentar audiencias y dirigir mensajes específicos plantea el riesgo de que la información compartida por los usuarios en redes sociales sea

utilizada con fines políticos sin su consentimiento. Este uso potencialmente invasivo de los datos personales ha suscitado intensos debates sobre la ética de los algoritmos y la responsabilidad en la gestión de la información. Existe la preocupación de que la información compartida por los usuarios en redes sociales pueda ser utilizada con fines políticos sin su consentimiento, planteando serias cuestiones sobre la privacidad y el uso responsable de los datos personales. El caso de Cambridge Analytica se ha convertido en un ejemplo paradigmático de cómo el uso de *big data* y técnicas avanzadas de análisis pueden influir en las campañas políticas y en los procesos electorales. Cambridge Analytica, una empresa de análisis de datos, fue ampliamente criticada por su papel en la campaña del Brexit en el Reino Unido y en la elección presidencial de Donald Trump en 2016 (Kanakia et al., 2019; ur Rehman, 2019). Utilizando datos obtenidos sin el consentimiento explícito de los usuarios, la empresa implementa estrategias de *microtargeting* que permitieron dirigir mensajes altamente personalizados a segmentos específicos de la población. Este enfoque no solo maximiza el impacto de las campañas al adaptar el contenido a las preferencias y comportamientos de los votantes, sino que también exacerbó la polarización política al enfocar las campañas en las divisiones sociales existentes.

El uso de *big data* en estos contextos permitió a Cambridge Analytica procesar y analizar información para predecir y manipular el comportamiento electoral. Esta capacidad de análisis predictivo se basa en la recopilación de datos detallados sobre las preferencias, comportamientos y creencias individuales, lo que facilita la formulación de estrategias de comunicación política altamente específicas y efectivas (Ceron et al., 2016). La prospectiva sobre el comportamiento de los electores se vuelve crucial en un momento de alta polarización social e ideológica, donde la capacidad de identificar y explotar divisiones puede determinar el éxito de una campaña (Zhukov et al., 2022).

Este caso, además, subraya la necesidad de un enfoque ético en la aplicación de técnicas de análisis de datos en la política. La controversia sobre la explotación de datos personales sin consentimiento y el impacto en la privacidad de los usuarios ha generado un debate significativo sobre las prácticas responsables en la gestión de información. La experiencia destaca la importancia de implementar regulaciones y salvaguardas que protejan la privacidad y promuevan el uso ético de los datos en la formulación de estrategias políticas y electorales (Kanakia et al., 2019; ur Rehman, 2019).

El impacto del *big data* y la capacidad de segmentación avanzada no se limitan únicamente a las campañas políticas; también tienen implicaciones más amplias para la gestión de conflictos y la prevención de crisis. La alta capacidad de segmentación de datos permite a las organizaciones no solo influir en votantes indecisos, sino también identificar y abordar patrones emergentes que podrían desencadenar tensiones sociales. Por ejemplo, el seguimiento preventivo de datos sobre discursos de odio y otros indicadores en plataformas sociales como Twitter puede proporcionar a las organizaciones de paz y a los responsables de políticas la información necesaria para intervenir de manera temprana en sociedades de alto riesgo (Kaiser, 2019).

Este tipo de análisis puede prevenir violaciones de derechos humanos y evitar conflictos bélicos. El seguimiento de discursos de odio en plataformas sociales puede proporcionar información valiosa para intervenir de manera temprana en sociedades de alto riesgo. Un estudio de la organización *Global Voices* mostró que el análisis de datos de redes sociales puede identificar señales tempranas de conflictos potenciales y violaciones de derechos humanos, facilitando la intervención antes de que los problemas se agraven (Global Voices, 2022).

Un caso ilustrativo es el análisis realizado durante el conflicto en Myanmar en 2018, donde se identificaron mensajes incendiarios dirigidos contra la comunidad rohingya. La detección temprana de estos discursos de odio permitió que Facebook coordinará esfuerzos con plataformas tecnológicas y actores locales para mitigar la propagación del odio y prevenir una escalada del conflicto. Facebook eliminó varias cuentas y páginas web que pertenecían a miembros del Ejército de Myanmar. La empresa anunció la estrategia poco después de que una misión de reconocimiento de Naciones Unidas acusó al Ejército de Myanmar de cometer genocidio en el Estado de Rakáin, donde los ataques contra los musulmanes rohinyá causaron la migración masiva de unas 700 000 personas en 2017 (Mong Palatino, 2018).

En conclusión, aunque el avance en la segmentación y análisis de datos ha abierto nuevas posibilidades para la comunicación política y la gestión de conflictos, también plantea desafíos significativos en términos de ética y privacidad. La implementación responsable de estas tecnologías es esencial para equilibrar el potencial de impacto positivo con la necesidad de proteger los derechos individuales y evitar abusos. A medida que la IA y el *big data* continúan evolucionando, será crucial

desarrollar marcos éticos y legales robustos que garanticen el uso responsable de estas herramientas en todos los ámbitos, desde la política hasta la prevención de conflictos internacionales.

Capítulo 2: Ciberseguridad

2.1 Beneficios de la inteligencia artificial en la detección y prevención de ciberamenazas en la diplomacia digital

En la actualidad, la seguridad de la información se ha convertido en un pilar fundamental para la diplomacia donde la IA tiene la capacidad de detectar y prevenir ciberamenazas, aportando herramientas avanzadas que mejoran significativamente la capacidad de los gobiernos para protegerse contra ataques cibernéticos, analizando vastas cantidades de datos en tiempo real, identificar patrones sospechosos y predecir posibles amenazas antes de que estas se materialicen (Choucri, Madnick, & Ferwerda, 2021). Esta capacidad de anticipación permite a los estados implementar medidas preventivas y responder de manera más efectiva a las amenazas emergentes, fortaleciendo la seguridad de sus comunicaciones y operaciones diplomáticas (Allan, 2018).

Sumado a esto, al implementarse IA en la diplomacia digital se optimiza la gestión de incidentes y la recuperación ante ataques. Gracias a algoritmos avanzados de aprendizaje automático, estas herramientas pueden identificar rápidamente vulnerabilidades en los sistemas, facilitar la creación de parches de seguridad y coordinar respuestas (Bjola, 2018). Además, estas tecnologías permiten el monitoreo continuo de las redes diplomáticas, lo que reduce significativamente el riesgo de intrusiones no detectadas. En un entorno global cada vez más interconectado y digitalizado, estos beneficios son esenciales para mantener la integridad y la confianza en las relaciones internacionales (Brynjolfsson & McAfee, 2021).

Esta capacidad para detectar anomalías permite a las organizaciones diplomáticas anticiparse a los ataques y tomar medidas preventivas antes de que se produzcan daños significativos. Tal como los algoritmos de aprendizaje automático pueden monitorear el tráfico de red y detectar desviaciones que sugieren la presencia de

malware o intentos de intrusión (Smith, 2019). El *malware*, o software malicioso, engloba una variedad de programas diseñados para infiltrarse, dañar o comprometer la integridad de sistemas informáticos y redes. Según la definición de la National Institute of Standards and Technology (NIST), incluye cualquier software creado con la intención de dañar orealizar acciones no autorizadas dentro de un sistema informático (NIST, 2020)

Un estudio realizado por Huang y Dong (2019) demostró que el uso de técnicas de aprendizaje profundo puede mejorar significativamente la precisión en la detección de amenazas, reduciendo el tiempo de respuesta y minimizando el impacto de los ataques. Además, sistemas avanzados de análisis predictivo, como los desarrollados por empresas líderes en ciberseguridad, permiten una vigilancia continua y adaptativa, ajustándose a nuevas amenazas y mejorando constantemente su eficacia (Zhang et al., 2020). Esta capacidad no solo mejora la seguridad de las redes diplomáticas, sino que también protege la integridad de la información sensible y la continuidad de las operaciones diplomáticas.

Cada vez existen más Estados que buscan utilizar estos beneficios a su favor. En particular, el gobierno de Israel es reconocido por su avanzada infraestructura de ciberseguridad, que incluye el uso de IA para proteger sus sistemas diplomáticos y gubernamentales. El gobierno israelí utiliza tecnologías de aprendizaje automático y análisis de datos para identificar y neutralizar ciberamenazas. Ha implementado sistemas de detección de intrusiones basados en IA que analizan continuamente el tráfico de red y alertan sobre actividades anómalas o sospechosas. La colaboración entre el sector público y privado en el país ha sido clave para el desarrollo de soluciones innovadoras en ciberseguridad. Esta colaboración ha permitido no solo proteger sus propias redes, sino también ofrecer su expertise en ciberseguridad a otros países, fortaleciendo así su posición diplomática en el ámbito global (Tirosh & Yelin, 2020).

La IA puede analizar vastas cantidades de datos en tiempo real, detectando patrones y comportamientos anómalos que estarían en condiciones de indicar una amenaza cibernética. Según un informe de Accenture (2019), el uso de la misma en la ciberseguridad ha mejorado significativamente la capacidad de respuesta ante incidentes, reduciendo el tiempo de detección de amenazas en un 11% y el tiempo de respuesta en un 12%.

En cuanto a la lucha contra el cibercrimen, Estonia es un ejemplo notable de un país que ha utilizado la IA para contrarrestar este fenómeno de manera eficaz. El país, uno de los países más digitalizados del mundo, ha desarrollado una infraestructura robusta de ciberseguridad. La introducción de soluciones basadas en IA le ha permitido no solo identificar amenazas de manera más rápida y precisa, sino también responder de mejor forma a posibles vulnerabilidades antes de que sean explotadas (Kaska, Tali, & Vihul, 2013).

La adopción de la IA en el ámbito de la ciberseguridad en Estonia incluye sistemas de análisis de comportamiento que monitorizan las redes, identificando patrones inusuales que serían capaces de indicar un ciberataque. Estos sistemas utilizan algoritmos de aprendizaje automático para evaluar información y detectar anomalías que eventualmente pasarían desapercibidas con métodos tradicionales. Además, ha implementado sistemas de alerta temprana que notifican a las autoridades pertinentes sobre posibles amenazas, permitiendo una respuesta rápida y coordinada (Rikk & Kont, 2018).

Por otro lado, un punto importante a tener en cuenta es la evaluación y mitigación de riesgos en infraestructuras críticas. Cuando hablamos de las infraestructuras críticas, nos referimos a redes eléctricas, sistemas de transporte, suministro de agua, y comunicaciones; son objetivos frecuentes de ciberataques debido a su importancia estratégica y a su potencial para causar disrupciones significativas. La IA puede proporcionar herramientas avanzadas para la evaluación de riesgos y la detección temprana de amenazas.

Los sistemas basados en IA pueden monitorizar continuamente el estado de las infraestructuras críticas, identificar patrones anómalos y predecir posibles fallos o ataques antes de que ocurran. En Singapur, la Agencia de Seguridad Cibernética ha implementado soluciones de IA para proteger sus infraestructuras críticas. Estas herramientas permiten una vigilancia constante y la capacidad de responder rápidamente a incidentes de seguridad, minimizando el impacto potencial (Cyber Security Agency of Singapore, 2021).

Esta herramienta tecnológica puede ayudar a desarrollar estrategias de mitigación más efectivas. Mediante simulaciones y modelos predictivos, los sistemas de

IA pueden evaluar diferentes escenarios de ataque y proponer medidas preventivas para reducir los riesgos. Esto es especialmente útil para preparar a las organizaciones y gobiernos para responder a incidentes cibernéticos de manera más coordinada y eficiente (Feldmann et al., 2019). En Alemania, el Centro Nacional para la Protección de Infraestructuras Críticas la utilizan para evaluar riesgos y diseñar planes de respuesta que involucran a múltiples actores, incluyendo sectores públicos y privados, asegurando una defensa más integrada (BBK, 2021).

Asimismo, es posible mejorar significativamente la capacidad de respuesta ante incidentes ya que al automatizar procesos y proporcionar análisis avanzados en tiempo real, la IA permite una reacción más rápida y eficiente a los ciberataques, minimizando así el impacto potencial en la diplomacia digital y en la seguridad de la información.

Los sistemas basados en IA pueden monitorear continuamente las redes y detectar actividades sospechosas de inmediato. Cuando se identifica una amenaza, estos sistemas pueden generar alertas y activar protocolos de respuesta previamente establecidos. A modo de ejemplo, el Centro Nacional de Ciberseguridad (NCSC) del Reino Unido ha adoptado tecnologías de IA para monitorear y analizar amenazas cibernéticas. Este enfoque incluye el uso de algoritmos de aprendizaje automático que detectan actividades inusuales y potencialmente peligrosas en redes gubernamentales y diplomáticas. El NCSC la utiliza para analizar patrones de tráfico de red y detectar comportamientos anómalos que eventualmente indicarían intentos de intrusión o ciberataques. La colaboración entre este y empresas privadas, así como instituciones académicas, ha sido fundamental para mejorar continuamente sus capacidades de ciberseguridad mediante la integración de nuevas tecnologías. Esta colaboración ha permitido al Reino Unido mantener una posición avanzada en la protección de sus sistemas diplomáticos y de seguridad (NCSC, 2020).

Además, IBM Security ha implementado su sistema *Watson for Cyber Securit*y, que utiliza capacidades de aprendizaje automático para revisar datos sobre hechos pasados y extraer conocimientos relevantes. Este sistema no solo ayuda a identificar tendencias y patrones en los ataques, sino que también proporciona recomendaciones basadas en datos históricos para optimizar las respuestas futuras. Al integrar estas recomendaciones en los protocolos de seguridad, las organizaciones pueden adaptar sus estrategias de respuesta y reducir el riesgo de futuros incidentes (IBM Security, 2021).

Asimismo, facilita la coordinación entre diferentes equipos y agencias mediante plataformas de colaboración basadas en IA, se puede compartir información y cooperar en acciones de respuesta de manera más eficiente. Esto es especialmente importante en el ámbito de la diplomacia digital, donde los ciberataques pueden tener implicaciones internacionales. Específicamente, la Organización del Tratado del Atlántico Norte (OTAN) ha implementado tecnologías de IA para mejorar la colaboración entre sus países miembros en la gestión de amenazas cibernéticas. La plataforma de colaboración de ciberseguridad de la OTAN, respaldada por IA, facilita la comunicación y la coordinación de acciones durante un problema cibernético. Esta coordinación es vital para enfrentar amenazas que pueden tener implicaciones globales, permitiendo a los países miembros compartir información crítica y crear estrategias de respuesta de manera eficiente (OTAN, 2021). La capacidad de esta para integrar y analizar datos provenientes de diversas fuentes contribuye a una respuesta más cohesionada ante ciberataques, fortaleciendo la resiliencia colectiva frente a amenazas cibernéticas.

Por otro lado, también tiene un gran impacto a nivel interno, donde estas pueden surgir de empleados descontentos, errores humanos, o incluso agentes malintencionados que tienen acceso a información sensible. La IA permite a las organizaciones identificar comportamientos sospechosos y prevenir posibles filtraciones de datos antes de que ocurran.

Una de las herramientas más avanzadas en este ámbito es el sistema de detección de anomalías basado en IA. Plataformas como *Varonis* utilizan algoritmos de aprendizaje automático para monitorear continuamente el comportamiento de los usuarios dentro de una red. Estos sistemas pueden identificar desviaciones significativas en los patrones de uso, como accesos inusuales a archivos confidenciales o transferencias de datos fuera del horario laboral. Cuando se detectan comportamientos que se desvían de la norma, el sistema genera alertas automáticas para que los equipos de seguridad sean aptos para investigar y tomar medidas preventivas. (Varonis, 2022).

Además, la IA puede ser utilizada para fortalecer la vigilancia de la comunicación interna y los accesos a sistemas críticos. Un ejemplo significativo es el uso de *Darktrace*, una plataforma que emplea técnicas de aprendizaje automático para crear un perfil de comportamiento normal para cada usuario en una red. Cuando un usuario comienza a actuar de manera que no coincide con su perfil establecido, como

realizar búsquedas inusuales o acceder a datos que no son pertinentes a su rol, Darktrace genera alertas que permiten a los equipos de seguridad intervenir antes de que se produzca un daño. Este tipo de tecnología también es capaz de identificar patrones de ataque que podrían ser indicativos de una amenaza interna que intenta evadir la detección (Darktrace, 2021).

El fortalecimiento de las medidas de seguridad interna mediante el uso de IA también se refleja en las estrategias de respuesta a incidentes. Los sistemas pueden integrar datos de diversas fuentes, como correos electrónicos, registros de acceso y comunicaciones internas, para proporcionar una visión holística del contexto de una amenaza interna. Esta integración facilita una respuesta más coordinada y efectiva, permitiendo a las organizaciones implementar medidas correctivas rápidamente y minimizar el impacto potencial de las amenazas internas (Gartner, 2021).

Por lo tanto, aunque la IA ofrece herramientas poderosas para mejorar la ciberseguridad, también plantea nuevos desafíos que requieren enfoques innovadores y una vigilancia constante. La lucha contra las amenazas cibernéticas debe adaptarse continuamente para abordar tanto las oportunidades como los riesgos que trae consigo.

Debemos tener en cuenta que la colaboración internacional y la compartición son de gran ayuda para mitigar los efectos negativos. En un mundo cada vez más interconectado, los ataques cibernéticos a menudo trascienden fronteras nacionales, lo que hace esencial una respuesta coordinada a nivel global. La IA puede facilitar enormemente esta cooperación al permitir el intercambio rápido y eficiente de datos relevantes sobre amenazas entre diferentes países y organizaciones. Herramientas basadas en IA pueden analizar datos recopilados de diversas fuentes internacionales y generar alertas sobre posibles amenazas emergentes en tiempo real. Por ejemplo, la Unión Europea ha implementado sistemas de IA para compartir información sobre ciberamenazas entre sus estados miembros, lo que ha resultado en una mejora significativa en la detección y respuesta a ataques cibernéticos (EU Agency for Cybersecurity, 2020). Además, plataformas de colaboración como el Foro Mundial de Ciberseguridad (WCF) utilizan la misma para analizar tendencias globales en ciberseguridad y compartir mejores prácticas entre las naciones participantes (WCF, 2021). Este enfoque colaborativo no solo fortalece las capacidades de defensa de cada país, sino que también crea una red de seguridad más robusta y resiliente.

La integración de sistemas de información para la coordinación internacional es un componente esencial en la detección y prevención de ciberamenazas en la diplomacia digital. Los ciberataques no conocen fronteras y, a menudo, involucran a actores de múltiples países. Por lo tanto, la cooperación internacional y el intercambio de información son críticas para una respuesta eficaz.

Mediante el uso de IA, se pueden crear plataformas centralizadas que agreguen datos de múltiples fuentes, permitiendo a las agencias de seguridad y organizaciones internacionales compartir información. Esto no solo mejora la capacidad de detección de amenazas, sino que también agiliza la toma de decisiones y la respuesta a incidentes. Por ejemplo, Europol ha implementado el uso de IA en su plataforma de ciberinteligencia para mejorar la cooperación entre los países miembros de la Unión Europea en la lucha contra el cibercrimen. Esta plataforma utiliza algoritmos avanzados para analizar datos de diversas fuentes, identificar patrones de actividad maliciosa y coordinar respuestas rápidas (Europol, 2020).

En un mundo donde los ciberataques se vuelven cada vez más sofisticados, la capacidad de la IA para analizar vastas cantidades de datos y detectar patrones de comportamiento potencialmente peligrosos permite una respuesta más rápida y efectiva ante amenazas emergentes. Sin embargo, a medida que nuestras herramientas de seguridad continúan mejorándose, es crucial que también aumentemos la conciencia pública sobre los riesgos asociados con el uso de redes sociales y la información compartida en ellas. En un entorno digital donde una persona común puede no entender las implicaciones de su actividad en línea, es fundamental educar y proteger a los usuarios, asegurando que la IA se utilice de manera responsable y ética para prevenir y combatir crímenes en todas sus formas.

2.2 Desafíos asociados con los ciberataques y el espionaje, y estrategias de mitigación y protección para los Estados

El avance vertiginoso de las tecnologías emergentes, junto con la expansión masiva del uso de Internet, ha generado una profunda interdependencia a nivel global. Esta interconexión ha llevado a los gobiernos de todo el mundo a enfrentar desafíos sin precedentes en materia de seguridad cibernética. Según Nye (2004), en la era digital actual, los Estados se ven confrontados con la necesidad urgente de fortalecer sus

capacidades de defensa contra ciberataques que pueden comprometer desde infraestructuras críticas hasta la privacidad de los ciudadanos. Este fenómeno ha colocado a la protección en el ciberespacio en lo más alto de las agendas de seguridad nacional, destacando la importancia de implementar estrategias avanzadas y colaborativas para mitigar los riesgos asociados.

Así, la protección contra ciberamenazas se erige no solo como una medida defensiva, sino también como un componente vital para la seguridad. En términos de seguridad y defensa, el ciberespacio debe ser entendido como un dominio comparable con otros escenarios militares tradicionales, como el mar, el aire, la tierra y el espacio. La diferencia principal radica en que, en el ciberespacio, el objetivo primordial es la información (Nye, 2011).

La interdependencia digital también ha intensificado la vulnerabilidad de los sistemas y datos nacionales ante amenazas transnacionales y sofisticadas. Según Kaiser (2019), el aumento en la conectividad global ha ampliado el alcance y la complejidad de los ataques cibernéticos, que ahora pueden afectar múltiples países simultáneamente. Esta realidad ha impulsado a los estados a adoptar enfoques proactivos y multilaterales en la prevención y respuesta ante incidentes cibernéticos, buscando no solo proteger sus propias infraestructuras críticas, sino también fortalecer la resiliencia cibernética a nivel global (European Commission, 2020).

Un caso concreto es Estados Unidos, donde la estrategia de ciberseguridad incluye la protección de infraestructuras críticas y la defensa contra ciberataques provenientes de actores estatales y no estatales. Del mismo modo, China ha desarrollado capacidades avanzadas en ciberseguridad para proteger su información estatal y comercial, además de utilizar el ciberespionaje para obtener ventajas estratégicas (Segal, 2016). En Europa, países como Alemania han implementado medidas robustas para proteger sus redes y sistemas de información contra amenazas cibernéticas, reconociendo la importancia de este dominio en la defensa nacional (Federal Office for Information Security, 2018).

Estas actividades maliciosas no solo comprometen la integridad de las infraestructuras críticas, sino que también ponen en riesgo la confidencialidad de la información gubernamental y la privacidad de los ciudadanos. Los ciberataques pueden

tener efectos devastadores, desde el sabotaje de servicios esenciales hasta la manipulación de datos y la desinformación, lo que a su vez puede desestabilizar a los gobiernos y erosionar la confianza pública (Kostka & Gkritzali, 2020).

Con el afianzamiento de la tecnología en la nube y la expansión del 5G, se prevé un nuevo punto de inflexión en el aumento de ciberataques (Dircom, 2020). Esta evolución tecnológica, si bien promete beneficios sin precedentes en términos de conectividad y eficiencia, también incrementa significativamente las superficies de ataque, exponiendo a las organizaciones a nuevas y sofisticadas amenazas cibernéticas. El Foro Económico Mundial ha advertido que los ciberataques y el fraude o robo de datos son dos de los cinco riesgos principales a los que se enfrentan los CEO en la actualidad (Zerfass, Verhoeven, Moreno, Tench & Verčič, 2020). Esto subraya la urgente necesidad de implementar medidas robustas de ciberseguridad para proteger activos críticos y salvaguardar la integridad de la información.

Algunos gobiernos prevén el uso de tecnología de manera agresiva, con el objetivo de reducir el poder de los países considerados enemigos. Esta perspectiva plantea un gran desafío para la sutileza propia de la diplomacia, ya que convierte la IA en una herramienta casi matemática de los Estados, basando su actuación en la información y las estadísticas que esta tecnología proporciona (Kostka & Gkritzali, 2020). Sin embargo, este enfoque puede ser contraproducente, ya que la diplomacia requiere un manejo delicado y estratégico de las relaciones internacionales, donde el conocimiento de la psicología del poder y de la sociedad es fundamental (Bjola, 2018).

Debemos tener en cuenta que uno de los desafíos más críticos que enfrentan los Estados en el ámbito de la diplomacia digital es el compromiso de información confidencial. Los ciberataques pueden conducir al acceso no autorizado y al robo de datos altamente sensibles, lo que pone en peligro la seguridad nacional y las relaciones diplomáticas. Información clasificada sobre estrategias diplomáticas, acuerdos internacionales, y negociaciones puede ser sustraída y utilizada por actores malintencionados para obtener ventajas estratégicas, económicas o políticas. Este tipo de información, cuando es expuesta o manipulada, puede traer como consecuencia diversos efectos como la desconfianza y tensiones entre países, complicando los esfuerzos diplomáticos y llevando a posibles conflictos.

Un ejemplo notable de este tipo de riesgo es el ciberataque sufrido por el Departamento de Estado de Estados Unidos en 2014, cuando *hackers* vinculados a un gobierno extranjero accedieron a correos electrónicos no clasificados pero sensibles, lo que generó una preocupación significativa sobre la seguridad de la información diplomática (Sanger, 2014). Este ataque destacó la vulnerabilidad de los sistemas diplomáticos y la necesidad urgente de fortalecer las medidas de seguridad cibernética.

Además, la complejidad y el anonimato del ciberespacio hacen que sea difícil atribuir con certeza estos ataques a un perpetrador específico. La atribución incorrecta puede llevar a acusaciones infundadas y aumentar las tensiones internacionales. Como señala Rid y Buchanan (2015), la atribución de ciberataques es un proceso complejo que requiere una combinación de evidencia técnica y análisis de inteligencia, y la falta de certeza en este proceso puede complicar aún más las reylaciones diplomáticas.

La misma tecnología que fortalece la defensa cibernética también es utilizada por los atacantes para desarrollar técnicas más avanzadas de cibercrimen. Actualmente, una de las maneras más comunes de desinformación con fines maliciosos es el uso de *deep fakes*, que son audios, videos y textos manipulados para parecer auténticos. Esta tecnología puede alterar rostros en videos, sincronizar labios con audios falsificados y generar imágenes de personas diciendo o haciendo cosas que nunca ocurrieron. Según Chesney y Citron (2019), representan una amenaza significativa para la integridad de la información, ya que pueden ser utilizados para desinformar, difamar y engañar tanto a individuos como a sistemas automatizados. Esta tecnología ha evolucionado rápidamente, y la calidad ha mejorado a tal punto que es cada vez más difícil para el ojo humano detectar la manipulación. Este fenómeno no solo amenaza la privacidad y la seguridad personal, sino que también plantea riesgos significativos para la seguridad nacional y la estabilidad política.

Los *deep fakes,* junto con las *fake news,* se han convertido en herramientas poderosas para campañas de desinformación, ya que pueden crear contenidos falsos que son prácticamente indistinguibles de los reales, creando un desafío adicional para la detección y prevención de ciberamenazas. Estas notas, diseñadas para parecer verídicas, pueden influir en la opinión pública y manipular el comportamiento de las personas y organizaciones. Según un estudio de Lazer et al. (2018), la propagación de *fake news* se

ha acelerado con el uso de algoritmos de IA, que pueden generar y distribuir contenido falso a gran escala con una eficiencia alarmante.

En marzo de 2022, durante el conflicto entre Rusia y Ucrania, se difundió un *deep fake* del presidente ucraniano, Volodymyr Zelensky, en el que parecía pedir a las tropas ucranianas que se rindieran y depusieran las armas. El video fue generado utilizando técnicas de IA, específicamente redes neuronales generativas adversarias (GANs), que permitieron sincronizar los movimientos de los labios de Zelensky con un audio falsificado, logró engañar a muchas personas inicialmente, exacerbando las tensiones y sembrando confusión en un momento crítico del conflicto (Vincent, 2022).

La rápida propagación del video en las redes sociales tuvo repercusiones significativas. Al ser compartido masivamente, tuvo el potencial de socavar la moral de las fuerzas ucranianas y crear una percepción errónea de la situación en el terreno. La manipulación no solo afectó la opinión pública, sino que también puso en peligro la estabilidad y la cohesión de la resistencia ucraniana contra la invasión rusa (Vincent, 2022).

Para mitigar el impacto, el gobierno ucraniano actuó rápidamente. Zelensky desmintió personalmente el video a través de sus canales oficiales, asegurando a los ciudadanos y a las fuerzas armadas que la grabación era falsa y reafirmando su compromiso con la defensa del país. Además, las plataformas de redes sociales trabajaron para eliminar el video y detener su difusión, aunque no sin ciertos desafíos debido a la velocidad con la que se había propagado (Vincent, 2022).

Estas acciones destacaron la importancia de la respuesta rápida y coordinada ante la desinformación digital. La capacidad de identificar y contrarrestar los *deep fakes* es crucial en tiempos de conflicto, donde la información veraz es fundamental para mantener la moral y la cohesión social.

Por otro lado, el espionaje cibernético es utilizado tanto por actores estatales como no estatales, permitiéndoles acceder a información altamente sensible y estratégica. Esta práctica no solo proporciona una ventaja indebida en el ámbito geopolítico, sino que también socava la confianza entre las naciones, generando tensiones que pueden desestabilizar el orden internacional (Hocking et al., 2012). Un ejemplo destacado es la Operación Aurora en 2009, donde atacantes cibernéticos

vinculados al gobierno chino comprometieron las redes de Google y otras grandes corporaciones, accediendo a datos críticos que incluían propiedad intelectual y comunicaciones de activistas de derechos humanos. Este incidente no solo demostró la capacidad de los Estados para ejecutar ciberespionaje a gran escala, sino también expuso la vulnerabilidad de las infraestructuras digitales frente a tales amenazas (McAfee, 2021).

Además, las redes sociales han emergido como un campo fértil para las actividades de espionaje, debido a la gran cantidad de datos personales que estas plataformas recogen. Estas plataformas no solo son utilizadas para monitorear a individuos, sino también para manipular opiniones y conductas. Un caso concreto fue cuando en 2018 se descubrió que hackers rusos utilizaron perfiles falsos en LinkedIn para establecer conexiones con empleados de empresas de defensa, logrando así acceder a información sensible y comprometer la seguridad nacional (Nakashima, 2018). Este caso subraya cómo incluso las plataformas profesionales, que suelen percibirse como más seguras, pueden ser instrumentalizadas para el espionaje.

Hoy en día garantizar la soberanía digital se ha convertido en un desafío para los Estados, los gobiernos deben equilibrar cuidadosamente la implementación de medidas de seguridad cibernética con el respeto a la soberanía digital y la privacidad de sus ciudadanos. Este equilibrio es fundamental para asegurar que las acciones destinadas a proteger el ciberespacio no infrinjan los derechos humanos y las libertades fundamentales.

Según Deibert (2019), la soberanía digital se refiere al control y la protección de los datos e infraestructuras digitales dentro de las fronteras de un país. Donde los datos personales y sensibles pueden ser explotados por actores malintencionados, lo que obliga a los Estados a implementar robustas medidas de ciberseguridad. Sin embargo, la implementación de estas medidas debe ser compatible con los derechos humanos y las libertades fundamentales. Deibert destaca que cualquier enfoque hacia la ciberseguridad debe considerar las implicaciones sobre la privacidad y la libertad de expresión.

Un ejemplo de la importancia de este equilibrio es el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. El GDPR no sólo establece normas estrictas para la protección de datos personales, sino que también garantiza que las

medidas de seguridad cibernética no violen la privacidad de los ciudadanos. Este reglamento ha servido como modelo para otros países que buscan equilibrar la seguridad cibernética con la soberanía digital y la protección de la privacidad (European Parliament, 2016).

Según Weber (2017), la construcción de un marco legal internacional que respete la soberanía digital de cada nación, mientras facilita la cooperación y el intercambio de información, es crucial para enfrentar las ciberamenazas. Implica que los Estados deben tener control sobre su infraestructura digital y ser capaces de proteger sus sistemas de información de interferencias extranjeras. Sin embargo, la cooperación internacional y la interoperabilidad de las normativas son esenciales para combatir eficazmente las amenazas cibernéticas globales

La creciente interdependencia hace que la seguridad cibernética no sea solo una cuestión nacional, sino un desafío internacional que requiere cooperación y coordinación entre Estados. Además, la rápida evolución de las tecnologías digitales demanda una actualización constante de las estrategias de defensa para enfrentar nuevas amenazas y vulnerabilidades en el ciberespacio (Kello, 2017). Esta dinámica subraya la importancia de desarrollar políticas y marcos legales que permitan a los Estados proteger eficazmente su información y asegurar la resiliencia de sus infraestructuras digitales.

La colaboración internacional y la compartición de información son pilares fundamentales en la detección y prevención de ciberamenazas en la diplomacia digital. En un mundo cada vez más interconectado, los ataques cibernéticos a menudo trascienden fronteras nacionales, lo que hace esencial una respuesta coordinada. La IA puede facilitar enormemente esta cooperación al permitir el intercambio rápido y eficiente de datos relevantes sobre amenazas entre diferentes países y organizaciones. Herramientas basadas en IA pueden analizar datos recopilados de diversas fuentes internacionales y generar alertas sobre posibles amenazas emergentes en tiempo real. Un caso es la Unión Europea que ha implementado sistemas de IA para compartir información sobre ciberamenazas entre sus Estados miembros, lo que ha resultado en una mejora significativa en la detección y respuesta a ataques cibernéticos (EU Agency for Cybersecurity, 2020). Además, plataformas de colaboración como el Foro Mundial de Ciberseguridad (WCF) utilizan IA para analizar tendencias en ciberseguridad y

compartir mejores prácticas entre las naciones participantes (WCF, 2021). Este enfoque colaborativo no solo fortalece las capacidades de defensa de cada país, sino que también crea una red de seguridad global más robusta y resiliente.

Capítulo 3: Ética y acceso a los datos

3.1 La influencia de la disparidad en el acceso y uso de la IA en las relaciones internacionales

Para comenzar a hablar sobre este tópico es importante entender que la adopción y el uso de estas tecnologías no son homogéneos a nivel mundial, lo que genera una disparidad significativa en el acceso y aprovechamiento de la IA entre diferentes países y regiones. Las naciones desarrolladas, con recursos tecnológicos avanzados y una infraestructura sólida, pueden integrar la IA en sus sistemas de gobierno, economía y defensa de manera más efectiva que los países en desarrollo. Esta brecha tecnológica no solo afecta la competitividad económica, sino que también tiene profundas implicaciones en la política internacional y la seguridad global (Allan, 2018).

En el caso de Singapur, al ser un líder en la adopción de IA, utiliza su avanzada infraestructura tecnológica para fortalecer su posición en la diplomacia digital. La capacidad del país para implementar y gestionar tecnologías de IA le proporciona una ventaja en la creación de políticas de ciberseguridad y en la promoción de su influencia en foros internacionales relacionados con la tecnología y la innovación (Cheng, 2021). Esta integración efectiva de la IA contribuye a la capacidad de Singapur para participar activamente en discusiones globales sobre normas y regulaciones tecnológicas, y a mantener una posición competitiva en el escenario internacional.

Además, su estrategia también se centra en inversiones significativas en sectores clave como la atención médica, el transporte y la seguridad, utilizando la IA como un motor para mejorar la calidad de vida y la eficiencia gubernamental (Smart Nation Singapore, 2019). Bajo la iniciativa "*Smart Nation",* el país ha lanzado una serie de proyectos que emplean IA para optimizar la gestión urbana y los servicios públicos. Un ejemplo destacado es el sistema "*Intelligent Transport Systems*" de la Autoridad de Transporte Terrestre (LTA), que utiliza IA para gestionar de manera eficiente el tráfico, reducir la congestión y mejorar la experiencia de los usuarios del transporte público.

Asimismo, podemos observar cómo China ha implementado diversas estrategias y políticas para posicionarse como un líder global en IA. En 2017, el gobierno chino presentó el "Plan de Desarrollo de Inteligencia Artificial de Nueva Generación", un documento estratégico que marca un hito en la aspiración del país por convertirse en la principal potencia mundial en el campo de la IA para 2030 (Zhang, L., 2018). Este plan integral no solo abarca la creación de una infraestructura tecnológica avanzada, sino que también se enfoca en tres áreas cruciales: la formación de talento especializado, la inversión en investigación y desarrollo (I+D), y la creación de un ecosistema propicio para la innovación.

Este país ha destinado grandes cantidades de recursos tanto públicos como privados para lograr estos objetivos. En el ámbito de la investigación y el desarrollo, el plan chino contempla inversiones masivas para fomentar la innovación. Estas están dirigidas a desarrollar nuevas tecnologías de IA y mejorar las existentes, con el objetivo de lograr avances significativos que permitan al país mantener una ventaja competitiva en el mercado global. Según el "Informe de Inteligencia Artificial Global" de 2020, China invierte significativamente en investigación en IA y ha superado a otras naciones en la cantidad de publicaciones académicas y patentes relacionadas con esta temática (Zengler, 2020). Además, el gobierno chino ha fomentado la colaboración entre universidades, institutos de investigación y empresas tecnológicas para acelerar el desarrollo y la implementación de tecnologías avanzadas.

China ha utilizado su liderazgo en IA para expandir su influencia global a través de la iniciativa "Ruta de la seda", promoviendo la cooperación tecnológica y el intercambio de conocimientos con otros países en desarrollo, y estableciendo estándares internacionales que pueden fortalecer su posición en la diplomacia digital (Huang & Li, 2021).

La asignación de recursos sustanciales a I+D permite a los países no solo crear nuevas aplicaciones de IA, sino también mejorar las existentes, manteniéndose así a la vanguardia de la innovación tecnológica. Este liderazgo tecnológico es fundamental en el contexto internacional, donde la capacidad de utilizar y avanzar en tecnologías de IA puede traducirse en ventajas estratégicas y competitivas a nivel global (Brynjolfsson & McAfee, 2021).

Estos factores interrelacionados delinean las capacidades internas de los Estados para integrar y beneficiarse del avance tecnológico que representa la IA. La capacidad de un país para adaptarse y prosperar con las tecnologías emergentes está íntimamente relacionada con su entorno cultural y organizacional que valora y promueve la innovación. Según Singer y Friedman (2014), una cultura de innovación no solo impulsa el desarrollo y la integración de nuevas tecnologías, sino que también contribuye a la eficacia en su implementación en diversos sectores, desde la administración pública hasta la industria.

En particular, los países que alientan una mentalidad abierta hacia la innovación y el cambio tecnológico pueden experimentar una transición más fluida hacia la adopción de tecnologías avanzadas como la IA. Estos países suelen contar con ecosistemas de innovación que incluyen políticas gubernamentales favorables, apoyo financiero para startups y empresas emergentes, y una fuerte colaboración entre el sector académico y la industria. Esta atmósfera no solo facilita la integración de tecnologías emergentes, sino que también promueve la creatividad y la experimentación, elementos cruciales para el avance en el campo de la IA.

No obstante, debemos comprender que la decisión de implementar IA en áreas como la diplomacia depende de una serie de factores como la capacidad tecnológica, la inversión en investigación y desarrollo, y consideraciones estratégicas, las cuales pueden variar de país en país. La falta de acceso a tecnologías avanzadas en algunas naciones no solo limita su capacidad para competir en el ámbito internacional, sino que también tiene impactos profundos en su desarrollo interno y en la calidad de vida de su población. Estos efectos son especialmente agudos en contextos donde la infraestructura tecnológica es débil o inexistente, lo que agrava las crisis existentes y dificulta la implementación de soluciones efectivas. Un ejemplo es Venezuela, donde la falta de acceso a tecnologías avanzadas tuvo consecuencias graves en la crisis del sistema de salud. Durante el brote de enfermedades como el sarampión y la malaria en los últimos años, la falta de herramientas avanzadas de IA para el seguimiento de datos epidemiológicos y la predicción de brotes ha dificultado enormemente la respuesta del gobierno. Sin un sistema adecuado para procesar grandes volúmenes de datos y anticipar focos de infección, el país no pudo contener adecuadamente estos brotes, lo que resultó en un aumento significativo de casos y una crisis sanitaria prolongada.

Además, la limitada infraestructura tecnológica ha impedido la implementación de soluciones de telemedicina basadas en IA, lo que ha exacerbado la falta de acceso a atención médica en áreas rurales y ha contribuido al colapso del sistema de salud pública. Esta situación ha llevado a una mayor dependencia de la asistencia internacional y ha agravado la crisis humanitaria en el país (Rodríguez, 2019).

Este contraste afecta profundamente a los Estados y se manifiesta en varios aspectos. Por un lado, la disponibilidad de una infraestructura tecnológica adecuada es crucial para la efectiva implementación y aprovechamiento de las herramientas de diplomacia digital. La infraestructura permite a los Estados implementar y operar sistemas de IA que pueden potenciar significativamente sus capacidades diplomáticas. Davenport y Harris (2007) destacan que una infraestructura tecnológica robusta, que incluye tanto el hardware necesario como los recursos técnicos y humanos, es vital para que los Estados sean capaces de integrarse y beneficiarse de la IA. Una infraestructura deficiente puede limitar la capacidad de un país para adoptar tecnologías avanzadas, afectando su competitividad y su posición en la escena internacional. Estas capacidades pueden otorgar a los Estados una ventaja estratégica, permitiéndoles anticipar movimientos de otros actores y responder de manera más efectiva a las amenazas globales.

La infraestructura adecuada también facilita la creación y mantenimiento de canales de comunicación seguros y eficientes. Las redes de alta velocidad y baja latencia, como la tecnología 5G, permiten una transmisión rápida y confiable de información entre las embajadas, consulados y oficinas gubernamentales. Esto es vital para la diplomacia, donde la capacidad de comunicarse de manera rápida y segura es crucial para la toma de decisiones informadas y la coordinación de políticas internacionales (Taleb et al., 2017).

Otro punto importante a tener en cuenta es el nivel de alfabetización digital de la población; según el Gobierno de Argentina. (n.d.) es la capacidad de los individuos para comprender, evaluar y utilizar tecnologías de manera efectiva y segura en diversos contextos, desde el ámbito personal hasta el profesional y social, buscando la promoción de inclusión y reducción de la brecha. Como indica Ceron, Curini y Iacus (2016), solo una sociedad bien informada y capacitada en competencias puede maximizar los beneficios de la IA. La educación y la formación en tecnología son

esenciales para que los ciudadanos puedan adaptarse a los cambios tecnológicos y utilizar las herramientas de IA de manera correcta. Sin una población digitalmente alfabetizada, los beneficios de la IA pueden quedar fuera del alcance de muchos, exacerbando las desigualdades internas.

Los Estados que invierten en la alfabetización digital de su población pueden participar más efectivamente en la diplomacia ya que les permite negociar, comunicarse y proyectar su poder blando en plataformas internacionales que puede mejorar la posición de un Estado en la arena global.

El uso de plataformas tecnológicas en la diplomacia permite la creación de redes de cooperación más amplias y efectivas. Los Estados que dominan estas herramientas pueden movilizar rápidamente apoyo global para sus causas, establecer alianzas estratégicas, y responder a crisis internacionales con mayor celeridad. Como señala Westerman (2012), el entorno digital ofrece a los Estados la capacidad de expandir su influencia más allá de las limitaciones geográficas, participando activamente en la formación de la agenda global.

Un ejemplo relevante es Sudán del Sur, un país que ha enfrentado conflictos prolongados y crisis humanitarias desde su independencia en 2011. Según un informe del Banco Mundial (2022), la escasez de habilidades digitales limita gravemente el potencial de crecimiento económico al restringir el acceso a servicios clave en sectores como la educación y la salud. Sin una población capacitada para utilizar las tecnologías, el país pierde oportunidades para impulsar su desarrollo económico, exacerbando las desigualdades sociales y económicas. Esta brecha digital también debilita la capacidad del gobierno para implementar políticas eficaces y gestionar servicios públicos, afectando negativamente la transparencia y la eficiencia en la administración pública. Además, la falta de formación en tecnología impide el desarrollo y la implementación de infraestructura tecnológica avanzada, perpetuando la dependencia de soluciones externas y limitando la capacidad del país para generar sus propias soluciones tecnológicas. En términos de diplomacia digital, la ausencia de habilidades también afecta la capacidad de Sudán del Sur para participar en plataformas internacionales y proyectar su poder blando. Sin las herramientas y habilidades necesarias para negociar y comunicarse efectivamente en el entorno global, el país pierde influencia en el escenario

internacional, lo que limita su participación en la diplomacia y su capacidad para interactuar de manera efectiva con otros actores globales (Banco Mundial, 2022).

Siguiendo con este lineamiento, la disponibilidad de personal capacitado en tecnología de la información y ciencia de datos es esencial, los Estados que invierten en la formación de sus profesionales en estas áreas pueden desarrollar y mantener sistemas de IA más avanzados. Según Manyika et al. (2017), la escasez de talento especializado puede limitar severamente la capacidad de un país para competir; esto significaría que un país se rezaga en la adopción de nuevas tecnologías. Ello limita su capacidad para innovar y adaptarse a las demandas cambiantes del entorno diplomático, haciendo que sus estrategias sean menos efectivas y menos competitivas en comparación con las de otros países que sí invierten en el desarrollo de talento tecnológico.

Esta falta de expertos obliga a las naciones a recurrir a soluciones y servicios tecnológicos provenientes del extranjero, lo que puede llevar a una dependencia que compromete su soberanía digital. Cuando un país depende de tecnología controlada por otros Estados o grandes corporaciones multinacionales, su capacidad para proteger sus intereses nacionales y tomar decisiones autónomas en la arena internacional se ve significativamente reducida.

Esta dependencia tecnológica puede limitar la capacidad de un Estado para implementar políticas y proteger su infraestructura crítica. Además, la falta de control sobre las herramientas tecnológicas utilizadas en comunicaciones diplomáticas y en la gestión de datos sensibles puede exponer a un país a riesgos de espionaje y manipulación, debilitando su posición en el ámbito internacional. Un ejemplo claro es el caso de Mongolia que ha enfrentado desafíos significativos debido a su infraestructura tecnológica subdesarrollada, el país ha tenido que depender en gran medida de proveedores extranjeros para servicios clave, incluyendo tecnología de la información y ciberseguridad. En 2021, se descubrió que Mongolia fue víctima de un ataque cibernético significativo que comprometió datos personales de millones de ciudadanos y funcionarios gubernamentales (Baldwin, 2022). El ataque fue facilitado en parte por la falta de infraestructura interna robusta para la protección de datos y la ciberseguridad.

La dependencia de proveedores externos también ha afectado la capacidad de Mongolia para implementar políticas tecnológicas efectivas y autónomas. La falta de un

marco tecnológico nacional fuerte ha llevado a una situación en la que las decisiones tecnológicas importantes, como la gestión de datos críticos y la protección contra ciberamenazas, están influenciadas por las capacidades y los intereses de los proveedores extranjeros. Según una evaluación de la Fundación para el Desarrollo Sostenible (2022), esta situación no solo ha expuesto a Mongolia a riesgos de seguridad, sino que también ha limitado su capacidad para participar de manera equitativa y proteger tanto su diplomacia como su soberanía digital.

Los Estados pueden adoptar diversos enfoques en la integración de la IA, lo que añade una capa adicional de complejidad a la intersección entre la política exterior y la tecnología. Los países que presentan sistemas educativos menos desarrollados o acceso limitado a recursos tecnológicos enfrentan significativos desafíos en la preparación de su población para el uso efectivo de IA. La brecha tecnológica puede amplificar las tensiones y conflictos internacionales, ya que los países rezagados pueden experimentar una creciente sensación de inseguridad y vulnerabilidad, exacerbando la necesidad de buscar alianzas estratégicas y adoptar políticas proteccionistas y de ciberdefensa. En consecuencia, esta dinámica puede intensificar las rivalidades geopolíticas y contribuir a un entorno internacional más fragmentado y conflictivo, donde las naciones con menos recursos tecnológicos quedan atrapadas en una espiral de dependencia y desventaja estratégica (Choucri, 2012).

Además, la incapacidad de estos países para integrar la IA en sus sistemas de gobierno y en su economía puede llevar a una desventaja competitiva, limitando su capacidad para influir en la toma de decisiones internacionales y participar eficazmente en la diplomacia. Este círculo vicioso de desventajas tecnológicas y dependencia externa no solo refuerza la brecha entre naciones desarrolladas y en desarrollo, sino que también puede contribuir a una mayor inestabilidad y fragmentación en el sistema internacional (Choucri, 2012).

Las inversiones en educación y la inclusión de programas de capacitación en tecnologías emergentes son cruciales para cerrar esta brecha. Los programas de alfabetización digital deben ser accesibles y estar diseñados para incluir a todas las partes de la sociedad, especialmente a grupos vulnerables y marginados.

3.2 Consideraciones éticas en el desarrollo y uso de la IA en la diplomacia digital

La globalización actual plantea una serie de desafíos éticos que requieren una reflexión cuidadosa, especialmente en el contexto de la diplomacia digital. A medida que la IA se integra en los procesos diplomáticos, surgen interrogantes cruciales sobre la transparencia y la responsabilidad en su aplicación. Estos desafíos no solo repercuten en la eficacia y legitimidad de las políticas internacionales, sino que también tienen implicaciones significativas para la soberanía de los Estados y la protección de los derechos humanos. Por lo tanto, es esencial examinar las consideraciones éticas asociadas al uso de la IA en la diplomacia, garantizando que estas tecnologías sean implementadas de manera justa y responsable, y que contribuyan efectivamente a la promoción de la paz y la cooperación internacional.

Un aumento en el número de actores, como organizaciones internacionales, corporaciones, medios de comunicaciones o ONGs, puede generar complejidades adicionales, como la necesidad de coordinar y gestionar una mayor cantidad de información y comunicación entre múltiples entidades. Además, la implementación de IA en la diplomacia plantea desafíos significativos relacionados con la transparencia, la ética y la seguridad. Así como la falta de procedimientos claros y estandarizados para el uso de IA podría llevar a un escenario donde las misiones diplomáticas se desarrollen en un entorno caótico, en lugar de uno cohesivo y estratégico. La ausencia de normativas claras podría derivar en decisiones automatizadas ambiguas, éticamente cuestionables o incluso inseguras, lo que afectaría negativamente la confianza entre las naciones y la legitimidad de los procesos diplomáticos.

Esto subraya la urgencia de establecer marcos legales y normativos que regulen la aplicación de la IA en la diplomacia. Tales marcos no solo deben garantizar que la implementación de estas tecnologías mejore la eficacia de las relaciones internacionales, sino también que se respeten los principios mencionados anteriormente. De lo contrario, el uso inadecuado de la IA podría erosionar la integridad de la diplomacia global, complicando aún más un panorama internacional ya de por sí complejo (Bjola, 2018).

La transparencia es uno de los aspectos claves para que la IA sea utilizada de manera correspondiente en la diplomacia digital, las instituciones públicas tienen la

responsabilidad de comunicar de manera clara cómo gestionan sus recursos y toman decisiones. En este contexto, las TIC han abierto nuevas oportunidades para que las administraciones públicas no solo divulguen información y la hagan accesible al público, sino también para establecer un canal bidireccional con la ciudadanía. (Paez y Montoya, 2020).

Esto, a su vez, fomenta una mayor participación ciudadana y contribuye al fortalecimiento de la confianza en las instituciones democráticas. Un claro ejemplo es el portal de datos abiertos de Estonia, una nación que ha sido pionera en la implementación del gobierno electrónico. A través de este portal, el gobierno de Estonia no solo proporciona acceso a una amplia gama de datos gubernamentales, sino que también permite a los ciudadanos interactuar con la información, hacer sugerencias y expresar sus inquietudes (Mickoleit, 2014).

La demanda de transparencia se refiere a la necesidad de que los sistemas de IA sean comprensibles y auditables, permitiendo a los usuarios y a los reguladores entender cómo se toman las decisiones y qué datos se utilizan. Según Dastin (2018), la falta de transparencia en los sistemas de IA puede llevar a la implementación de tecnologías que operan como "cajas negras", donde las decisiones y los procesos subyacentes son opacos y difíciles de interpretar. Esta opacidad puede agravar problemas como la discriminación y el sesgo, ya que las decisiones automatizadas pueden perpetuar desigualdades sin que se pueda identificar claramente la causa.

Además, el llamado a la transparencia en la IA también está vinculado a la responsabilidad y la rendición de cuentas. La claridad sobre los algoritmos utilizados y los datos empleados es crucial para asegurar que las decisiones automatizadas sean justas y que se logren corregir errores cuando se presenten. Por ejemplo, la iniciativa del *Institute of Electrical and Electronics Engineers* (IEEE) para desarrollar estándares globales de ética en la IA enfatiza la importancia de la transparencia como un principio clave para garantizar que las tecnologías sean utilizadas de manera responsable y equitativa (IEEE, 2020). Esta iniciativa busca promover prácticas de desarrollo que permitan a las partes interesadas comprender y cuestionar los procesos algorítmicos, fomentando así un entorno en el que la IA pueda ser utilizada de manera que beneficie a toda la sociedad sin comprometer los valores éticos.

A medida que los sistemas de IA se vuelven más autónomos, surge la cuestión de quién es responsable de las decisiones tomadas por estas tecnologías. Se deben establecer entornos claros de responsabilidad para asegurar que las acciones basadas en IA sean justificables y estén sujetas a revisión (Davenport & Harris, 2007).

El marco legal es fundamental, ya que establece las regulaciones y normativas necesarias para garantizar un uso seguro de la IA. Según Mayer (2019), los Estados que desarrollan un marco legal sólido para la IA pueden gestionar mejor los riesgos asociados con esta tecnología, asegurando su uso responsable y alineado con los principios éticos. Este aspecto es esencial para evitar abusos y para fomentar la confianza tanto de los ciudadanos como de los socios internacionales.

Otro de los principales desafíos en el uso de la IA en la diplomacia digital es la privacidad y la protección de datos. La recopilación y el análisis de datos a gran escala pueden invadir la privacidad de individuos y naciones, lo que genera preocupaciones sobre el manejo y la seguridad de esta información sensible (Allan, 2018). Es esencial que los diplomáticos y las organizaciones internacionales implementen políticas robustas para proteger los datos y asegurar su uso correcto.

A medida que las tácticas y herramientas utilizadas por actores malintencionados se vuelven más sofisticadas, los marcos normativos existentes a menudo se quedan obsoletos. Esto requiere que se trabaje continuamente para actualizar las normativas internacionales y asegurarse de que se implementen de manera coherente.

El desarrollo de políticas y regulaciones debe ser ágil y adaptativo. Las normativas deben contemplar no solo las amenazas actuales sino también prever posibles escenarios futuros. Según Singer y Friedman (2014), la capacidad de adaptación es crucial para enfrentar la naturaleza dinámica de las ciberamenazas. Esto implica un esfuerzo constante de monitoreo y análisis de tendencias emergentes en el ciberespacio.

Un ejemplo de la necesidad de políticas actualizadas es la normativa General de Protección de Datos (GDPR) de la Unión Europea, que establece estándares estrictos para la protección de datos personales. Aunque originalmente diseñada para abordar la privacidad de los datos, el GDPR también ha tenido implicaciones significativas en la

ciberseguridad, ya que obliga a las organizaciones a implementar medidas de seguridad robustas para proteger la información personal de los ciberataques (European Parliament, 2016).

Además, los diplomáticos deben negociar y coordinar políticas a nivel internacional para asegurar una respuesta unificada a las ciberamenazas. La Convención de Budapest sobre Ciberdelincuencia es un ejemplo donde se establecen normas comunes para la lucha contra el cibercrimen. Esta convención facilita la cooperación entre países y proporciona un marco para el intercambio de información y asistencia mutua en investigaciones (Council of Europe, 2001).

No obstante, la implementación de políticas y regulaciones efectivas enfrenta varios desafíos. La diversidad de sistemas legales y niveles de desarrollo tecnológico entre países puede dificultar la armonización de normativas. Además, las preocupaciones sobre la soberanía nacional y la privacidad pueden generar resistencia a la adopción de ciertos estándares internacionales. Según Weber (2017), la construcción de confianza y la negociación de compromisos son esenciales para superar estas barreras y lograr una cooperación eficaz en ciberseguridad.

Debemos tener en cuenta que los avances tecnológicos rápidos a menudo superan la capacidad de los marcos legales y regulatorios para mantenerse al día. Por otro lado, las preocupaciones sobre la soberanía nacional pueden dificultar la armonización de políticas a nivel internacional.

El sesgo en los algoritmos de IA puede llevar a decisiones injustas o discriminatorias. Los sistemas de IA pueden perpetuar y amplificar los prejuicios existentes si no se diseñan y supervisan adecuadamente. Esto es especialmente preocupante en el contexto de la diplomacia, donde las decisiones pueden tener consecuencias significativas a nivel global. La transparencia en el desarrollo y la implementación de algoritmos de IA es crucial para mitigar estos riesgos (Brynjolfsson & McAfee, 2021).

Según Smith (2020), el manejo inapropiado de estas tecnologías puede llevar a la discriminación racial, étnica o de género. Los sistemas de reconocimiento facial, han mostrado ser menos precisos en identificar a personas de etnias diversas, lo que puede resultar en perfiles discriminatorios y acciones de vigilancia desproporcionadas.

Un caso relevante que tuvo implicaciones significativas en la diplomacia se produjo con el sistema de reconocimiento facial desarrollado por la empresa Clearview AI. Este sistema, utilizado por diversas agencias gubernamentales, fue criticado por su alta tasa de errores y su sesgo racial. En 2020, investigaciones revelaron que el software de Clearview AI tenía una precisión significativamente menor en el reconocimiento facial de personas de color en comparación con los blancos. Este sesgo en los algoritmos generó preocupaciones sobre la posibilidad de que el sistema contribuyera a decisiones injustas en contextos como la seguridad pública y la inmigración, afectando desproporcionadamente a comunidades marginadas. La falta de transparencia en el diseño y en los datos utilizados para entrenar estos algoritmos subrayó la necesidad de revisar y regular el uso de IA para asegurar la justicia y la equidad en decisiones que pueden tener implicaciones diplomáticas y de derechos humanos (Raji & Buolamwini, 2019).

Debemos entender que para lograr abordar la problemática de la discriminación y la vulneración de derechos en el uso de IA se requiere un enfoque multifacético que incluya principios éticos, regulaciones estrictas y la participación de diversos grupos en el desarrollo de estas tecnologías

Ante estos retos, la idea de promover una gobernanza ética de la IA se hace cada vez más necesaria. Y es justamente ahí, donde la diplomacia juega un rol de suma importancia, el ejercicio diplomático puede facilitar la creación de alianzas y acuerdos internacionales que establezcan reglas y normativas éticas para el desarrollo y uso de la IA en espacios bilaterales, plurilaterales y multilaterales.

La ausencia de procedimientos estandarizados por parte de los Estados sobre el uso de la IA en la diplomacia subraya la necesidad urgente de adoptar marcos legales globales. La falta de una codificación clara podría tener consecuencias significativas y negativas, lo cual se refleja en la creciente preocupación por un "nuevo orden global" y la posibilidad de una "nueva guerra mundial" en la última década. En este contexto, tanto la diplomacia como la IA desempeñarán roles cruciales en la configuración de las relaciones internacionales y en la gestión de potenciales conflictos (Nye, 2004).

Además, la implementación responsable de estas tecnologías es esencial para equilibrar el potencial de impacto positivo con la necesidad de proteger los derechos

individuales y evitar abusos. A medida que la IA y el *big data* continúan evolucionando, será crucial desarrollar marcos legales robustos que garanticen el uso responsable de estas herramientas en todos los ámbitos, desde la política hasta la prevención de conflictos internacionales.

Reflexiones finales

A lo largo de esta tesina, se ha confirmado la hipótesis que sustenta el trabajo. Según esta hipótesis, la IA tiene el potencial de convertirse en una parte troncal de la diplomacia en el futuro, mejorando significativamente la eficiencia y efectividad de las interacciones diplomáticas, siempre y cuando se desarrollen y apliquen adecuadas medidas de seguridad y mejores prácticas para proteger la integridad de la información diplomática en un entorno digital. Podemos optimizar la gestión y el análisis de datos, mejorando la precisión y rapidez en la toma de decisiones, así como la capacidad de los diplomáticos para interactuar y comunicarse con diversas audiencias. Asimismo, con las estrategias adecuadas, es factible asegurar que los beneficios de la diplomacia digital sean accesibles para todos los estados, independientemente de su nivel de desarrollo tecnológico.

La integración de la IA en la diplomacia marca una de las transformaciones más significativas en las relaciones internacionales contemporáneas. A lo largo de esta tesina, se ha demostrado cómo la IA ha pasado de ser una mera herramienta tecnológica a convertirse en un actor clave que reconfigura las dinámicas de poder, las estrategias diplomáticas y los principios éticos que sustentan la interacción entre los Estados. Este fenómeno no solo ha cambiado la forma en que los diplomáticos realizan su labor, sino que también ha generado nuevas oportunidades y desafíos que exigen una reevaluación constante de las prácticas y teorías diplomáticas tradicionales.

Uno de los temas abordados en la tesina es la capacidad de la IA para mejorar la toma de decisiones en el ámbito diplomático. Mediante el análisis de grandes volúmenes de datos en tiempo real, la IA permite a los Estados anticiparse a crisis potenciales, adaptar sus estrategias en función de escenarios cambiantes, y personalizar sus mensajes a audiencias específicas con una precisión sin precedentes. Esto ha llevado a una mayor eficiencia operativa y a una toma de decisiones más informada y estratégica. Sin embargo, esta capacidad también plantea preguntas sobre la transparencia y la responsabilidad en el proceso de toma de decisiones, ya que las decisiones basadas en algoritmos pueden estar sujetas a sesgos y errores que podrían tener consecuencias graves en el ámbito internacional.

Debemos comprender que esta herramienta será un beneficio para la diplomacia digital siempre y cuando se desarrollen y apliquen adecuadas medidas de seguridad y mejores prácticas para proteger la integridad de la información diplomática en un entorno digital. La IA ofrece la posibilidad de optimizar la gestión y el análisis de datos. Con las estrategias adecuadas, es factible asegurar que los beneficios de la diplomacia digital sean accesibles.

En cuanto a la ciberseguridad, la IA ha demostrado ser una herramienta poderosa para la detección y prevención de ciberamenazas, un aspecto cada vez más crucial en la diplomacia digital. Los Estados han comenzado a emplear sistemas de IA para proteger sus infraestructuras críticas y sus comunicaciones diplomáticas, lo que ha llevado a una mayor seguridad en el manejo de la información sensible. No obstante, la creciente dependencia de la IA en la ciberseguridad también conlleva riesgos. La posibilidad de que actores malintencionados desarrollen IA igualmente sofisticadas para perpetrar ciberataques plantea un desafío constante en la protección de la seguridad nacional y la integridad de las relaciones diplomáticas.

Por otro lado, podemos advertir que la presencia de la IA en la diplomacia es más potencial que real. Si bien ya forma parte de la actualidad, su verdadero potencial es incalculable, y la tecnología, incipiente. Esto sugiere que la plena integración de la IA en la diplomacia aún está en una etapa inicial, y que su desarrollo futuro podría traer consigo cambios aún más radicales en la manera en que los Estados manejan sus relaciones internacionales. Sin embargo, también es cierto que la comprensión de sus implicaciones requiere un abordaje interdisciplinario y un análisis más profundo que permita dimensionar sus efectos en los sistemas democráticos contemporáneos y en el funcionamiento del gobierno (Jungherr, 2023).

Además de los avances técnicos, la IA también ha reconfigurado las dinámicas de poder en las relaciones internacionales. Los Estados con acceso a tecnologías avanzadas de IA han ganado una ventaja competitiva significativa, lo que ha exacerbado las desigualdades entre las naciones. Esta brecha tecnológica no solo afecta la capacidad de algunos Estados para participar de manera efectiva en la diplomacia digital, sino que también plantea interrogantes sobre la equidad y la justicia en el sistema internacional. Es fundamental que la comunidad internacional aborde estas desigualdades y trabaje

hacia un acceso más equitativo a las tecnologías avanzadas para evitar que la brecha digital se convierta en una fuente de tensión y conflicto global.

La fortaleza de la cultura científica y tecnológica (C&T) en una sociedad también es crucial para comprender el potencial éxito del desarrollo de la IA y su adopción institucional. Como señala Bjola (2020), la C&T sirve como un importante determinante estructural de la forma en que la tecnología en general, y la IA en particular, podrían ser vistas como un asistente natural para la expansión del conocimiento o como una posible amenaza para el desarrollo social. El Índice de Preparación de IA del Gobierno de 2019 subraya la importancia de la cultura C&T para fomentar un ambiente propicio para la adopción de la IA, a través de indicadores como "Habilidades y Educación". Sin una fuerte cultura C&T nacional, los gobiernos podrían verse obligados a depender en gran medida de atraer y retener talento extranjero, un recurso ya de por sí escaso.

La incorporación de la IA en la agenda diplomática de los Estados constituye un avance crucial en el reconocimiento de la relevancia de esta tecnología en el escenario global. Sin embargo, como detalla Bjola (2020), es crucial destacar que su mera inclusión en la agenda no garantiza, necesariamente, que los Estados adopten esta tecnología para sus propios fines de política exterior. La adopción efectiva de la IA en la diplomacia dependerá de la capacidad de los Estados para superar los desafíos asociados con su implementación, incluyendo la falta de infraestructura adecuada, las brechas en las habilidades digitales, y las preocupaciones éticas que rodean su uso.

Desde una perspectiva ética, el uso de la IA en la diplomacia introduce una serie de desafíos que requieren una atención cuidadosa. La posibilidad de utilizar la IA para manipular la opinión pública, influir en elecciones, o incluso participar en operaciones de desinformación, plantea serios dilemas éticos que podrían socavar la confianza en las instituciones diplomáticas y la estabilidad del orden internacional. Es esencial que los Estados y las organizaciones internacionales establezcan marcos regulatorios claros que garanticen el uso responsable y ético de la IA en la diplomacia, protegiendo al mismo tiempo los derechos humanos y las libertades fundamentales.

Mirando hacia el futuro, es evidente que la IA continuará desempeñando un papel central en la evolución de la diplomacia. Los avances tecnológicos futuros, como

la IA explicable y la automatización avanzada, probablemente amplificarán las capacidades de los diplomáticos, permitiéndoles manejar situaciones complejas con mayor eficacia. Sin embargo, para aprovechar plenamente estas oportunidades, los Estados deberán invertir en la capacitación de sus diplomáticos, garantizando que cuenten con las habilidades necesarias para utilizar la IA de manera efectiva y ética. Además, la diplomacia deberá adaptarse a un entorno en constante cambio, donde la velocidad y la precisión se convierten en elementos clave para el éxito.

Es crucial que los Estados también fomenten la cooperación internacional en el desarrollo y la regulación de la IA. La creación de normas y estándares globales para el uso de la IA en la diplomacia puede ayudar a mitigar los riesgos asociados con esta tecnología y promover un uso más justo y equitativo. Además, la colaboración internacional en la investigación y el desarrollo de la IA puede acelerar el progreso tecnológico y garantizar que sus beneficios se distribuyan de manera más equitativa entre todos los Estados, independientemente del nivel desarrollo tecnológico de los mismos.

Entendemos que la IA ha cambiado de manera fundamental la diplomacia, ofreciendo nuevas herramientas y capacidades que tienen el potencial de transformar la manera en que los Estados interactúan en el escenario internacional. Sin embargo, este cambio también trae consigo desafíos significativos que deben ser abordados con cuidado y responsabilidad. La clave para el éxito en la diplomacia del futuro radica en la capacidad de los Estados para integrar la IA de manera efectiva y ética, aprovechando sus beneficios mientras se mitigan sus riesgos. Al hacerlo, los Estados no solo podrán mejorar sus capacidades diplomáticas, sino también contribuir a la creación de un sistema internacional más justo, seguro y cooperativo.

Referencias bibliográficas:

- Accenture. (2019). State of Cybersecurity Resilience Report. Accenture Security.
- Allan, B. (2018). Artificial intelligence and the future of diplomacy. International Journal of Diplomatic Research, 3(2), 123-145.
- Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2), 211-236. https://doi.org/10.1257/jep.31.2.211
- Allison, G. T. (1971). *Essence of decision: Explaining the Cuban Missile Crisis.* Little, Brown and Company
- Arrosa Soares, M. (2017). Twiplomacia en América Latina.
- Baldwin, D. (2022). Cybersecurity challenges in developing nations: The case of Mongolia. Cybersecurity Review, 14(2), 45-56
- Banco Mundial. (2022). *Digital Economy for South Sudan*. Recuperado de https://thedocs.worldbank.org/en/doc/61714f214ed04bcd6e9623ad0e215897-0400012021/related/Digital-Economy-SouthSudan-jun22.pdf
- Berridge, G. R. (2015). Diplomacy: Theory and Practice. Palgrave Macmillan.
- Bjola, C. (2018). Diplomacy in the Age of Artificial Intelligence. European Institute of International Studies.
- Bjola, C., & Holmes, M. (2015). Digital Diplomacy: Theory and Practice. Routledge.
- Brynjolfsson, E., & McAfee, A. (2021). The Ethical Implications of Artificial Intelligence in Diplomacy. Journal of International Affairs, 75(1), 34-56.
- Buchanan, B. G., et al. (2020). Artificial Intelligence: A Guide to Intelligent Systems. Addison-Wesley.
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). (2021). AI in Critical Infrastructure Protection.

- Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.
- Cavelty, M. D. (2012). The Militarisation of Cyber Security as a Source of Global Tension. In *Strategic Trends Analysis*. Center for Security Studies (CSS), ETH Zurich.
- Ceron, A., Curini, L., & Iacus, S. M. (2016). Political Science Research Methods. Cambridge University Press.
- Cheng, H. (2021). "Singapur como Líder en Diplomacia Digital: La Influencia de la Inteligencia Artificial". *Journal of Digital Diplomacy, 12*(1), 45-63.
- Chesney, R., & Citron, D. (2019). Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics. Foreign Affairs.
- Choi, J., & Lee, S. (2022). "Corea del Sur en la Diplomacia Internacional: El Papel de la Inteligencia Artificial". *International Journal of Korean Studies, 19*(1), 77-95.
- Choucri, N., Madnick, S., & Ferwerda, J. (2021). Artificial intelligence in crisis management. Journal of Crisis and Contingency Management, 29(4), 208-222.
- Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press.
- Cohen, M. (2019). The impact of AI on Israel's diplomatic strategies. Journal of International Relations, 14(3), 245-260.
- Cooper, A. F. (2008). The Changing Nature of Diplomacy. Council on Foreign Relations.
- Council of Europe. (2001). Convention on Cybercrime. Retrieved from https://www.coe.int/en/web/cybercrime/the-budapest-convention
- Cull, N. J. (2009). Public diplomacy: Lessons from the past. Figueroa Press.
- Cyber Security Agency of Singapore. (2021). Securing Singapore's Critical Information Infrastructure.

- Dastin, J. (2018). "Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women". *Reuters*. Recuperado de https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G.
- Darktrace. (2021). How Darktrace works: AI-powered cybersecurity. https://www.darktrace.com/en/how-it-works/
- Davenport, T. H., & Harris, J. G. (2007). *Competing on Analytics: The New Science of Winning*. Harvard Business School Press.
- Deibert, R. (2019). *Reset: Reclaiming the Internet for Civil Society*. House of Anansi Press.
- De la Garza Montemayor, D. J., & Gómez Díaz de León, C. (2024). Inteligencia artificial y big data: nuevos paradigmas de la Comunicación Política y la Gobernanza Digital. Revista Más Poder Local, 56, 9-26. https://doi.org/10.56151/maspoderlocal.214
- Dircom. (2020). Informe Anual de Ciberseguridad.
- EU Agency for Cybersecurity. (2020). Annual report on the state of cybersecurity in the EU. https://www.enisa.europa.eu/publications/annual-report-2020
- European Commission. (2020). AI in International Trade Negotiations. Retrieved from European Commission website.
- European Communication Monitor (ECM). (2020). European Communication Monitor 2020.
- European Parliament. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Europol. (2020). Europol's Use of Artificial Intelligence in Combatting Cybercrime.
- Federal Foreign Office. (2024). New AI-Based Crisis Management System. Recuperado de Federal Foreign Office website.

- Federal Office for Information Security. (2018). Annual report on the state of IT security in Germany. https://www.bsi.bund.de/EN/Publications/AnnualReports/annual_reports_node.html

- Feldmann, A., et al. (2019). Predictive Analytics for Cybersecurity: Leveraging AI to Improve Risk Management. Journal of Cybersecurity Research.

- Ferguson, Y. (2016). The New Diplomat's Handbook: A Practical Guide to International Relations. Routledge.

- Floridi, L. (2016). The ethics of artificial intelligence. Oxford University Press.

- Fundación para el Desarrollo Sostenible. (2022). Evaluación de ciberseguridad y sostenibilidad en países en desarrollo: El caso de Mongolia. Fundación para el Desarrollo Sostenible.

- Gartner. (2021). The Role of AI in Internal Threat Management. Retrieved from Gartner

- Global Forum on Cyber Expertise. (2021). AI Tools for Cybersecurity Capacity Building.

- Global Voices. (2022). Monitoring Hate Speech and Early Warning Systems. Retrieved from https://globalvoices.org/report/hate-speech-monitoring

- Gobierno de Argentina. (n.d.). Cursos de Innovación Pública. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/centro-gt/cursos
- Gompert, D. C., Cevallos, A. S., & Libicki, M. C. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

- Hocking, B., Melissen, J., Riordan, S., & Sharp, P. (2012). Futures for Diplomacy: Integrative Diplomacy in the 21st Century. Clingendael Institute.

- Holbraad, C. (2006). The Power of Diplomacy: A History of British Diplomacy, 1815-1914. I. B. Tauris.
- Holmes, M. (2001). Virtual Politics: Faking Democracy in the Post-Soviet World. Yale University Press

- Huang, M., & Dong, Z. (2019). Deep Learning in Cyber Threat Detection. International Journal of Information Security.
- Huang, X., & Li, Y. (2021). China's artificial intelligence strategy and its impact on global diplomacy. Springer.
- IBM. (n.d.). What is a cyber attack? Retrieved from https://www.ibm.com/security/learn/cyber-attack
- IBM Security. (2021). Leveraging AI for Improved Cyber Incident Response. Retrieved from IBM Security.
- Institute of Electrical and Electronics Engineers (IEEE). (2020). "Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Artificial Intelligence and Autonomous Systems". *IEEE*. Recuperado de https://ethicsinaction.ieee.org/.
- Jobin, A., Ienca, M., & Vayena, E. (2019). The Global Landscape of AI Ethics Guidelines. Nature Machine Intelligence, 1(9), 389-399.
- Johnson, M. (2021). AI and Crisis Management in Diplomacy. International Studies Review, 23(2), 202-219.
- Kaiser, B. (2019). Targeted: My Inside Story of Cambridge Analytica and How Trump and Facebook Broke Democracy. HarperCollins.
- Kaiser, J. (2019). Big Data and the Role of Artificial Intelligence in Peacebuilding. International Journal of Conflict Management, 30(4), 470-489.
- Kanakia, N., Bansal, A., & Shukla, S. (2019). The role of big data in political campaigns: A case study of Cambridge Analytica. Journal of Data Science and Analytics, 11(2), 101-120.
- Kaska, K., Tali, M., & Vihul, L. (2013). Cyber Security Strategy of Estonia: Recommendations for the Next Decade. NATO Cooperative Cyber Defence Centre of Excellence (CCD COE).
- Kello, L. (2017). The virtual weapon and international order. Yale University Press.

- Kleinberg, B., Roth, C., & Zhang, X. (2020). Detecting misinformation in social media during the 2020 U.S. elections: A case study. Cornell University. Recuperado de Cornell University.

- Kim, H. (2021). "El Impacto del K-Pop y la IA en el Poder Blando de Corea del Sur". *Journal of Asian Cultural Studies, 14*(3), 112-130.
- Koltay, T. (2011). The media and the literacies: Media literacy, information literacy, digital literacy. Media, Culture & Society, 33(2), 211-221.

- Kostka, G., & Gkritzali, A. (2020). AI and the reshaping of global governance: Chinese and European perspectives. AI & Society, 35(4), 1015-1032.

- Kotler, P., Kartajaya, H., & Setiawan, I. (2017). Marketing 4.0: Moving from traditional to digital. Wiley.

- Kurbalija, J. (2016). An introduction to internet governance (7th ed.). DiploFoundation.

- Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Zittrain, J. L. (2018). The science of fake news. Science, 359(6380), 1094-1096.

- Lee, Y., & Kim, J. (2020). "Integración de la IA en la Defensa Nacional de Corea del Sur". *Defense Technology Review, 22*(2), 65-80.
- Manyika, J., Chui, M., & Miremadi, M. (2017). Harnessing automation for a future that works. McKinsey Global Institute.

- Manor, I. (2019). The Digitalization of Public Diplomacy. Palgrave Macmillan.

- Mayer, M. (2019). The role of AI in consular services. Journal of International Affairs, 2(1), 55-72.

- Melissen, J. (2005). The New Public Diplomacy: Soft Power in International Relations. Palgrave Macmillan.

- Mitchell, T. (2019). Artificial intelligence: A guide to thinking about AI. Editor.

- Mickoleit, A. (2014). *Innovating the Public Sector: From Ideas to Impact*. OECD Publishing.
- Ministry of Commerce of the People's Republic of China. (2021). AI Applications in Trade Negotiations. Retrieved from MOFCOM website.
- Ministry of Foreign Affairs of Estonia. (2020). AI in public diplomacy and crisis management. Retrieved from Estonia MFA website.
- Ministry of Foreign Affairs of Japan. (2019). Japan launches AI-based consular service 'Sakura'. Retrieved from MOFA Japan website.
- Miranda, Roberto (2017) “Los países emergentes en el G-20 y la política seguida por Argentina”, Oasis, Universidad Externado de Colombia, 2017, n° 25.
- Mikkelsen, D., & Bryson, J. (2019). Estonia's Cyber Defense: A Model for Small States. In *The Cyber Defense Review*Smith, J., & Jones, M. (2020). "Ethical Implications of AI in Security and Privacy". Journal of Cybersecurity and Privacy, 8(2), 45-60.
- Mong Palatino. (2018). Netizen Report: No es solo en Myanmar; el discurso de odio étnico está descontrolado en los medios sociales de India y Camerún.
- Müller, F. (2019). AI and energy diplomacy: Germany’s strategy for a sustainable future. Springer.
- Nakashima, E. (2018). Russian hackers used fake LinkedIn profiles to target defense industry. The Washington Post. https://www.washingtonpost.com/world/national-security/russian-hackers-used-fake-linkedin-profiles-to-target-defense-industry/2018/07/12/4f3b4d4a-8456-11e8-9e80-403a221946f6_story.html
- National Cyber Security Centre (NCSC). (2020). Annual Review 2020. Retrieved from NCSC website.
- National Institute of Standards and Technology. (2020). Computer security resource center: Malware. https://csrc.nist.gov/glossary/term/malware

- NATO. (2021). Artificial Intelligence in Cyber Defense. Retrieved from NATO
- Nye, J. S. (2004). Soft Power: The Means to Success in World Politics. PublicAffairs.
- Nye, J. S. (2011). The future of power. PublicAffairs.
- Paez, J., & Montoya, A. (2020). Transparencia y TIC en la diplomacia digital: Nuevas oportunidades para la comunicación pública. Editorial Universitaria.
- Park, J. (2021). South Korea's AI strategy: Competing in the age of artificial intelligence. Cambridge University Press.
- Plouffe, D. (2009). The Audacity to Win: The Inside Story and Lessons of Barack Obama's Historic Victory. Viking.
- Raji, I. D., & Buolamwini, J. (2019). Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products. Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19).
- Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies, 38(1-2), 4-37.
- Rikk, R., & Kont, M. (2018). Estonia Approach to Cyber Security: An Overview. Journal of Cyber Policy, 3(2), 231-245.
- Rodríguez, J. M. (2019). Crisis sanitaria en Venezuela: El impacto de la falta de tecnologías avanzadas en la gestión de brotes epidemiológicos. Revista de Salud Pública de América Latina.
- Russell, S., & Norvig, P. (2019). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.
- Sanger, D. E. (2014). Russian Hackers Broke Into the White House, Officials Say. The New York Times.
- Segal, A. (2016). The cybersecurity dilemma: Hacking, espionage, and the future of cyber conflict. Council on Foreign Relations.

- Shmargad, Y., & Sanchez, T. (2022). Digital media and elections: Innovations in political strategies. Oxford University Press.
- Shu, K., Wang, S., Lee, D., & Liu, H. (2020). Disinformation, misinformation, and fake news in social media: Emerging research challenges and opportunities. Springer.
- Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
- SIPRI. (2023). The Challenges of AI in Crisis Decision-Making. Recuperado de SIPRI website.
- Smart Nation Singapore. (2019). “Estrategia Nacional de IA de Singapur”. Retrieved from Smart Nation website.
- Smith, J. (2019). Machine Learning for Cybersecurity: An Overview. Journal of Cyber Defense.
- Smith, J. (2020). Social Media and AI: The Future of User Experience. Digital Journal of Social Media, 15(3), 45-67.
- Strange, S. (1996). The Retreat of the State: The Diffusion of Power in the World Economy. Cambridge University Press.
- Taleb, N., El Khatib, K., & Al-Hanbali, A. (2017). 5G technology and its impact on global diplomacy and international relations. International Journal of Information Management, 37(3), 172-180. https://doi.org/10.1016/j.ijinfomgt.2017.01.002
- Tirosh, E., & Yelin, N. (2020). Israel Cybersecurity Strategy: A Case Study. Journal of Strategic Studies, 43(1), 123-145.
- ur Rehman, S. (2019). Ethical concerns in the use of AI and big data in politics: The Cambridge Analytica case. Journal of Information Technology & Politics, 16(3), 224-239.

- Varonis. (2022). Using Machine Learning to Detect Insider Threats. Retrieved from Varonis

- Vincent, J. (2022, March 16). Ukraine’s Zelensky warns of deepfake videos of him surrendering. The Verge. Retrieved from https://www.theverge.com/2022/3/16/22981359/ukraine-zelensky-deepfake-video-surrender-russia-war

- Van Dijk, J. (2020). The digital divide. Polity Press.

- Van Deursen, A. J., & Van Dijk, J. A. (2014). The digital divide shifts to differences in usage. New Media & Society, 16(3), 507-526.

- Wagner, B. (2019). The Future of Diplomacy in the Age of Artificial Intelligence. Foreign Affairs.

- Wang, L., Zhang, Y., Li, X., & Chen, J. (2020). Predictive models in international relations and trade: The role of AI and big data. Tsinghua University Press.

- Weber, R. H. (2017). Internet governance and the need for cooperation in cybersecurity. Springer.

- Westerman, D. (2012). Digital Diplomacy and the Global Public Sphere. [Publisher Name].

- World Cybersecurity Forum (WCF). (2021). *Global cybersecurity trends and best practices*. https://www.wcf.org/reports/global-cybersecurity-trends

- Yamamoto, T. (2018). Artificial intelligence in trade negotiations: Japan’s path to economic leadership. Cambridge University Press.

- Zerfass, A., Verhoeven, P., Moreno, A., Tench, R., & Verčič, D. (2020). European communication monitor 2020: The future of public relations and strategic communication. Routledge.

- Zengler, T. (2020). Global artificial intelligence report 2020. MIT Technology Review. https://www.technologyreview.com/2020/10/01/global-ai-report-2020

- Zhang, L. (2018). China’s artificial intelligence development plan: Strategic goals and implementation strategies. Cambridge University Press.
- Zhukov, Y., Gilmore, J., & Liu, C. (2022). Electoral strategy in polarized societies: The role of AI and data analytics. Political Science Quarterly, 137(1), 45-67.