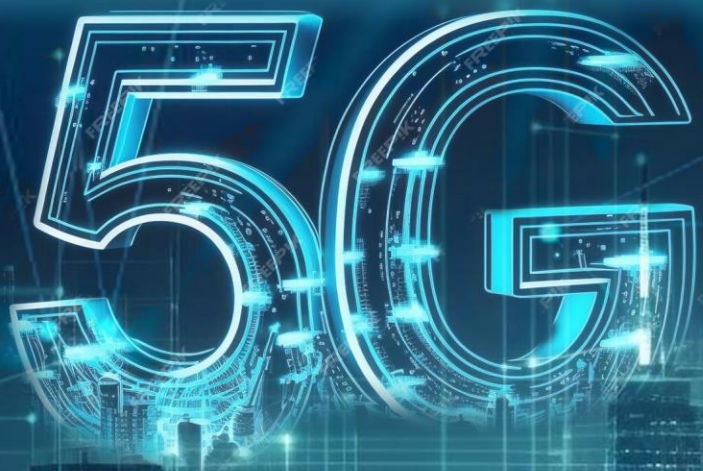
SEGURIDAD Y DEFENSA
ICP POLICY LAB

LA TECNOLOGÍA 5G CHINA y los riesgos para Colombia

Análisis comparado y recomendaciones de política



ICP
DESDE 1987

KONRAD ADENAUER STIFTUNG

La tecnología 5G china y los riesgos para Colombia
Análisis comparado y recomendaciones de política

ISBN: 978-628-95318-1-7

Autores
Carlos Augusto Chacón Monsalve
Director ejecutivo

Laura Herrera
Investigadora *Senior* del ICP

Andrea Calle
Coordinadora de Investigación

Edición y corrección de estilo
Andrea Calle
Coordinadora de Investigación

Katherinn Cuervo
Coordinadora de comunicaciones

Stefan Reith
Representante para Colombia KAS

Andrea Valdelamar
Coordinadora de Proyectos KAS

Diseño y diagramación
Luisa Peña
Profesional en comunicaciones

Fundación Konrad Adenauer - KAS
Calle 93b #18-12
(+57) 601 743 0947 Bogotá, D.C., Colombia.
www.kas.de/web/kolombien

Instituto de Ciencia Política Hernán Echavarría Olózaga - ICP
Calle 70 #7a - 29
(+57) 313 431 20 95
www.icpcolombia.org

Diciembre 2023
Bogotá, Colombia

Contenido

Resumen

La adopción de la tecnología 5G representa una transformación significativa en la conectividad global. Sin embargo, adjudicar estas redes sin condiciones suficientes de seguridad plantea desafíos para la seguridad de los países, la integridad de la información y los datos del sector público y privado, la atracción de inversión y los procesos de innovación. Este documento examina la introducción de la tecnología 5G de empresas chinas en Colombia, centrándose en las preocupaciones legítimas relacionadas con la seguridad nacional y la ciberseguridad, debido a la legislación de ese país y a los riesgos de que existan "puertas traseras". Este análisis propone que la implementación de la tecnología 5G no solo es una cuestión tecnológica, sino una decisión estratégica cuya finalidad debe ser preservar la seguridad nacional y evitar desincentivar la inversión y la innovación.

Abstract:

While the adoption of 5G technology represents a significant transformation in global connectivity, awarding these networks without sufficient security conditions poses challenges for the security of countries, the integrity of public and private sector information and data, as well as investment attraction and innovation processes. This paper examines the introduction of 5G technology from Chinese companies in Colombia, focusing on legitimate concerns related to national security and cybersecurity, due to that country's legislation and the risks of "backdoors". This analysis proposes that the implementation of 5G technology is not only a technological issue, but a strategic decision whose purpose should be to preserve national security and avoid discouraging investment and innovation.

Presentación

China se ha convertido en las últimas décadas en uno de los principales socios comerciales de América Latina y el Caribe. Los intercambios comerciales pasaron de 14.000 millones en el 2000 a 500.000 millones en el 2022 (CEPAL, 2023). Además, ese país otorga préstamos, invierte en el desarrollo de proyectos en sectores estratégicos, entre ellos infraestructura, energías renovables y telecomunicaciones, y tiene presencia a través de empresas en sectores minero-energéticos.

En la región 21 países hacen parte de la iniciativa de la Franja y la Ruta (BRI por sus siglas en inglés), con la cual China desde el 2013 implementa una estrategia de desarrollo de infraestructura y cooperación internacional con el fin de reforzar su posición como un actor relevante en el contexto global y asegurar sus intereses nacionales y continuar por la senda trazada por Xi Jinping, quien en el 20º Congreso del Partido Comunista Chino (PCCh) ha reconocido que *"la influencia internacional, el atractivo y el poder de moldear de China han aumentado notablemente"* (Nikkei Asia, 2022).

La forma como ha aumentado ese poder de moldear las relaciones chinas con el resto del mundo, especialmente en términos de las relaciones de dependencia creadas mediante acuerdos comerciales, inversiones y desarrollo de proyectos de infraestructura, ha empezado a ser cuestionada, tanto por los intereses nacionales que persigue el PCCh que van más allá de la cooperación y el comercio internacional en el marco de un orden internacional basado en reglas, como por los métodos y los resultados, en muchos casos cuestionables como sucedió en Venezuela (Fundación Andrés Bello, 2023).

Como lo hemos advertido desde el Instituto de Ciencia Política Hernán Echavarría Olózaga -ICP-, es importante entender cómo China influye, utilizando diferentes tácticas que incluyen acciones de poder blando (soft power) y/o de poder incisivo (sharp power). Las relaciones económicas y de inversión, especialmente en áreas estratégicas, pueden tener consecuencias reales para los países. Esto es algo que debe considerarse, teniendo en cuenta los objetivos del PCCh y sus expresiones de poder a través de empresas privadas controladas por el PCCh, así como en organismos multilaterales donde ese país ha ganado una importante influencia.

En el marco de la cuarta revolución industrial, China ha concentrado sus esfuerzos en convertirse en una potencia técnica capaz de competir geopolíticamente con Estados Unidos y las economías más desarrolladas del mundo. Uno de los principales campos de competencia se desarrolla en el ámbito de las redes móviles de quinta generación -5G-, con implicaciones en materia económica, política, de seguridad y defensa.

En materia económica la tecnología 5G ofrece oportunidades que van más allá de los equipos de redes móviles, como son los relacionados con sectores de la economía digital, el internet de las cosas, la inteligencia artificial, y la producción y distribución de energía, entre otros. En el campo político y de seguridad tiene implicaciones en materia de información, datos, algoritmos, almacenamiento en la nube, secretos industriales, ciberseguridad y ciberdefensa, los cuales tienen efectos en la sociedad, la estabilidad de la democracia, el desarrollo productivo y la infraestructura crítica.

En el contexto de las telecomunicaciones y el desarrollo de redes móviles 5G se ha identificado que existe un riesgo real respecto a la confiabilidad de los protocolos de seguridad para el almacenamiento y la gestión de la información y los datos, dada la relación entre las empresas de telecomunicaciones de ese país (especialmente Huawei y ZTE) y el gobierno chino.

En diversas regiones del mundo, se ha planteado la posibilidad de que las empresas chinas que suministran tecnología 5G puedan tener "puertas traseras" que permitan el acceso remoto. Esta preocupación conlleva riesgos significativos, incluyendo la amenaza a la seguridad de la información y los datos, la integridad de la infraestructura de las redes, nubes y servidores. Asimismo, se destaca el potencial de instrumentalización de estos servicios en situaciones de conflictos geopolíticos, lo que podría comprometer gravemente la seguridad de los equipos de red.

Estos riesgos subrayan la tensión inherente entre las oportunidades brindadas por la tecnología 5G de China, tanto en términos de costos como de innovación, y las preocupaciones relativas a la seguridad y la independencia. Este escenario ha motivado a numerosos países a tomar decisiones políticas restrictivas y/o implementar mecanismos para abordar posibles amenazas asociadas con la tecnología china. Estas medidas se centran en las cadenas de suministro, la integridad de la información y los datos, así como la estabilidad y los niveles de dependencia que podrían surgir en el ámbito de la conectividad.

En Colombia el 20 de diciembre de 2023 se llevará a cabo la subasta para otorgar permisos de uso del espectro radioeléctrico a nivel nacional, que incluye las bandas remanentes del 4G y la banda de 3500 MHz en la que se empezará a desplegar la tecnología 5G. Un proyecto fundamental para que el país pueda mejorar las condiciones de conectividad y competitividad.

Considerando que, en el contexto colombiano, las empresas de telecomunicaciones que participan en la subasta utilizan infraestructura proporcionada por empresas chinas en diversos porcentajes, que van desde el 50 % hasta el 100 %, es esencial que, más allá del aspecto económico, al otorgar estos permisos se realice una evaluación crítica de su confiabilidad, relevancia y

factibilidad. Además, se deben tomar medidas con respecto a las posibles implicaciones derivadas de depender exclusivamente de un solo proveedor.

Por esta razón, el Instituto de Ciencia Política Hernán Echavarría Olózaga y la Fundación Konrad Adenauer, en el marco del ICP Policy Lab, consideran indispensable promover un debate informado con el fin de promover la adopción de un marco regulatorio para una política de relacionamiento y gobernanza respecto a las tecnologías 5G, garantizando las condiciones de seguridad informática de las redes móviles, la confiabilidad de los proveedores extranjeros y la autonomía estratégica en este sector.

Si bien el pragmatismo parece ser la premisa rectora de diversos sectores respecto a las relaciones con China, tanto la opinión pública y como los tomadores de decisión deben reconocer que parte de la estrategia para mitigar riesgos y garantizar la resiliencia en un sector tan importante y al mismo tiempo vulnerable, consiste en garantizar la diversidad de proveedores y en definir criterios técnicos y no técnicos para evaluar su confiabilidad.

1. Introducción

La evolución de la conectividad hacia la tecnología 5G predice una transformación significativa en la interconexión global e innovación, delineando un nuevo paradigma en la estructura de las naciones y sus economías. Al reconocer la importancia estratégica de estas infraestructuras a nivel mundial, han surgido desafíos cruciales, especialmente para actores destacados en el ámbito tecnológico, como la empresa china Huawei.

En los últimos años, la compañía ha enfrentado una resistencia global y una prudencia cada vez más evidente entre los gobiernos, manifestadas a través de la suspensión de proyectos piloto, la limitación de colaboraciones e incluso la prohibición directa de la participación de Huawei en mercados locales de infraestructura 5G como sucedió recientemente en Costa Rica.

Este documento explora las complejidades asociadas a la introducción de la tecnología 5G procedente de empresas chinas en el contexto colombiano, examinando las preocupaciones legítimas relacionadas con la seguridad nacional y la ciberseguridad. En el centro de estas preocupaciones se encuentra la dependencia exclusiva de empresas chinas para la implementación del 5G, debido a que las experiencias internacionales exponen su posible vulnerabilidad frente al control ejercido por los servicios de inteligencia del gobierno chino.

Asimismo, el contexto colombiano presenta desafíos adicionales derivados de la carencia de una infraestructura y de legislación acorde a los desafíos y las dinámicas del sector, adaptada a las complejidades de las redes 5G. La falta de una base sólida en estos aspectos expone al país a riesgos significativos en términos de seguridad nacional.

Por consiguiente, la implementación de la tecnología 5G no puede considerarse únicamente como una cuestión tecnológica; más bien, se erige como una decisión estratégica que demanda un enfoque integral, que adopte estándares rigurosos de seguimiento y evaluación a la implementación, configuración y operaciones, que incorpore mejores prácticas y que se sustente en un marco regulatorio a partir de un benchmarking normativo, en particular en materia de protección de datos, privacidad y ciberseguridad.

En este contexto, el presente análisis propone examinar de qué manera la tecnología 5G china incidirá en Colombia, partiendo de la hipótesis que sugiere que dicha incidencia podría representar un riesgo considerable en términos de ciberseguridad para el país y de dependencia en el largo plazo. Experiencias internacionales han demostrado los peligros de depender únicamente de tecnología 5G proveniente de empresas chinas, las cuales, como se resalta, pueden estar controladas por los servicios de inteligencia chinos.

2. Revisión de literatura:

La denominación 5G hace referencia a la quinta generación de redes móviles, marcando un avance significativo desde las antiguas redes 1G hasta la actual 4G. Cada generación ha ampliado las capacidades de las redes móviles, desde la simple capacidad de hablar (1G) hasta la banda ancha y el streaming en tiempo real (4G). Por su parte el 5G, como proceso evolutivo, busca maximizar la conectividad y ofrecer velocidades excepcionales, permitiendo navegar a velocidades de hasta 10 GBps, diez veces más rápido que las ofertas de fibra óptica actuales. Además, la baja latencia, reducida a 5 milisegundos, posibilitará la conexión prácticamente en tiempo real (MinTIC, 2019).

Aparte de la velocidad, el 5G permitirá un aumento exponencial en el número de dispositivos conectados, desde vehículos y robots industriales hasta dispositivos electrónicos en el hogar (Flores, 2022). El 5G abrirá oportunidades para la implementación de tecnologías emergentes como el Internet de las Cosas (IoT) y la Inteligencia Artificial (IA), así como el desarrollo de proyectos de ciudades inteligentes y vehículos autónomos (MinTIC, 2019). Este avance beneficiará no solo al sector de las telecomunicaciones, sino a diversos sectores como comunicaciones, agricultura, salud, servicios financieros, entretenimiento, turismo,

entre otros, que involucran las actividades cotidianas del ser humano, democratizando nuevos productos y servicios.

La incorporación de esta tecnología requiere de una infraestructura específica, los componentes clave de la infraestructura 5G incluyen torres RAN y la infraestructura de celdas pequeñas 5G. Además, la infraestructura 5G ofrece cobertura de baja latencia para flujos de datos masivos que alimentan equipos de IoT y vehículos semiautónomos (Tribunal de Cuentas Europeo, 2022)

Según Mordor Intelligence[1] (2022), los actores clave en el mercado global de infraestructura 5G son: Hewlett Packard Enterprise Development LP, Huawei Technologies Co. Ltd, Ceragon, Samsung Electronics Co. Ltd, Nokia Corporation, JMA Wireless, Telefonaktiebolaget LM Ericsson, ZTE Corporation, Altiostar, Cisco Systems Inc., Casa Systems, Mavenir, NEC Corporation, CommScope Inc., Parallel Wireless, Comba Telecom Systems Holdings Ltd., Fujitsu Limited, Airspan Networks y Aviat Networks Inc. Sin embargo, no todas las empresas comparten el mismo nivel de capacidades e inversiones en los temas clave de la industria.

Cabe señalar que las compañías chinas han tenido gran incidencia en el mercado global del 5G, especialmente Huawei. En las últimas tres décadas, Huawei se ha convirtió en la empresa de telecomunicaciones más grande del mundo, reportando ingresos por USD $91.500 millones en 2022, cuenta con 3 mil millones de usuarios de sus productos y servicios, opera en más de 170 países, 75 lanzamientos y pruebas comerciales de 5G y ha contado con hasta USD $75.000 millones en apoyo del gobierno chino desde 1987, año de su creación (Berman et al., 2023).

Según el portal alemán de estadística, Statista (2023), China liderará el número de conexiones 5G en los próximos cinco años, con un aumento significativo en los ingresos del mercado. Dónde Huawei se ha destacado entre los demás proveedores de esta tecnología, ya que ha sido la compañía que más ha contribuido al avance tecnológico del 5G en China, especialmente en el mercado de teléfonos inteligentes.

Es importante señalar que Huawei ha invertido en tecnologías en la nube e infraestructuras para mantener su liderazgo en el mercado tanto nacional como internacional (Slotta, 2023). Sin embargo, ha tenido que afrontar sanciones por parte de Estados Unidos y algunos países europeos, entre otros, lo cual ha afectado su participación en el mercado de la tecnología 5G.

[1] Empresa de investigación de mercados.

Algunos expertos han planteado la posibilidad de que el gobierno chino esté desempeñando un papel significativo en Huawei, e incluso se ha visto como una *"extensión comercial del Partido Comunista Chino"* (Berman et al., 2023).

Se han puesto de manifiesto los riesgos frente a la vulnerabilidad de depender de proveedores chinos de 5G, destacando posibles riesgos para sistemas críticos, la colaboración militar y el posible uso de la infraestructura 5G para labores de espionaje, lo cual genera riesgos para la seguridad nacional. (Nouwens, 2021)

Como se ha podido evidenciar, China busca estratégicamente aprovechar el valor militar del 5G, evidenciado en patentes y aplicaciones de doble uso desarrolladas por instituciones de investigación y empresas privadas. Aunque no cuenta con una estrategia militar independiente para el 5G, como algunos estados de la OTAN, los funcionarios del Ejército Popular de Liberación de China -EPL- han explorado su papel en futuros conflictos bélicos. Instituciones vinculadas al EPL han presentado patentes relacionadas con tecnologías de doble uso para el 5G, desde la Universidad de la Fuerza de Cohetes que describe una red de comunicaciones para un "internet militar de las cosas" hasta la Academia de Ciencias Militares que presenta tecnología de drones con comunicación 5G. Estas patentes indican el interés del EPL en la investigación y desarrollo del 5G para aplicaciones de uso dual, aunque expertos señalan la necesidad de evaluar la calidad de estas presentaciones. En consecuencia, las investigaciones futuras deben abordar desafíos y oportunidades de las aplicaciones militares y de doble uso en las redes 5G, monitorear los planes de China y proponer medidas para mantener la ventaja de la OTAN (WU, 2023).

Por otra parte, Huawei ha sido señalada por, presuntamente, llevar a cabo prácticas corruptas, inflar costos e incurrir en demoras injustificadas en el desarrollo de los contratos que le son adjudicados (Farivar, 2019). Esta compañía también ha sido acusada de aprovechar situaciones con regímenes corruptos y aliarse con el partido de gobierno para filtrar información sobre los ciudadanos, especialmente la oposición (International Republican Institute, 2022).

Este comportamiento se refleja en varios casos concretos, como en Algeria (Saarinen, 2012) y Uganda (Privacy International, 2020), donde Huawei ha sido objeto de investigaciones por prácticas corruptas. Además, en diversos proyectos, como el Islamabad Safe City Project en Pakistán (Shahid, 2019), el acuerdo entre Huawei y TelOne en Zimbabwe (Mukandatsama, 2015) y el de Entel Bolivia (La Nación, 2010) Huawei ha enfrentado críticas por sobrecostos y demoras significativas en la ejecución de los contratos, e incluso ha sido sancionado por incumplimientos contractuales.

Por otro lado, China enfrenta acusaciones de emplear la llamada "trampa de la deuda" como un instrumento diplomático. Mediante préstamos e inversiones en infraestructura, bajo la justificación de construir y fortalecer la Ruta de la Seda, China ha buscado ejercer influencia a nivel mundial, especialmente en países menos desarrollados. Las acusaciones expresan temores de que China pueda asumir el control de estos activos o utilizarlos como herramienta de presión en futuras negociaciones (Clark, 2023).

En ese contexto, las compañías chinas, especialmente Huawei, ha venido enfrentando dificultades considerables en el ámbito global debido a la percepción de riesgos relacionados con la seguridad nacional, la transparencia en la contratación y en la ejecución de los proyectos, así como en los riesgos a la inversión privada que surgen en torno a sus contribuciones a las infraestructuras 5G.

3. Estudios de caso: Incidencia de la tecnología 5G china

En ese contexto, existen casos específicos que vale la pena traer a colación, en los que la ciberseguridad de varios países se ha visto afectada por compañías como Huawei y ZTE. En primera instancia se examinará el caso de algunos países europeos y la Unión Europea, así como Australia, Canadá y Costa Rica.

3.1. Análisis de caso de Países europeos

- El Reino Unido en el año 2020 tomó la decisión de prohibir a Huawei y a otros proveedores que consideraba una amenaza significativa para la seguridad de las redes 5G. El año pasado, amplió el plazo para eliminar el equipo de Huawei de la red central 5G hasta finales de 2023 (Sandle, 2022).
- Por su parte, el parlamento de Estonia en 2021 aprobó una nueva legislación que prohíbe a los operadores de telecomunicaciones optar por proveedores chinos de equipos de telecomunicaciones (Barton, 2021).
- En Dinamarca el mismo año, legisladores daneses aprobaron una legislación que permite la selección de inversiones extranjeras con el fin de asegurar que no representen una amenaza para la seguridad nacional (Veyet et al., 2023).
- En cuanto a Francia, en 2020, las autoridades francesas informaron a los operadores de telecomunicaciones que tenían la intención de adquirir equipos 5G de Huawei que no podrían renovar las licencias para dicho equipo una vez que expiren, lo que conlleva a una eliminación gradual de Huawei de las redes móviles (Veyet et al., 2023).
- En lo que respecta a Alemania, el Ministerio del Interior propuso una medida que requeriría a los operadores de telecomunicaciones eliminar todos los componentes críticos fabricados por Huawei y ZTE de sus redes centrales 5G para el año 2026 (Marsh, 2023).

- Aunque Italia no ha implementado una prohibición total de los equipos de Huawei, en 2020 impidió que el grupo de telecomunicaciones Fastweb firmara un acuerdo para que Huawei suministrara equipos para su red 5G (Veyet et al., 2023).
- Por su parte, Letonia firmó un acuerdo con Estados Unidos centrado en la seguridad 5G, diseñado para restringir las operaciones de empresas chinas en el país (LRN, 2020).
- En Lituania en 2021, el parlamento de Lituania decretó que solo el equipo aprobado por el gobierno, por razones de seguridad nacional, podría ser utilizado en la red 5G de próxima generación del país (Veyet et al., 2023).
- El organismo de control de las telecomunicaciones de Portugal anunció el 18 de septiembre de 2023 que estaba colaborando con los operadores para implementar una resolución de alto nivel que impediría la presencia del equipo de Huawei en las redes móviles 5G del país (Goncalves, 2023).
- En el año 2021, el gobierno de Rumania aprobó un proyecto de ley respaldado por Estados Unidos que efectivamente excluía a China y a Huawei de participar en el desarrollo de la red 5G del país (Marinas, 2021).
- Suecia, de igual forma, tomó la medida de prohibir en 2020 los equipos de telecomunicaciones de Huawei y ZTE en su red 5G (Mukherjee, 2022).

3.2. Análisis del caso de la Unión Europea

A nivel comunitario, el Parlamento Europeo adoptó en 2019 la resolución sobre las amenazas en materia de seguridad relacionadas con la creciente presencia tecnológica de China en la Unión Europea y la posible acción a escala de la Unión para reducirlas. Se toman en consideración las preocupaciones sobre los vendedores de equipos de terceros países, especialmente tras la implementación de la Ley china de seguridad del Estado. Esta Ley establece amplias obligaciones para ciudadanos y entidades, como el deber de colaborar con las agencias de inteligencia nacionales, sin restricción alguna incluso sin la garantía de que no sea aplicada extraterritorialmente. Ante esta situación, distintos países han reaccionado de diversas maneras, desde evaluaciones de seguridad hasta prohibiciones totales, debido al riesgo percibido para la seguridad de la Unión.

Por esta razón, en la resolución se proponen medidas tanto a nivel de la UE como en cada uno de los Estados miembros con el fin de hacer frente a los riesgos que se identifican a causa de las acusaciones de posibles puertas traseras en equipos 5G de empresas chinas que podrían facilitar el acceso no autorizado a datos y comunicaciones de la Unión. También señala la inquietud ante posibles vulnerabilidades en estos equipos durante el despliegue de las redes 5G en los años venideros.

Esta resolución del Parlamento Europeo considera que, en diciembre de 2018, la autoridad nacional de ciberseguridad de la República Checa emitió una

advertencia sobre las amenazas a la seguridad asociadas con las tecnologías proporcionadas por las empresas chinas Huawei y ZTE. El caso de la República Checa es parte del reporte **"Entendiendo el riesgo de las empresas chinas de tecnologías de la información y comunicación (TIC): La perspectiva de la República Checa"** elaborado por el Proyecto Sinopsis, una organización sin ánimo de lucro de ese país, el cual ha sido traducido y divulgado por el ICP en Colombia.

En marzo de 2019, tras el respaldo del Consejo Europeo a un enfoque coordinado para la seguridad de las redes 5G, la Comisión Europea adoptó la mencionada Recomendación sobre ciberseguridad en las redes 5G. Esta recomendación instó a los Estados miembros a realizar evaluaciones de riesgos nacionales y preparar una Caja de Herramientas con medidas de mitigación. Cada Estado completó su evaluación y transmitió los resultados a la Comisión y la Agencia Europea de Ciberseguridad - ENISA (Unión Europea, 2020) En octubre de 2019, los Estados miembros publicaron un informe coordinado de riesgos en ciberseguridad en redes 5G, identificando amenazas, vulnerabilidades y activos sensibles. Las conclusiones del Consejo, llevado a cabo en diciembre de 2019, respaldaron el enfoque coordinado y la aplicación efectiva de la Recomendación para evitar la fragmentación en el mercado único, instando a tomar medidas para garantizar la seguridad de las redes 5G.

En junio de 2023 la Comisión Europea anunció los próximos pasos en materia de ciberseguridad de las redes 5G como complemento al último informe sobre la implementación de la Caja de Herramientas de la UE para la ciberseguridad en la red 5G. **Se destaca que 24 Estados miembros están adoptando medidas legislativas para evaluar y restringir proveedores de alto riesgo, y 10 ya han impuesto restricciones, incluyendo a Huawei y ZTE**.

La Comisión, en su comunicación, expresa fuertes preocupaciones sobre los riesgos de ciertos proveedores, respalda las decisiones de excluir a Huawei y ZTE de las redes 5G, considerándolos riesgos más altos según la Caja de Herramientas 5G. Por lo tanto, la Comisión implementará medidas de ciberseguridad en línea con la caja de herramientas 5G, evitando el uso de Huawei y ZTE en sus comunicaciones corporativas. Se tomarán medidas de seguridad para no adquirir nuevos servicios de conectividad de estos proveedores y se trabajará con Estados miembros y operadores para eliminar gradualmente su presencia en servicios existentes de conectividad en sitios de la Comisión.

Un aspecto muy importante que hace parte de la decisión de la Comisión tiene que ver con la intención de reflejar estas medidas en todos los programas e instrumentos de financiamiento relevantes de la Unión Europea. Esta decisión resulta relevante si se tienen en cuenta las relaciones con la UE, en particular frente a las iniciativas y

proyectos en el marco de la asociación estratégica birregional y del acuerdo comercial de Colombia con ese bloque.

3.3. Análisis del caso de Australia.

Según Peter Hartcher (2021), Australia prohibió a Huawei en su red 5G debido a preocupaciones de seguridad nacional, principalmente el riesgo de interferencia del gobierno chino. Las agencias de inteligencia, incluyendo Australia Security Intelligence Organisation (ASIO) y la Dirección de Señales de Australia, encontraron que permitir a Huawei, que tenía fuertes lazos con el gobierno chino, suministrar infraestructura 5G podría llevar a espionaje potencial, intrusión cibernética y compromiso de infraestructura crítica.

En 2019 Mike Burgess, director general de la Dirección Australiana de Señales (ASD), enfatizó en la importancia de asegurar la infraestructura crítica sobre las amenazas a la ciberseguridad. Por lo que la prohibición se basa en el temor de que compañías como Huawei, con sede en países con leyes que podrían obligarlas a cooperar con esfuerzos de inteligencia nacional, representan un riesgo (Smyth, 2019). Lo anterior, hace referencia a la Ley Nacional de Inteligencia de China, que obliga a todas las organizaciones y ciudadanos a apoyar el trabajo de inteligencia del estado.

En ese contexto, el gobierno australiano identificó un riesgo en la posibilidad de que dichas compañías cierren o interfieran con servicios críticos como redes eléctricas, suministros de agua y sistemas de alcantarillado, de los cuales el país dependerá cada vez más a medida que integren la tecnología 5G. Concluyendo que los riesgos no podían mitigarse y era imperativo optar por prohibir a Huawei suministrar equipos 5G debido a preocupaciones de seguridad nacional (Hartcher, 2021; Smyth, 2019).

Por otro lado, la ASD, en coordinación con otras agencias de seguridad, evaluó a los fabricantes de equipos chinos, incluidos Huawei y ZTE, y colocó el 5G en la parte superior de la lista de infraestructura crítica, debido a la dependencia anticipada de varias industrias en esta tecnología (Smyth, 2019).

Esta preocupación sobre la infraestructura crítica, hace referencia a la expectativa de que muchas industrias dependerán fuertemente de la tecnología 5G. Se espera que el 5G sea la base para tecnologías emergentes y sistemas esenciales, como redes de energía, comunicaciones, transporte, servicios públicos, entre otros. La dependencia de estas industrias en la tecnología 5G significa que cualquier vulnerabilidad o control indebido sobre esta tecnología podría tener consecuencias significativas para la seguridad nacional e incluso la economía.

Por lo tanto, al poner el 5G en lo más alto de la lista de infraestructura crítica, la ASD y otras agencias australianas destacan la importancia de proteger estos sistemas y la necesidad de garantizar que los proveedores de equipos 5G sean confiables y no estén bajo la influencia de gobiernos extranjeros que podrían tener intereses contrarios a los de Australia.

3.4. Análisis del caso de Canadá.

En 2022, el gobierno canadiense anunció la prohibición de que los operadores de telefonía móvil instalen equipos de Huawei y ZTE en sus redes 5G de alta velocidad. Canadá, que era el único miembro de la alianza Five Eyes[2] sin restricciones previas para Huawei, se unió a Estados Unidos, Gran Bretaña, Australia y Nueva Zelanda en la prohibición de esta empresa china (Gobierno de Canadá, 2022).

Por su parte, Estados Unidos ha estado presionando a sus aliados, incluyendo a Canadá, para que excluyan a Huawei de las redes móviles 5G debido a preocupaciones de ciberespionaje. Este país advirtió que reconsideraría el intercambio de inteligencia con Estados que usen equipos de Huawei, aunque la compañía ha negado repetidamente las acusaciones.

El exembajador de Canadá en China, Guy Saint-Jacques, ha manifestado que esa decisión debió haberse tomado hace años, puesto que China a través del tiempo se ha vuelto más agresiva en la forma en que obtiene información para lograr sus objetivos. Según la ley china, ninguna empresa puede rechazar una solicitud del gobierno chino para compartir información. Saint-Jacques concluyó que China ha utilizado el comercio como arma en disputas anteriores, y esta no sería la excepción (The Associated Press, 2022).

3.5. Análisis del caso Costa Rica

En el contexto de la iniciativa de seguridad informática impulsada por Costa Rica tras el hackeo al Ministerio de Hacienda y otras entidades en abril de 2022, el país ha tomado la decisión de desarrollar una normativa para garantizar la ciberseguridad en las redes 5G, que establece requisitos estrictos para las redes y servicios de telecomunicaciones, incluyendo un régimen de protección a la intimidad y derechos de los usuarios (Cordero, 2023).

[2] Alianza en temas de inteligencia que integra cinco países: Australia, Canadá, Estados Unidos, Nueva Zelanda y Reino Unido.

Este reglamento impone la obligación a operadores y proveedores de implementar sistemas y medidas técnicas y administrativas necesarias para la seguridad de la información, abordando el riesgo existente de interceptación de información confidencial por agentes extranjeros para fines de espionaje y la intromisión de Estados a través de la cadena de suministro. Asimismo, busca evitar riesgos asociados a la dependencia de un único proveedor (Cordero, 2023).

A partir de dicho reglamento se establece que los procesos de compra pública incorporan mecanismos para verificar que los oferentes hayan considerado los aspectos relacionados con la gestión y mitigación de los riesgos. Asimismo prohíbe la participación de compañías provenientes de países no suscritos al Convenio sobre ciberdelincuencia de Budapest de 2001, incluyendo a China y Rusia, en los procesos de licitación de 5G del país (Heinze et al, 2023).

En ese entendido, Huawei se ha quedado por fuera de la subasta anticipada para la adopción de tecnología 5G (El Espectador, 2023). Esta elección se fundamenta en las preocupaciones significativas relacionadas con la ciberseguridad.

4. Posibles riesgos a tener en cuenta de poner en manos de empresas chinas esta tecnología en Colombia.

China ha planteado como una de sus prioridades en materia internacional, el establecimiento de una Ruta de la Seda digital, mediante la cuál busca afianzar su liderazgo mundial. Para ello ha usado dos estrategias (1) suscribir acuerdos de cooperación con diferentes países alrededor del mundo, incluyendo América Latina y (2) promover inversiones tecnológicas por parte de empresas chinas, como sucede en Colombia actualmente con Huawei frente al 5G (Colombia Risk Analysis, 2023).

Las preocupaciones de seguridad relacionadas con la tecnología china van más allá del acceso o control de la infraestructura nacional. Las redes 5G deben ser consideradas como parte de la amplia integración de tecnologías chinas a través de la Ruta Digital de la Seda. La preocupación por posibles puertas traseras en la infraestructura de red es solo una de las inquietudes de seguridad para los gobiernos al decidir la integración de tecnología china en infraestructuras críticas. Aunque los debates se centran en la privacidad de datos, la seguridad de la infraestructura crítica y las implicaciones militares, la literatura aún no aborda ampliamente las repercusiones de la Ruta Digital de la Seda en las industrias de defensa occidentales.(Nouwens, 2021)

Como se hace evidente en acápites anteriores, varios países han manifestado sus preocupaciones por la intervención de empresas chinas que prestan servicios de

tecnología 5G en sus países, por considerarlo una amenaza a la seguridad nacional. Es importante que el Estado colombiano tenga en cuenta este tipo de situaciones en el marco de la subasta del espectro radioeléctrico que llevará a cabo el Ministerio de las Tecnologías de la Información y las Comunicaciones el próximo 20 de diciembre de 2023. Aunque los participantes en el proceso son principalmente operadores, como Claro, Tigo, Movistar, WOM y Telecall, en el ámbito de la implementación de esta tecnología y en el sector empresarial en general, hay otros actores significativos como aquellos que suministran la infraestructura, Huawei es uno de ellos.

En Latinoamérica, los ingresos de Huawei en el año 2022 superaron los US$4.300 millones. Sin embargo, en diversas naciones de Latinoamérica y el Caribe, la geopolítica está desempeñando un papel decisivo en la implementación de la tecnología 5G. Un caso ilustrativo es el de Costa Rica, que ha decidido no incluir a Huawei en la subasta adelantada en su país para adoptar esta tecnología, basándose en preocupaciones relacionadas con ciberseguridad.

La organización Colombia Risk Analyst ha resaltado que "*No es fácil comprender el papel que juega el PCCh en las decisiones de inversión internacional y en el establecimiento de estrategias de inversión y desarrollo. La falta de transparencia en la gobernanza corporativa de las empresas chinas crea un entorno altamente especulativo, propenso a malas interpretaciones y malentendidos*" (Colombia Risk Analysis, 2023).

A pesar de los antecedentes y las implicaciones significativas para la seguridad y el desarrollo estratégico del país, en Colombia no se impondrán restricciones a esta empresa, ni se ha abordado en el ámbito político la necesidad de avanzar en el desarrollo de normativas y regulaciones para implementar protocolos y mecanismos que garanticen las condiciones de seguridad y protección de la información y los datos. Este tema ha pasado desapercibido tanto en la esfera pública como en las instancias de toma de decisiones, generando interrogantes sobre si esto se debe a la falta de conocimiento o a la eficacia del lobby de las empresas y el gobierno chino. En los últimos años, dicho lobby ha involucrado acciones de diplomacia estatal, pública y académica, incluyendo viajes de congresistas de diversos partidos a China (Cardenal, 2021).

En ese sentido, en esta sección se abordarán los posibles riesgos a los que se enfrenta Colombia, que deben ser tenidos en cuenta por el gobierno, de poner en manos de empresas chinas esta tecnología. Lo anterior se analizará desde tres puntos: a) falta de experticia en Colombia sobre tecnología 5G, b) riesgo de monopolio de Huawei en términos de infraestructura y de prestación del servicio y c) importancia de esta tecnología para Colombia.

4.1. Falta de experticia en Colombia sobre tecnología 5G.

Desde el punto de vista técnico existen varios retos en Colombia para desplegar la tecnología 5G. Según César Funes (2023), vicepresidente de Relaciones Institucionales de Huawei Latinoamérica, son los siguientes: "*despliegue de infraestructura; poner a disposición tanto espectro como sea posible para el sector, al precio correcto y en el tiempo correcto; incentivar la demanda; y garantizar cobertura en áreas rurales*" (El Espectador, 2023).

Es importante resaltar que Colombia carece de una protección efectiva ante temas de Ciberseguridad. A pesar de haber realizado varios intentos para formular una política pública en cuanto al tema, a la fecha no existe ninguna. Sin embargo, se han implementado instrumentos de política en función de la ciberseguridad, como el Centro Cibernético Policial del 2001 y el Grupo Investigativo de Delitos Informáticos que hoy se denomina Grupo de Investigaciones Tecnológicas (GITEC).

Además, en el país no se cuenta con una entidad que establezca políticas y acciones que propendan por la seguridad digital. Por ejemplo, Estados Unidos cuenta con la Agencia de Ciberseguridad e Infraestructura de seguridad (CISA, por sus cifras en inglés); en España existe el Instituto Nacional en Ciberseguridad (INCIBE); Italia cuenta con la Agencia Nacional de Ciberseguridad; el Reino Unido tiene el Centro Nacional en Ciberseguridad (NCSC); Australia el Centro de Ciberseguridad australiano (ACSC); Canadá el Centro de Ciberseguridad canadiense; Alemania la Oficina Federal de Alemania para la Seguridad de la Información; y la Unión Europea con la Agencia Europea de Ciberseguridad.

Aunque Colombia cuenta con una amplia normativa frente al tema, no tiene un mecanismo que permita una adecuada implementación y la articulación interinstitucional e interagencial requerida. A modo de ilustración, desde el año 2005 las organizaciones han venido aplicando los lineamientos de la norma ISO 27001, que recoge los procedimientos y los recursos necesarios en algunos casos para proteger los datos y la información. También se cuenta con la Ley 1273 de 2009, por medio de la cual se modifica el código penal y crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos", creando diez tipos penales nuevos.

La Ley 1581 de 2021 establece el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar su información personal. El Decreto 1008 de 2018, sobre lineamientos generales de la política de gobierno digital. Asimismo, en el 2022 el Gobierno Nacional expidió el Decreto 338 que da los lineamientos para organizar el ecosistema digital y su seguridad, así como la implementación de la gobernanza de dicho ecosistema.

Posteriormente, con el CONPES 3701 "Lineamientos de política para la Ciberseguridad y Ciberdefensa" del año 2011, se asignó al Centro Cibernético Policial como responsable de la Ciberseguridad en Colombia. En 2016 el Departamento Nacional de Planeación (DNP) emitió un nuevo documento CONPES 3854 "Política Nacional de Seguridad Digital" en el cual se fortalece la seguridad digital del país. En el 2020 se emitió el CONPES 3995 "Política Nacional de Confianza y Seguridad Digital", el cual crea el Grupo de Respuestas a Emergencias Cibernéticas de Colombia (COLCERT).

Finalmente, en el marco del PND 2022-2026 se incluyeron los artículos 307 y 308 que crearían la Agencia de Seguridad Digital y Asuntos Espaciales; aunque este artículo no fue aprobado en la discusión legislativa, la necesidad de la creación de la Agencia quedó establecida en las bases del PND 2022-2026. Actualmente, el Ministerio de Tecnologías de la información y la comunicación (MinTIC) presentó al Congreso un proyecto de ley para crear la mencionada agencia.

Como se mencionó anteriormente, en Colombia no existe un indicador con el que actualmente se mida o se pueda ilustrar con certeza el grado de ciberseguridad. Adicionalmente, los mecanismos existentes no están articulados, por lo que no se puede hacer un seguimiento preciso sobre este tema en el país, lo que dificulta la actualización, mejora de procesos e intercambio de buenas prácticas permanentemente.

Por lo tanto, es importante mencionar que, a través de un centro unificado de ciberseguridad, se pueden utilizar medios específicos para mitigar riesgos en este campo, ya que permitiría una evaluación periódica sobre el status de la ciberseguridad en el país. Lamentablemente, Colombia no cuenta con una política pública de Estado que pueda ejercer como un mecanismo de control sobre un posible ataque, identificación y mitigación de amenazas a la infraestructura digital del país.

4.2. Riesgo de monopolio de Huawei en términos de infraestructura y de prestación del servicio.

En el marco de la llegada de la tecnología 5G, el Estado colombiano debe tener en cuenta los posibles riesgos del monopolio de Huawei en términos de infraestructura y de prestación del servicio. Kaska et al. (2019), exponen los riesgos que enfrentan los países al poner en manos de empresas como Huawei tecnología de este tipo.

En primera medida, las preocupaciones que han tenido otros países se han basado en la relación entre las empresas de tecnología de comunicaciones chinas y sus

servicios de inteligencia, reforzadas por el entorno político y legal de China que exige la cooperación con las agencias de inteligencia. Por lo tanto, adoptar tecnología 5G de Huawei introducirá una dependencia crítica de los equipos que potencialmente pueden ser controlados por los servicios de inteligencia chinos y el ejército, tanto en tiempos de paz como en crisis.

Como se mencionó anteriormente, Huawei ha sido vinculado con casos de espionaje en varios países. Algunos Estados tienen reservas sobre otras compañías de comunicaciones chinas como ZTE, Hytera Communications Corporation, Hangzhou Hikvision y Dahua Technology, cuya tecnología ha sido prohibida en redes gubernamentales de Estados Unidos (US Congress, 2018).

Por otro lado, la Ley de Inteligencia Nacional de China de 2016 requiere que todas las empresas "*apoyen, brinden asistencia y cooperen en el trabajo de inteligencia nacional, y resguarden el secreto de cualquier trabajo de inteligencia nacional del cual tengan conocimiento. El Estado protegerá a individuos y organizaciones que respalden, cooperen y colaboren en el trabajo de inteligencia nacional*". De igual forma, la Ley de Contrainteligencia de 2014, junto con sus actos de implementación, establece obligaciones para las "organizaciones e individuos pertinentes" de proporcionar información, instalaciones u otra asistencia, y establece que las "organizaciones e individuos pertinentes" "no deben negarse" a cooperar. (Hoffman & Kania, 2018).

Estas acciones brindan escasa certeza en cuanto a la existencia de una supervisión judicial o pública efectiva para prevenir la introducción de posibles vulnerabilidades, en caso de que el Estado considere necesario hacerlo en aras de su amplia concepción de preservar la seguridad nacional, subrayando así la vital importancia de la ciberseguridad.

La presencia de la tecnología de Huawei en las redes de comunicaciones críticas implica que formaría parte integral de la infraestructura central de comunicaciones del país, en la cual se apoyan diversos servicios esenciales y funciones socioeconómicas (Kaska et al., 2019). Como se ha hecho evidente, Huawei tiene antecedentes de ciberespionaje en varias partes del mundo donde ha sido sancionado y excluido de los procesos de licitación. Entregar infraestructura crítica a un proveedor con un historial de desconfianza podría llegar a ser contraproducente para salvaguardar no solo la ciberseguridad, sino la seguridad nacional.

Por otro lado, es importante resaltar que quienes harían uso de estas redes no son únicamente entidades públicas, sino empresas privadas que manejan información reservada, como secretos industriales y empresariales. La protección de esta información es crucial en los procesos de innovación, pues estos conllevan altos

costos no sólo económicos sino en capital humano y de tiempo. Además, son inversiones de alto riesgo pues existe la posibilidad de que el proyecto no dé como resultado el producto esperado, que no tenga suficiente acogida en el mercado, ni genere rentabilidad o retorno a la inversión.

A pesar de ello lo que motiva a las empresas a continuar con la investigación e innovación es la expectativa futura de tener una ventaja frente a sus competidores. Sin embargo, si existen riesgos inminentes de que esta información sea captada por el gobierno chino y las empresas público privadas de este país, donde la mano de obra y los costos de producción son menores, este riesgo se hace mucho mayor y se desincentiva la innovación.

El riesgo asociado con la contratación de empresas como Huawei para desarrollar la infraestructura de tecnología 5G también actúa como un factor desalentador para la inversión. Las compañías extranjeras, especialmente aquellas originarias de países donde Huawei y otras empresas similares enfrentan sanciones o prohibiciones, podrían no ver a Colombia como un destino atractivo para invertir. **¿Por qué una empresa optaría por establecerse aquí si no existen garantías suficientes de seguridad?** Aquellas que decidan hacerlo probablemente elijan implementar redes privadas, lo cual conlleva costos adicionales en sus operaciones. Este desembolso adicional en la inversión podría generar dudas sobre la viabilidad de estar presente en Colombia.

4.3. Importancia de esta tecnología para Colombia.

El Plan 5G del Ministerio de las Tecnologías de la Información y las Comunicaciones de 2019, destaca la importancia de la introducción exitosa de la tecnología 5G en Colombia, señalando que no solo se requiere la evolución de infraestructuras y redes de telecomunicaciones, sino también el desarrollo de un ecosistema completo de plataformas, servicios y contenidos mediante la innovación y el emprendimiento. Se resalta la necesidad de fortalecer el sector de Tecnologías de la Información y Comunicación (TIC) para llegar a todos los habitantes (MinTIC, 2019).

Adicionalmente, el Departamento Nacional de Planeación evaluó el impacto de aumentos en la penetración de Internet, con velocidades adecuadas, en la desigualdad de ingresos en Colombia, medida por el índice de GINI (DNP, 2018). Se concluye que un incremento significativo en la penetración de Internet para los quintiles de ingresos más bajos puede reducir este índice, contribuyendo a cerrar brechas sociales.

Según un informe de la OCDE (2019), los beneficios económicos de la tecnología 5G recaen en su potencial para impulsar la innovación y satisfacer las crecientes demandas de la economía digital. Puesto que representa un nuevo enfoque para sistemas de comunicación convergentes, donde el objetivo es hacer un uso más eficiente de los recursos disponibles, permitiendo el desarrollo de servicios y aplicaciones nuevas y mejoradas. El beneficio económico completo de 5G en todo el mundo podría materializarse para 2035 en sectores como transporte, salud, educación e IoT industrial (OCDE, 2019).

Una Colombia conectada a 5G puede mejorar la competitividad, la productividad de las regiones y generar empleo, lo que tendría impactos significativos en la reactivación económica y sentaría las bases para el desarrollo adecuado de la Cuarta Revolución Industrial (MinTIC, 2019).

En ese sentido, "más que una tecnología de comunicaciones, el 5G será el sistema nervioso de las sociedades contemporáneas" (Kaska et al., 2019), por lo que se requiere que el proveedor de esta tecnología cuente con la mayor supervisión y confianza. Dejar en manos está responsabilidad en una empresa que se encuentra sancionada y limitada en su accionar por considerarse una amenaza para la seguridad de los Estados, merece la evaluación cautelosa y reconsideración por parte de las autoridades colombianas.

4.4. Proceso de licitación

El Ministerio de Tecnologías de la Información y la Comunicación (MinTIC), mediante Resolución definitiva 3947 de 2023 declaró la apertura del proceso de selección objetiva mediante el mecanismo de subasta para otorgar permisos de uso del espectro radioeléctrico a nivel nacional, así como los requisitos, condiciones y el procedimiento para participar.

> *"Las bandas que se están subastando corresponden a espectro remanente en las bandas donde actualmente operan los sistemas 4G (700 MHz, 1900 MHz, AWS extendida, 2500 MHz) y a la banda de 3500 MHz. Para el caso de 3500 MHz, banda en la que se empezará a desplegar la tecnología 5G, cada bloque de los 4 dispuestos de 80 MHz tiene un valor de reserva de $317.717 millones*" (MinTIC, 2023).

El 4 de diciembre de 2023 cuatro operadores fueron habilitados para participar en el proceso de asignación de permisos: Comunicación Celular Comcel (Claro), Telecall Colombia S.A.S. (promesa de sociedad futura), Partners Colombia (WOM) y la Unión Temporal Colombia Móvil - Telefónica, fueron habilitados para participar en el proceso de asignación de permisos (MinTIC, 2023).

"*La subasta se celebrará el próximo 20 de diciembre y el permiso del uso del espectro dura hasta 2044, con la posibilidad de renovar según los operadores y el Gobierno. Con el fin de evitar una monopolización del espectro radioeléctrico, se subastarán diferentes bloques correspondientes a las diferentes bandas*" (Colombian Risk Analyst, 2023).

Actualmente, Huawei cuenta con participación en el sector de telecomunicaciones de Colombia, mediante equipos e infraestructura para el desarrollo de redes 3G y 4G. Según Colombia Risk Analysis (2023) el 50% de las redes de Claro y Movistar y el 100% de las redes de Tigo y WOM, son proveídas por Huawei.

A pesar de los evidentes riesgos que puede traer permitir a Huawei proveer la infraestructura para las redes 5G en el país, gran parte de los requisitos para competir en esta licitación se concentran en la capacidad para la prestación del servicio, pero no se incluyen condición mínimos de seguridad y ciberseguridad, que mantengan la privacidad de los datos que circulan por dichas redes.

"*Las decisiones de inversión en tecnología deben evaluarse no sólo bajo criterios técnicos sino también bajo consideraciones geopolíticas. A menos que Colombia establezca normas y especificaciones claras para las inversiones en el sector tecnológico con el fin de promover la interoperabilidad, podría abrir un espacio para la dependencia injustificada, la influencia o poner al país en riesgo de quedar anclado con los proveedores chinos, lo que podría poner a otros competidores en desventaja e ir en contra de algunos acuerdos comerciales firmados*". *(Heinze, 2023)*

5. Conclusiones y recomendaciones al gobierno de Colombia para tener en cuenta sobre la adjudicación de un contrato con empresas chinas.

A medida que más países reconocen la importancia estratégica de estas infraestructuras, han surgido desafíos frente al desarrollo de los proyectos para implementar las tecnologías 5G, en particular frente a los riesgos identificados cuando los proveedores son empresas chinas.

La suspensión de proyectos piloto y colaboraciones, así como las prohibiciones anunciadas por algunos países para la participación de Huawei y ZTE en el mercado local de infraestructura 5G, demuestran la creciente resistencia y cautela respecto a la participación de esta y otras empresas chinas en las redes 5G de los

países. Estos obstáculos están vinculados, en parte, a tensiones geopolíticas y a las preocupaciones sobre la seguridad de la tecnología 5G.

Como se ha señalado, algunos países han implementado diversas medidas para salvaguardar la seguridad de sus redes 5G, proporcionando valiosas lecciones que Colombia debería considerar y adoptar. Entre estas buenas prácticas se incluyen:

(i) **definir procesos para la revisión periódica de las vulnerabilidades en los estándares técnicos y no técnicos**, que garanticen condiciones de seguridad y confiabilidad, con el fin de determinar criterios para adoptar decisiones sobre eventuales restricciones o prohibiciones a los intercambios y transacciones que puedan comprometer la seguridad nacional en el ámbito de la tecnología 5G;

(ii) supervisar por medio de entidades reguladoras del servicio de comunicaciones la prestación de estos servicios entre el país y el extranjero, **diseñando mecanismos que permitan evaluar el riesgo para identificar las maneras de explotar y comprometer las redes móviles, así como certificar la confiabilidad de los proveedores de la tecnología 5G**;

(iii) desarrollar normativas que regulen la comercialización de dispositivos emisores de radiofrecuencia, **fundamentadas en estudios de certificación que determinen el nivel de riesgo que representan para el Estado colombiano,** con el fin de desarrollar capacidades que permitan construir y mantener redes móviles seguras y resilientes; y,

(iv) desplegar protocolos de inteligencia para identificar los proveedores que pueden ser considerados riesgosos por comprometer la infraestructura, los servidores y la nube. **A partir del análisis de riesgo y evaluación periódica, exigir a los operadores que sus proveedores de la tecnología 5G cuenten con los máximos estándares de seguridad y ciberseguridad, así como su total independencia de cualquier gobierno o legislación extranjera que pueda poner en riesgo la integridad de la información y los datos, estableciendo incluso si se debe prohibir el uso de equipos y servicios de determinadas empresas.**

Adicionalmente, la discusión sobre la tecnología 5G no es un tema meramente tecnológico, puesto que involucra a otros sectores que en un futuro podrían verse afectados por un mal manejo de esta herramienta. Sobre todo, tiene implicaciones económicas y de seguridad nacional. Como lo menciona Kaska et al (2019), considerar la seguridad de las 5G simplemente como un asunto de seguridad digital y no tener en cuenta una posible dimensión de seguridad nacional podría resultar en última instancia más costoso y perjudicial para el bienestar de la sociedad a largo plazo.

La introducción de la tecnología 5G de China en Colombia plantea inquietudes legítimas en términos de ciberseguridad para el país. La preocupación principal se centra en la dependencia exclusiva de empresas chinas para la implementación del 5G, pues las experiencias internacionales evidencian la posibilidad de que estas empresas estén sujetas al control del servicio de inteligencia chino. Esta dependencia plantea interrogantes sobre la seguridad de la red y la protección de datos sensibles.

Por otra parte, se destaca que Colombia enfrenta desafíos adicionales debido a la falta de infraestructura y legislación integral relacionada con la red 5G. La ausencia de una base sólida en estos aspectos podría exponer al país a riesgos significativos en términos de seguridad cibernética y operativa.

Por esta razón, las condiciones de ciberseguridad constituyen un asunto crítico que debe ser abordado teniendo en cuenta tanto los aspectos técnicos y tecnológicos, como los geopolíticos. Esto impone la necesidad de reconocer los riesgos y considerar las implicaciones que tendría la interrupción de las redes móviles más allá de la telefonía celular o de la captura de información y datos, tanto de los personales, como del gobierno o el sector privado.

No se trata necesariamente de excluir competidores únicamente por ser empresas de un origen específico. En el caso de las empresas chinas su nivel de riesgo se asocia a la legislación de ese país, dado que están obligadas a colaborar con organismos de inteligencia sin la posibilidad de oponerse, incluso en situaciones que involucren información privilegiada y sensible tanto pública como privada. Además de los riesgos frente a la posibilidad de que existan "puertas traseras" en la infraestructura que estas empresas proveen. Bajo ese entendido, sería improbable que estas empresas cumplan con los criterios más rigurosos de acuerdo a estrictos estándares de seguridad.

Hasta tanto no se modifique la legislación de ese país, logrando garantizar la total independencia de las empresas privadas de proveedores de tecnología 5G, y no existan todas las condiciones que le permitan a Colombia anticiparse e identificar oportunamente la presencia de "puertas traseras", a través de las cuales se podría acceder y filtrar información y datos, es necesario observar con atención las medidas que han tomado otros países y llevar a cabo los ajustes necesarios en la normativa interna para tener un estricto control sobre la tecnología proveniente de dichas empresas.

6. Referencias

Asamblea Popular Nacional de China. (2017). Ley Nacional de Inteligencia de China. https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf

Barton, J. (2021). Estonia aligning with Europe against Huawei. Developing Telecoms. https://developingtelecoms.com/telecom-business/telecom-regulation/12394-estonia-aligning-with-europe-against-huawei.html

Berman, N., Maizland, L., & Charzky, A. (2023, febrero 8). Is China 's Huawei a Threat to U.S. National Security? Council on Foreign Relations. https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security

Cardenal, J. P. (2021). El arte de hacer amigos. El Partido Comunista Chino y los partidos en América. Fundación Konrad Adenauer. Latinahttps://dialogopolitico.org/documentos/dp-enfoque/dp-enfoque-nro-3-el-arte-de-hacer-amigos/

CEPAL. (2023). Perspectivas del Comercio Internacional de América Latina y el Caribe. Naciones Unidas. https://repositorio.cepal.org/server/api/core/bitstreams/1228f586-a9f3-4e82-8584-acf932c2da04/content

Clark, N. (2023). The Rise and Fall of the BRI. Council on Foreign Relations. https://www.cfr.org/blog/rise-and-fall-bri

Comisión Europea. (2023). La Comisión anuncia los próximos pasos en materia de ciberseguridad de las redes 5G como complemento al último informe de situación de los Estados miembros. https://ec.europa.eu/commission/presscorner/detail/en/IP_23_3309

Congreso de la República de Colombia. (2009). Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Congreso de la República de Colombia. (2012). Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

CONPES 3701. (2011). Lineamientos de Política Pública para Ciberseguridad y Ciberdefensa. Bogotá. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

CONPES 3854. (2016). Política Nacional de Seguridad Digital. Bogotá. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CONPES 3995. (2020). Política Nacional de Confianza y Seguridad Digital. Bogotá. En: https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3995.pdf

Consejo de Europa. "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. http://www.secretariasenado.gov.co/senado/basedoc/ley_1928_2018.html

Cordero, C. (2023). Esto dice el decreto presidencial que prohibiría a China (Huawei) ser proveedor de 5G en el país. El financiero. https://www.elfinancierocr.com/ef-de-la-manana/gobierno-emitio-decreto-que-prohibe-compras-a/GPS76Z37CFALDBM7GPZFWEL57E/story/

DNP. (2018). Colombia productiva y sostenible. Un propósito de todos. Bogotá: DNP.

El Espectador. (2023, octubre 28). 'Nos quedaremos hasta que nos lo permitan': Huawei sobre América Latina. ELESPECTADOR.COM. https://www.elespectador.com/economia/empresas/huawei-sobre-america-latina-nos-quedaremos-hasta-que-nos-lo-permitan-noticias-hoy/

Farivar, M. (2019). Bribery, Corruption Charges Follow Huawei Around World. VOA. https://www.voanews.com/a/huawei-alleged-corruption-and-bribery/4781242.html

Flores, J. (2022, diciembre 15). Qué es el 5G y cómo nos cambiará la vida. www.nationalgeographic.com.es. https://www.nationalgeographic.com.es/ciencia/que-es-5g-y-como-nos-cambiara-vida14449

Fundación Andrés Bello. (2023). Seguimiento de los fondos conjuntos entre China y Venezuela. Centro de Investigación Chino Latinoamericano. https://fundacionandresbello.org/wp-content/uploads/2023/05/Informe-Ejecutivo-Seguimiento-Fondos-China-Venezuela.pdf

Gobierno de Canadá. (2022). Declaración política - Garantizar la seguridad del sistema de telecomunicaciones canadiense. https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement--securing-canadas-telecommunications-system.html

Gobierno de Costa Rica. (2023). Reglamento sobre medidas de ciberseguridad aplicables a los servicios de telecomunicaciones basados en la tecnología de quinta generación y superiores. https://www.imprentanacional.go.cr/pub/2023/08/31/ALCA166_31_08_2023.pdf

Goncalves, S. (2023). Portugal's telecom watchdog working with operators to bar Huawei. Reuters. https://www.reuters.com/business/media-telecom/portugals-telecom-watchdog-working-with-operators-bar-huawei-

2023-09-18/

Hartcher, P. (2021, mayo 21). Huawei? No way! Why Australia banned the world's biggest telecoms firm. The Sidney Morning Herald. https://www.smh.com.au/national/huawei-no-way-why-australia-banned-the-world-s-biggest-telecoms-firm-20210503-p57oc9.html

Heinze, C; Guzmá, S; & Poveda, D. (2023). Colombia Is Unprepared to Handle the Risks of Chinese Tech Investment. Global Americans. https://theglobalamericans.org/2023/12/colombia-is-unprepared-to-handle-the-risks-of-chinese-tech-investment/

Heinze, C; Guzmá, S; & Poveda, D. (2023). Entendiendo la huella tecnológica de China en Colombia. Colombia Risk Analysis. https://www.colombiariskanalysis.com/post/entendiendo-la-huella-tecnol%C3%B3gica-de-china-en-colombia

Hoffman, S., & Kania, E. (2018, septiembre 12). Huawei and the ambiguity of China's intelligence and counter-espionage laws. The Strategist. https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/

International Republican Institute. (2022). Global Thought Work. Case Studies on PRC Influence in Africa's Information Space. https://www.iri.org/wp-content/uploads/2022/04/Global-Thought-Work-Case-Studies-on-PRC-Influence-in-Africas-Information-Space.pdf

Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a Security Threat. Tallinn NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf

La Nación. (2010). Bolivia multa con $8 millones a Huawei por incumplir contrato. La Nación. https://www.nacion.com/economia/bolivia-multa-con-8-millones-a-huawei-por-incumplir-contrato/B67MBHUZXBD23NRRSUQ2KOOK6U/story/?print=1

LRT. (2020). Latvia signs 5G declaration with US to sideline China. https://www.lrt.lt/en/news-in-english/19/1146924/latvia-signs-5g-declaration-with-us-to-sideline-china

Marinas, R. (2021). Romania approves bill to bar China, Huawei from 5G networks. Reuters. https://www.reuters.com/business/media-telecom/romanian-govt-approves-bill-bar-china-huawei-5g-networks-2021-04-15/

Marsh, S.; Rinke, A. & Ersen, H. (2023). German proposal for Huawei curbs triggers telecom operator backlash. Reuters. https://www.reuters.com/business/media-telecom/german-interior-ministry-wants-force-5g-operators-slash-huawei-use-official-2023-09-19/

MinTIC. (2019). Plan 5G Colombia. El Futuro Digital es de Todos. Ministerio de Tecnologías de la Información y las Comunicaciones.

https://mintic.gov.co/micrositios/plan5g//764/w3-channel.html

MinTIC. (2023). Con la Resolución 3947 de 2023, el MinTIC reglamenta el proceso de la subasta 5G. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/281096:Con-la-Resolucion-3947-de-2023-el-MinTIC-reglamenta-el-proceso-de-la-subasta-5G

MinTIC. (2023). MinTIC confirma que los cuatro operadores interesados en la subasta 5G están habilitados para participar. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/327094:MinTIC-confirma-que-los-cuatro-operadores-interesados-en-la-subasta-5G-estan-habilitados-para-participar

Mordor Intelligence. (2022). Análisis del tamaño y la participación del mercado global de infraestructura 5G tendencias y pronósticos de crecimiento (2023 - 2028). https://www.mordorintelligence.com/es/industry-reports/5g-infrastructure-market.

Mukandatsama, V. (2015). $98 Million Telone-Huawei deal delay raises question marks. TechZim. https://www.techzim.co.zw/2015/09/98-million-telone-huawei-deal-delay-raises-question-marks/#.VwzJaqR97IU

Mukherjee, S. (2022). Swedish court upholds ban on Huawei sale of 5G gear. Reuters. https://www.reuters.com/business/media-telecom/swedish-court-upholds-ban-huawei-sale-5g-gear-2022-06-22/

Nikkei Asia. (2022). Transcript: President Xi Jinping's report to China's 2022 party congress. https://asia.nikkei.com/Politics/China-s-party-congress/Transcript-President-Xi-Jinping-s-report-to-China-s-2022-party-congress

Nowens, M. (2021). China's Digital Silk Road: Integration into National IT Infrastructure and Wider Implications for Western Defence Industries. The International Institute for Strategic Studies - IISS. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/china-digital-silk-road---iiss-research-paper.pdf

OCDE. (2019). The road to 5G networks: Experience to date and future developments (OECD Digital Economy Papers 284; OECD Digital Economy Papers, Vol. 284). https://doi.org/10.1787/2f880843-en

Parlamento Europeo. (2019). Resolución del Parlamento Europeo, de 12 de marzo de 2019, sobre las amenazas en materia de seguridad relacionadas con la creciente presencia tecnológica de China en la Unión y la posible acción a escala de la Unión para reducirlas (2019/2575(RSP)).

Privacy International. (2020). Huawei infiltration in Uganda. https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda

Saarinen, J. (2012). Huawei, ZTE banned from Algeria. IT News. https://www.itnews.com.au/news/huawei-zte-banned-from-algeria-304858

Sandle, P. (2022). UK extends deadline to remove Huawei equipment from 5G

network core. Reuters. https://www.reuters.com/business/media-telecom/uk-extends-deadline-remove-huawei-equipment-5g-network-core-2022-10-13/

Shahid, J. (2019). Technical evaluation of Safe City project will be carried out: DIG. DAWN. https://www.dawn.com/news/1484195

Slotta, D. (2023, 31). 5G in China—Statistics & facts. Statista. https://www.statista.com/topics/6705/5g-technology-in-china/

Smyth, J. (2019, marzo 27). Australia banned Huawei over risks to key infrastructure. Financial Times. https://www.ft.com/content/543621ce-504f-11e9-b401-8d9ef1626294

Sytas, A. (2021). Lithuania looks to ban 'untrustworthy' phones after Chinese censorship concerns. Reuters. https://www.reuters.com/technology/lithuania-looks-ban-untrustworthy-phones-after-chinese-censorship-concerns-2021-09-24/

The Associated Press. (2022, mayo 20). Canada bans China's Huawei Technologies from 5G networks. NPR. https://www.npr.org/2022/05/20/1100324929/canada-bans-chinas-huawei-technologies-from-5g-networks#:~:text=Canada%20bans%20China%27s%20Huawei%20Technologies%20from%205G%20networks%20%3A%20NPR&text=Canada%20bans%20China%27s%20Huawei%20Technologies%20from%205G%20networks%20Wireless%20carriers,the%20giant%20Chinese%20technology%20company.

The Economist Times. (2023, febrero 12). From Huawei to TikTok, Chinese tech giants face scrutiny amid spying concerns—ET Telecom. ETTelecom.Com. https://telecom.economictimes.indiatimes.com/news/from-huawei-to-tiktok-chinese-tech-giants-face-scrutiny-amid-spying-concerns/97838302

Tribunal de Cuentas Europeo. (2022). Informe especial 03 2022: Despliegue de la tecnología 5G en la UE: Retrasos en el despliegue de redes y problemas de seguridad que siguen sin resolverse. https://op.europa.eu/webpub/eca/special-reports/security-5g-networks-03-2022/es/

Unión Europea. (2020). Ciberseguridad de las redes 5G Caja de herramientas de la UE de medidas de mitigación de riesgos. El Grupo de Cooperación en materia de Redes y Sistemas de Información. https://ccdcoe.org/uploads/2020/01/EU-200129-Cybersecurity-of-5G-networks-EU-Toolbox-of-risk-mitigating-measures.pdf

US Congress. (2018). Text—H.R.5515—115th Congress (2017-2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019 | Congress.gov | Library of Congress. Congress.gov. https://www.congress.gov/bill/115th-congress/house-bill/5515/text

Veyet, T., Pothitos, A., & Lenkiewicz, L. (2023, septiembre 29). European countries

who put curbs on Huawei 5G equipment. Reuters. https://www.reuters.com/technology/european-countries-who-put-curbs-huawei-5g-equipment-2023-09-28/

Wu, H. (2023) China's Approach to Military 5G Networks and Related Military Applications.NATO Cooperative Cyber Defence Centre of Excellence - CCDCOE. https://ccdcoe.org/uploads/2023/03/20230314-003_5GChina_HWu.pdf


SEGURIDAD Y DEFENSA
ICP POLICY LAB
5G
ICP
DESDE 1987
KONRAD
ADENAUER
STIFTUNG