# Huawei, a mi manera o a la calle: ¿qué debe hacer la UE?

Ian Bond


***El 15 de mayo, el presidente estadounidense Donald Trump declaró "una emergencia nacional por las amenazas contra la tecnología y los servicios de información y comunicaciones en Estados Unidos". El propósito de su decisión parecía ser callar a China y, más en concreto, al gigante de las telecomunicaciones Huawei, que ha quedado fuera del mercado de la tecnología 5G en el país norteamericano. Sin embargo, el 23 de mayo, Trump pareció dar a entender que podría estar dispuesto a pasar por alto las preocupaciones de seguridad suscitadas por la compañía dentro de un acuerdo comercial con China.***

La primera declaración de Trump marcó una escalada del conflicto entre el Gobierno de EE UU y Huawei. Estados Unidos alega que Huawei tiene vínculos con los servicios de inteligencia chinos y ha violado las sanciones norteamericanas al suministrar productos que incluyen tecnología estadounidense a países prohibidos como Irán. La segunda declaración enturbió las aguas, al insinuar que la preocupación por la seguridad desaparecería si China ofreciese un acuerdo comercial apropiado. El año pasado se produjo una situación similar cuando el otro gran proveedor chino de material de telecomunicaciones, ZTE, fue acusado de violar las sanciones estadounidenses contra Irán y Corea del Norte, pero evitó el castigo de Trump cuando el presidente Xi Jinping convenció al líder norcoreano, Kim Jong-un, de que aceptara celebrar una cumbre con Estados Unidos.

La disputa con Huawei es ilustrativa de un problema más amplio que se le plantea a la UE: a medida que Estados Unidos trata a China, cada vez más, como un "adversario extranjero", los

demás países se sienten más presionados para tomar partido. Si Estados Unidos prohíbe la inclusión de tecnología propia esencial en los dispositivos de Huawei, en la práctica, obligará a los países europeos a escoger a otros proveedores. Pero los europeos temen que, si excluyen a Huawei de sus redes 5G, y Trump da marcha atrás, correrán el riesgo de sufrir represalias por parte de China y quedar en desventaja comercial.

A pesar de su "relación especial" con Estados Unidos, también el Reino Unido se enfrenta a este dilema. Al parecer, tiene planes para permitir que Huawei suministre ciertos tipos de material 5G que se consideran menos peligrosos para la red británica. Después de que el secretario de Estado norteamericano, Mike Pompeo, advirtiera públicamente en contra de "abrir las puertas a los jefes del espionaje de Pekín", las autoridades se prepararon para que Trump amenazara con reducir la cooperación entre los dos países en materia de inteligencia; sin embargo, en la rueda de prensa conjunta que dieron Trump y la primera ministra, Theresa May, el 4 de junio, el primero dijo: "Tenemos una relación increíble entre nuestros servicios de inteligencia y vamos a poder limar cualquier diferencia".


Los países europeos se encuentran ante una disyuntiva. La decisión de prohibir o no la presencia de Huawei por motivos de seguridad nacional corresponde de forma individual a los Estados miembros; no pueden dejar que sea la Comisión Europea la que decida y luego cargue con las culpas (aunque a algunos les gustaría). Casi todos piensan que se exageran los riesgos

y prefieren no poner en peligro ni sus relaciones de seguridad con Estados Unidos ni sus esperanzas de futuras inversiones chinas. Aunque Huawei es, teóricamente, una empresa privada, el Gobierno chino ha advertido de que habrá serias consecuencias para quienes sigan el ejemplo estadounidense. El embajador chino en Londres, Liu Xiaoming, ha dicho que eso supondría enviar “un mensaje muy malo y negativo” a los posibles inversores chinos.

Las empresas europeas también están en una situación delicada. Por ejemplo, pocos días después de anunciar el lanzamiento de la red 5G en el Reino Unido en julio, con móviles y routers domésticos de Huawei a disposición de los consumidores, Vodafone cambió sus planes después de que el gigante tecnológico estadounidense Google anunciara que iba a dejar de suministrar su sistema operativo Android a los nuevos dispositivos Huawei y que tampoco actualizaría los existentes. EE, rival de Vodafone, tomó la misma decisión, pero va a seguir usando material de Huawei en partes de su red central hasta 2022. Si Estados Unidos hace realidad su amenaza de no permitir que las empresas de telecomunicaciones que usen material de Huawei se conecten a sus redes, una empresa como la alemana T-mobile, con redes en Europa y Estados Unidos, tendrá grandes dificultades para operar.

Después del optimismo de hace unos años sobre el impulso económico que iban a aportar las inversiones chinas, en los últimos tiempos, los países europeos y sus empresas han empezado a compartir la preocupación de Estados Unidos por China. Entre otras cosas, por su robo de propiedad intelectual, su utilización de los subsidios estatales para que sus empresas (incluida Huawei) puedan producir y vender más barato que los rivales extranjeros e incluso expulsarlos del mercado y su disposición a aprovechar los vínculos económicos para adquirir influencia política. Al mismo tiempo, la UE piensa que, a falta de pruebas concretas de que Huawei está ayudando al Gobierno chino a penetrar en las redes de telecomunicaciones europeas, no puede vetar a la compañía sin más, como ha hecho Estados Unidos.

No obstante, la Unión Europea ha tomado poco a poco medidas para asegurarse de que la actividad china en Europa esté sujeta a más escrutinio. El Reglamento para el control de las inversiones extranjeras entró en vigor en abril de 2019 y estará en pleno funcionamiento en octubre de 2020; permite a la Comisión y los Estados miembros plantear preocupaciones sobre las inversiones extranjeras en sectores delicados (aunque deja la decisión definitiva en manos del Estado miembro en el que se haría la inversión propuesta). En marzo, la UE publicó unas recomendaciones sobre ciberseguridad para la tecnología 5G en las que declaraba que "cualquier vulnerabilidad en la tecnología 5G o un ciberataque contra las futuras redes en un Estado miembro afectaría a toda la Unión" y señalaba que los países de la Unión pueden negarse a dejar entrar a empresas extranjeras en sus redes 5G si representan una amenaza contra la seguridad nacional.

Estas medidas estaban de forma clara (aunque no explícita) dirigidas a China. Por si el mensaje no llegaba, la Comunicación Conjunta sobre China, también hecha pública en marzo de 2019, contiene una extensa sección sobre las medidas necesarias con el fin de mitigar los posibles riesgos para la seguridad de las infraestructuras críticas.

En algunos aspectos, el caso de Huawei muestra a la UE comportándose como Estados Unidos y a este comportándose como la Unión: normalmente, Bruselas defiende el principio de cautela y prohíbe (por ejemplo) la importación de carne de vacuno tratada con hormonas estadounidenses sin tener pruebas de que sea perjudicial para la salud humana. EE UU suele protestar por la aplicación que hace la UE del principio de cautela y defiende la gestión de riesgos. En el caso de Huawei, sin embargo, la Unión Europea está proponiendo la gestión de riesgos y Washington está presionando a los países europeos para que impidan por completo la entrada de las empresas chinas en el mercado, sin pruebas de que su participación en la tecnología 5G vaya a ser perjudicial. Lo irónico es que entre las compañías que saldrían beneficiadas si Bruselas sigue el ejemplo estadounidense están dos rivales europeas de Huawei, la sueca Ericsson y la finlandesa Nokia. Ericsson gana más en Estados Unidos, donde no tiene competencia de Huawei ni de una empresa norteamericana, que en Europa (donde Huawei sigue teniendo magníficos resultados).

La UE no puede impedir que Trump mezcle el comercio con la seguridad nacional. Pero sí puede y debe discutir con Estados Unidos todos los riesgos relacionados con la compra de material a Huawei, para ver si se pueden eliminar o gestionar.

El primero es el riesgo de espionaje. Tanto Estados Unidos como la Unión Europea quieren que a China le sea más difícil espiar a gobiernos occidentales y robar tecnología a empresas occidentales. Pero Pekín ha llevado a cabo operaciones de espionaje muy logradas sin material

de Huawei: entre 2012 y 2015, unos piratas presuntamente asociados a los servicios de inteligencia chinos lograron extraer datos confidenciales (incluidos huellas digitales y cuestionarios de seguridad) de 22 millones de funcionarios públicos de Estados Unidos, en activo y retirados, introduciéndose en los ordenadores de la Oficina de Gestión de Personal de la Administración estadounidense. Y, además, ha obligado a inversores occidentales en China a transferir tecnología a sus socios chinos para poder hacer negocios, aunque, en la cumbre UE-China de abril de 2019, ambas partes acordaron en su declaración conjunta que "no debe haber transferencia forzosa de tecnología".

Es difícil saber si la participación de Huawei en la tecnología 5G empeoraría mucho las cosas. A Estados Unidos parece preocuparle que, incluso aunque los productos de la compañía fueran perfectos al principio, el Gobierno chino pudiera obligarle a utilizar actualizaciones para crear orificios. Huawei ha sugerido la firma de acuerdos de "no espiar" con sus socios occidentales, pero no está claro cómo sería posible garantizar que se respetan ni por qué lo haría el Gobierno chino. Sin embargo, podría haber formas de mitigar los riesgos, por ejemplo dejando el material de Huawei fuera de las redes de comunicaciones gubernamentales y otras infraestructuras delicadas o (como al parecer piensa hacer Reino Unido) limitando el tipo de material que suministre.

En segundo lugar, existe el peligro de la piratería y los ciberataques, incluso contra infraestructuras críticas, de orígenes desconocidos. La estrategia de ciberseguridad de Huawei parece caprichosa. El Gobierno británico le obligó en 2010 a financiar un complejo en Reino Unido, el Centro de Evaluación de Ciberseguridad de Huawei (Huawei Cyber Security Evaluation Centre, HCSEC), "para mitigar cualquier riesgo aparente debido a la participación de Huawei en sectores de las infraestructuras nacionales críticas del Reino Unido". El último informe de su Junta de Supervisión expresa serias preocupaciones derivados de unas prácticas de ciberseguridad deficientes por parte de la compañía, pero no dice si considera que es algo deliberado. La Junta llega a la conclusión de que no puede garantizar que "todos los riesgos que supone para la seguridad nacional del Reino Unido la participación de Huawei en las redes críticas del país puedan mitigarse suficientemente a largo plazo".


Con el tiempo, la tecnología 5G formará parte esencial de las infraestructuras para coches sin conductor, procesos industriales, telemedicina (incluida la cirugía remota con robots controlados por médicos situados lejos de sus pacientes) y muchas más cosas. Existe el temor a que, en un momento de crisis, el Gobierno chino pueda obligar a Huawei a desconectar esos sistemas o permitir que China interfiera en ellos para causar perturbaciones. Pero además, sin un nivel máximo de ciberseguridad, las redes 5G serán vulnerables ante cualquier delincuente que intente robar datos personales, cometer fraudes o chantajear a los usuarios de la tecnología, un problema estudiado por Camino Mortera-Martínez en un informe político de CER, *¿Se acabó el juego? El problema cibernético de Europa*, en 2018. No solo la mayoría de los Estados miembros de la UE no tienen un equivalente al HCSEC, sino que el marco de certificación de ciberseguridad de la Unión (que deben respetar todos los proveedores, no solo Huawei), es meramente voluntario. Dado el volumen de datos que circulan entre ellos, Bruselas y Washington deberían trabajar para desarrollar unos criterios de ciberseguridad comunes y la UE debería implantar un sistema de certificación obligatorio.

En tercer lugar, existen preocupaciones de política industrial. La UE no quiere que Huawei utilice su facilidad de acceso a la financiación barata y otros subsidios del Gobierno chino para expulsar a las empresas europeas del mercado y monopolizar el sector de la tecnología 5G. Según un informe reciente de la Henry Jackson Society, gracias a esas facilidades, Huawei ya

ha conseguido debilitar a sus rivales europeos entre un 18 y un 30%. La Comisión Europea quiere una red 5G de gran calidad, basada en una sana competencia entre proveedores, no un monopolio chino. Por otra parte, vetar completamente a Huawei retrasaría el despliegue de las redes 5G en Europa y pospondría los beneficios teóricamente derivados. Lo paradójico es que, a través de sus filiales europeas, Huawei ya participa en varios proyectos de investigación financiados por la Unión para adquirir ventaja en esta tecnología, e incluso es socio científico de sus principales rivales. Las reglas actuales de la OMC sobre ayudas estatales son insuficientes para lidiar con el sistema chino, pero hacen falta muchos años para reformarlas. Como mínimo, mientras Huawei se aproveche injustamente del apoyo del Gobierno chino, Bruselas no debería permitirle participar en proyectos de investigación financiados por la Unión (y mucho menos controlar cualquier propiedad intelectual que se genere en ellos).

A la hora de la verdad, Estados Unidos puede hacer que sea muy difícil para Huawei operar fuera de China. La empresa utiliza chips del fabricante norteamericano Qualcomm, cuyo suministro estará prohibido de acuerdo con las nuevas reglas estadounidenses. Sin el sistema Android y otras aplicaciones de Google para los móviles, Huawei perderá cuota de mercado fuera de China (dentro no utiliza productos de Google). Pero las duras sanciones estadounidenses fomentarán el resentimiento entre los consumidores europeos y perjudicarán comercialmente a la empresa china y no conseguirán eliminar las amenazas que preocupan a Washington y Bruselas. Sería mucho mejor tratar de encontrar una estrategia colaborativa que eleve todos los criterios de ciberseguridad y promueva la competencia leal entre todos los proveedores de 5G que cumplan dichos criterios. Y, si la UE puede mantener la política comercial y la seguridad nacional separadas, mejor que mejor.

*A efectos de transparencia: Vodafone, BT (propietario de EE) y Qualcomm son miembros del consejo de CER. Sin embargo, las opiniones aquí expresadas pertenecen exclusivamente al autor y no representan las opiniones de dichas empresas.*

*El artículo original ha sido publicado en CER.*

*Traducción de María Luisa Rodríguez Tapia*

**Fecha de creación**
25 junio, 2019