ECONOMÍA

EEUU exige a España que excluya a China del 5G

Lo condiciona en Madrid a seguir compartiendo datos de inteligencia

EDUARDO FERNÁNDEZ MADRID

EEUU avisa a España al respecto de abrir sus redes de 5G a fabricantes chinos como Huawei y ZTE, pues se pondría en peligro la compartición de datos de seguridad e inteligencia, tal y como indicó ayer Robert L. Strayer, secretario de Estado adjunto de EEUU y responsable de política de información y comunicaciones cibernéticas e internacionales. Esta advertencia desde la Embajada, en una mesa redonda en la que participó EL MUNDO, llega un día después de conocerse que la Administración de Donald Trump contempla medidas ante la aprobación por parte del Gobierno de Pedro Sánchez de un proyecto de ley para la imposición de la llamada *tasa Google*.

Strayer, que en los últimos días ha visitado la conferencia internacional de seguridad de Munich y a las autoridades portuguesas en Lisboa, está inmerso en un *tour* por el Viejo Continente para lograr que Europa marque distancias con la tecnología 5G china. No hay anuncio de represalias, pero sí claridad cristalina: EEUU quiere a Huawei «totalmente excluida» de las redes. En el mercado español, la tecnológica china está asentada, aunque en Orange no la han introducido en el *core* de su despliegue y tanto Vodafone como Telefónica ya han puesto en marcha iniciativas para reducir esa exposición –Strayer se vio también ayer con responsables de la gran *teleco* española–. El *core*, donde reside la gestión de los datos en el estándar de las comunicaciones móviles del futuro, no parece bastar.

«No podemos poner nuestra información importante en riesgo de ser accedida por el Partido Comunista», dijo ayer Strayer, para el que «Huawei está realmente operando en nombre del Partido Comunista Chino». Consultados por este diario, en la firma de Shenzhen prefieren no hacer declaraciones al respecto.

LAS REDES DEL FUTURO

Defensa. Además de acelerar las conexiones y minimizar la latencia, el 5G servirá para conectar«miles de millones» de objetos, apunta Strayer, con innegables consecuencias en Defensa.

Trump. El presidente de EEUU se mostró preocupado en sus reuniones en Davos al respecto de las implicaciones militares de la quinta generación de telefonía móvil.

«No deberían ser las operadoras de telecomunicaciones las que tomen estas decisiones importantes de seguridad nacional, deberían ser los gobiernos», lanzó además Strayer a Moncloa. El adjunto a la Secretaría de Estado se ha reunido en Madrid con representantes del Ministerio de Asuntos Exteriores y de Economía.

Strayer admite que se pone «en riesgo la compartición de información» con los países que tengan en sus redes de telecomunicaciones componentes de esas firmas. Movilización de tropas, control de terroristas, información sobre criminales internacionales... Ésa es la relación que EEUU coloca sobre la mesa.

El representante de EEUU defiende que la marca sueca Ericsson, la finlandesa Nokia y la surcoreana Samsung están tan avanzadas en 5G como Huawei –«las únicas fuentes originales para asegurar [que están por delante] vienen de China»–. Por ello, invita a las autoridades europeas a decantarse por esas alternativas: «En EEUU usamos tres proveedores para desplegar 5G por docenas de ciudades norteamericanas». Mike Pompeo, secretario de Estado norteamericano, hizo también un alegato en Munich para forjar una alianza occidental frente a China.

Strayer pone el foco en un apartado del documento consensuado por la Unión Europea a finales de enero para la seguridad en la implantación del 5G, en concreto a la referencia a los riesgos que conlleva la incorporación a las redes de proveedores procedentes de países que adolezcan de una falta de sistemas de control e equilibrio democráticos. Para el diplomático, este apartado invalidaría a marcas como Huawei, aunque no se mencione a ésta *ex profeso*. «En China no hay Estado de Derecho (...) Por lo tanto, el Partido Comunista controla a proveedores como Huawei o ZTE para que tomen medidas que no responden a los intereses de los ciudadanos españoles o de los de todo el mundo».

«Hay una ley china que dice explícitamente que todas las entidades

El subsecretario de Estado adjunto de EEUU Robert Strayer, ayer. EFE

La seguridad del ciberespacio cada vez tiene más relevancia gracias a los avances tecnológicos, pero se necesita un cerco jurídico

EEUU-China: marco legal de la ciberseguridad

JAVIER CREMADES

TRIBUNA

En los últimos años hemos sido testigos de una intensa campaña de comunicación destinada a concienciar sobre la injerencia de la República Popular China en las compañías fabricantes de equipos de telecomunicaciones.

El punto de partida fue el dictamen elaborado en 2012 por el Comité Especial de Inteligencia de la Cámara de Representantes de los Estados Unidos que denunciaban de forma directa a Huawei y ZTE al afirmar que, «de acuerdo con las leyes chinas, ZTE y Huawei estarían obligados a cooperar con cualquier solicitud del Gobierno chino para hacer uso de sus sistemas o acceder a ellos con fines maliciosos bajo el pretexto de la seguridad del Estado». Las acusaciones posteriores, sin embargo, se centraron en la Ley de Inteligencia Nacional de China de junio de 2017. EEUU aseveraba que esta norma permitía al Gobierno chino exigir a las empresas tecnológicas que dieran acceso a su información con fines maliciosos, o incluso dicho instrumento legal, según estas publicaciones, daban cobertura para ejecutar actos que podrían considerarse de espionaje.

Pese a todo ello, recientemente algunos países como Alemania, Reino Unido o España han decidido permitir que Huawei y ZTE participen en el suministro de redes 5G.

En este controvertido escenario surgen varias dudas, ¿qué hay detrás de estas acusaciones? Además del hecho de que nunca se han detectado violaciones de este tipo, ¿existe alguna base legal para que el Gobierno chino exija a Huawei o a ZTE que implementen dispositivos de espionaje en sus equipos de telecomunicaciones? ¿O son estas acusaciones sólo un intento de convertir a Huawei en una moneda de cambio y criminalizar al adversario en la lucha de poder entre dos grandes potencias tecnológicas?

Desde una perspectiva legal, la respuesta es sencilla y clara. Analizando todo el entramado normativo chino que regula y/o afecta a la seguridad cibernética, no es posible encontrar ninguna disposición que permita al Gobierno chino ordenar a las empresas chinas implementar puertas traseras o *spyware* en sus equipos de telecomunicaciones o que de cualquier otra forma pudieran permitir llevar a cabo actividades de espionaje en el extranjero. De hecho, existe un principio general del derecho chino que no permite la aplicación extraterritorial de estas normas que afectan a la ciberseguridad, circunstancia jurídica que se ve garantizada por un sistema de sanciones para quien lleve a cabo actuaciones que inobserven el citado principio.

La Ley de Inteligencia china no se extiende a filiales europeas o a la actividad comercial

De este modo, en el marco de la Ley de Seguridad Cibernética china, el artículo 28 exige que sólo los operadores de redes –pero no los fabricantes de equipos de telecomunicaciones– presten asistencia al Gobierno chino para apoyar la seguridad nacional. Esto no implica *per se* ningún acto de espionaje.

Hay quien asegura que la Ley de Inteligencia china es la norma crítica, ya que algunos de sus preceptos obligan a los ciudadanos chinos a prestar ayuda en las labores de inteligencia nacional. Sin embargo, estos comentarios carecen, de nuevo, de base legal alguna, pues la citada norma no contiene disposiciones que permitan ni obliguen a que se pueda ordenar por las autoridades chinas la implementación de puertas traseras o dispositivos de espionaje en las redes e infraestructuras ni en China ni mucho menos en Europa. Esto se debe a que –tal y como ocurre con la Ley de Seguridad Cibernética– ésta sólo se aplica a los ciudadanos chinos en China y no se extiende a las filiales europeas o a sus actividades comerciales. El efecto extraterritorial de esta ley es limitado cuando entra en conflicto con las leyes de otros países.

El panorama es similar para la Ley de Contraespionaje, la Ley de Seguridad del Estado y la Ley Antiterrorista chinas, ninguna de las cuales es aplicable a las filiales europeas de los fabricantes de equipos chinos o a sus actividades comerciales. Tampoco respalda actuaciones de espionaje ni en China, ni me-

Montero responde a Trump: «¿Nos tenemos que arrodillar?»

La ministra de Hacienda contesta a las amenazas de EEUU por la 'tasa Google'

DANIEL VIAÑA MADRID

Antes del inicio de su comparecencia en la comisión de Hacienda del Congreso, la ministra María Jesús Montero se había mostrado cauta respecto a las advertencias de Estados Unidos en relación con la *tasa Google*. Es más, en un primer momento señaló que los avisos adelantados por este periódico no eran, en ningún caso, amenazas. Pero ya en su segundo turno de intervención, y ante las críticas del Partido Popular, Montero elevó el tono. Mucho.

«¿Por qué le conceden esa capacidad al señor Trump? ¿Usted qué cree, que nos tenemos que arrodillar o que lo que tenemos que hacer es liderar Europa para que sea un impuesto armonizado?», respondió con dureza la ministra de Hacienda a la portavoz del PP, Carolina España, que en su primer turno había criticado la aprobación del impuesto por parte del Gobierno a pesar de los avisos de Estados Unidos.

De esta manera, Montero incidió en la soberanía fiscal de un país, algo que ya ha hecho en anteriores ocasiones, aunque al mismo tiempo subrayó la necesidad de que la Unión Europea avance de manera conjunta en el impuesto sobre determinados servicios digitales. «El señor Trump no puede convertirse en un dirigente que diga a los países de la UE lo que tienen que hacer. Europa no va a dejar que ninguna potencia la chantajee», añadió.

Las palabras de Montero, que también tuvo un intercambio intenso con Ciudadanos, se produjo después de presentar los objetivos de su Ministerio para los próximos meses, y de dejar claro que quiere más impuestos y más gasto público. «Debemos acercar la media de tributación al nivel de la Unión Europea. Y tenemos que elevar también el gasto público. Somos el quinto país con menos ingresos sobre PIB de la UE», explicó Montero durante su intervención en la primera reunión de la mencionada Comisión en la presente legislatura.

> «Europa no va a dejar que ninguna potencia la chantajee», afirmó Mª Jesús Montero

Y acto seguido comenzó a enumerar los próximos pasos fiscales: elevar el tipo mínimo de Sociedades al 15%, cifra que llega al 18% en el caso de los bancos y las compañías de hidrocarburos; incremento al IRPF a las rentas más altas; o el impuesto *verde* que incrementará el precio del diésel.

Otro punto clave será la armonización fiscal entre comunidades, que no es otra cosa que igualar los impuestos cedidos a las regiones. Evitar lo que la ministra siempre califica como *dumping* fiscal, esto es, que unas comunidades puedan bajar más los impuestos para atraer inversiones o capitales. El caso más claro es Madrid, a la que en esta ocasión Montero no ha hecho referencia pero a la que sí ha acusado en más de una ocasión de incurrir en esta práctica. Para ello, y también para mejorar la distribución de los fondos entre comunidades, la ministra se comprometió a presentar en octubre un «esqueleto» de la reforma de la financiación autonómica.

deben cumplir los mandatos de los servicios de inteligencia y de seguridad en China y de mantener esa colaboración en secreto», afirmó Strayer. Esa normativa implicaría, según la versión norteamericana, que empresas como Huawei ocultaran sus vínculos con el Gobierno de su país de origen. Esta compañía ha sido vetada en EEUU, al quedar incluida en una *lista negra* que impide a las empresas norteamericanas mantener relaciones comerciales con Huawei, rupturas tan importantes como la de Google, que sirve el sistema operativo Android a *smartphones* asiáticos.

nos aún en el extranjero. Tales conclusiones han sido recientemente corroboradas por el propio Gobierno chino. Así, Yang Jiechi, consejero de Estado chino, confirmó públicamente que ninguna de las leyes que componen el ordenamiento jurídico en China exige a los fabricantes de equipos chinos instalar dispositivos de espionaje.

Por otro lado, existen países que aprueban leyes con efectos marcadamente extraterritoriales, como es el caso de muchas normas estadounidenses. Cabe mencionar la Ley de Vigilancia de la Inteligencia Exterior de EEUU, que fue enmendada en 2018 para permitir a la Agencia Nacional de Seguridad recopilar datos sobre comunicaciones digitales de personas físicas y jurídicas extranjeras fuera de EEUU sin necesidad de presentar una orden judicial.

Otro ejemplo de aplicación extraterritorial es la Ley Patriota de los Estados Unidos, aprobada en octubre de 2001, tras los atentados terroristas del 11 de septiembre de 2001, que restringió los derechos y libertades individuales y permitió a las autoridades tener acceso a numerosas bases de datos que contienen información confidencial sobre cientos de miles de ciudadanos y empresas estadounidenses.

Por último, la llamada *US Cloud Act*, aprobada el año pasado por la administración de Donald Trump, permite a las autoridades estadounidenses requerir a compañías tecnológicas información relevante almacenada ya sea en EEUU u otros estados. De hecho, algunos estados miembros de la UE expresaron su preocupación a este respecto. Según Ulrich Kelber, responsable alemán para la protección de datos y la libertad de información, las autoridades estadounidenses podrían invocar la ley de la *nube* para exigir el acceso a los datos en poder de ciertos proveedores de servicios de nube de EEUU lo que, sin duda, crearía un riesgo para los organismos gubernamentales alemanes que almacenan datos con ellos.

> La colaboración entre todos los actores económicos y sociales es fundamental

La información publicada sobre la normativa china en buena parte está generando miedo y desconfianza. A juzgar por el análisis y el estudio comparado de las leyes que afectan a la seguridad en la red, podría decirse que se ha proporcionado una visión desequilibrada y desigual respecto de los diferentes actores políticos que actualmente se encuentran en conflicto comercial.

Estamos en un momento donde la seguridad en el ciberespacio se ha convertido en un tema de enorme relevancia, debido al crecimiento incesante de los avances tecnológicos y la necesidad de generar un marco jurídico que dé respuesta a los retos que surgen en todos los ámbitos de la sociedad. En este sentido, la colaboración entre todos los actores económicos, sociales y jurídicos es fundamental para poder seguir implementando los correspondientes umbrales de seguridad que contribuyan a mantener un progreso tecnológico consistente en el tiempo.

Javier Cremades, Abogado Presidente Cremades & Calvo Sotelo Abogados