Manuel Conthe
Serrano, 26 – 4
28001 Madrid
España

Observaciones

sobre

Anteproyecto de Ley sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación

13 de enero de 2021

Índice

1. Introducción

1. Formulo estas Observaciones al Borrador de Anteproyecto de Ley sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación (en adelante, "el Anteproyecto") como aplicación práctica del Dictamen que preparé el 4 de julio de 2020 a petición de Huawei (que adjunto como Apéndice) sobre si existe riesgo de interferencia de las autoridades públicas chinas sobre Huawei y si sería adecuado aplicar a Huawei, como suministrador de las redes 5G españolas, alguna de las restricciones previstas en la medida estratégica SM 03 del documento "Caja de herramientas de la UE para la seguridad de las redes 5G" (en adelante, "*Toolbox*").

2. En consecuencia, estas Observaciones se refieren exclusivamente a aquellos aspectos del Anteproyecto que atañen a la eventual calificación de suministradores como de alto riesgo,[1] sin entrar en otras cuestiones de fondo (como, por ejemplo, la obligación de diversificación de suministradores que establece el artículo 8.3).

3. Estas Observaciones harán referencia al principio constitucional de "reserva de Ley", pero no abordarán, sin embargo, qué otras alternativas jurídicas pudieran resultar preferibles para plasmar en el Ordenamiento Jurídico español los objetivos que el Anteproyecto persigue: tomarán este como dado, y se limitarán a criticar alguno de sus preceptos y a proponer una mejora de su redacción.

4. Al igual que ocurrió con el Dictamen que desarrollan, he preparado estas Observaciones con independencia de criterio, como experto en varias de las cuestiones jurídicas relacionadas con el Anteproyecto, pero a petición de Huawei España, de forma retribuida.

5. Mi currículum está disponible públicamente en www.manuelconthe.com. Mi cualificación para escribir estas Observaciones se basa en la experiencia que ahí se expone y en particular

[1] Todos los subrayados que aparecen en el documento proceden del autor.

en mi trabajo como abogado y árbitro internacional desde 2009, y mi experiencia previa como alto funcionario en la Comisión Nacional del Mercado de Valores y en el Ministerio de Economía y Hacienda, así como en el Banco Mundial.

6. Las conclusiones esenciales de estas Observaciones son que, a pesar del loable objetivo del Anteproyecto y de muchos de sus preceptos, los dos primeros apartados de su artículo 11 (y algunos preceptos concordantes con ellos) merecen tres graves reproches íntimamente relacionados:

   - Copian bastante mecánicamente e incluso empeoran el texto del apartado de la Toolbox o Caja de Herramientas relativo al riesgo de interferencia estatal en la cadena de suministro del 5G (R5) y, al hacerlo, contienen una regulación indeterminada y vaga de la calificación de un suministrador como de alto riesgo que, por afectar al derecho constitucional de libre empresa, resulta contraria a la reserva de Ley que consagra el artículo 53 de la Constitución española, tal y como ha sido interpretado por el Tribunal Constitucional.

   - Permitirían un desarrollo reglamentario y aplicación por el Gobierno y por el Ministerio de Asuntos Económicos y Transformación Digital que podría desnaturalizar el bien jurídico que el proyecto dice proteger -la ciberseguridad de las redes 5G- y, so capa de ese objetivo, perseguir otros objetivos distintos, como la protección comercial de las compañías europeas suministradores de equipos 5G o la adopción de medidas injustificadas, por motivos culturales o políticos, contra suministradores basados en la República Popular China (en adelante, RPC), como Huawei, que ha hecho inversiones en España y merece el tratamiento previsto en el Acuerdo entre el Reino de España y la República Popular China para la Promoción y Protección Recíproca de Inversiones, de 14 de noviembre de 2005.

7. El apartado final de estas Observaciones sugerirá diversas mejoras en los dos primeros apartados del artículo 11 que, respetuosas con el objetivo del Anteproyecto -la ciberseguridad de las redes españolas 5G-, harían ese precepto clave más preciso y más ajustado a la jurisprudencia del Tribunal Constitucional y a las obligaciones internacionales de España.

2. El objetivo del Anteproyecto: la ciberseguridad de las redes 5G

8. La reciente Comunicación Conjunta de la Comisión Europea y del Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad sobre "Estrategia de Ciberseguridad de la UE en la Década Digital" comienza con una afirmación tan rotunda como incuestionable que, aplicable a la Unión Europea (UE) en su conjunto, lo es también a España:

   > "La ciberseguridad es parte integral de la seguridad de los europeos. Ya se trate de los dispositivos conectados, redes eléctricas, bancos, aeronaves, administraciones públicas u hospitales que usen o frecuenten, la gente tiene derecho a hacerlo con la seguridad de que estarán protegidos de ciberamenazas. La economía, democracia y sociedad de la UE dependen más que nunca de instrumentos digitales y conectividad seguros y

confiables. La ciberseguridad es, en consecuencia, esencial para construir una Europa resiliente, verde y digital".[2]

9. En el plano jurídico interno, el Tribunal Constitucional español ha destacado en múltiples ocasiones que la ciberseguridad, como sinónimo de la seguridad en la red, es una actividad que se integra en la seguridad pública. Así, la STC 142/2018, de 20 de diciembre, recuerda en su Fundamento Jurídico 4 que ya la Ley 36/2015, de 28 de septiembre, de seguridad nacional, identifica en su artículo 10 la ciberseguridad como uno de los "ámbitos de especial interés de la seguridad nacional…que requieren una atención específica, por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales". De ahí que el Tribunal Constitucional concluya que la ciberseguridad, "al referirse a las necesarias acciones de prevención, detección y respuesta frente a las ciberamenazas, afecta a cuestiones relacionadas con la seguridad pública y la defensa, las infraestructuras, redes y sistemas y el régimen general de telecomunicaciones".

10. Por todo lo anterior, resulta elogiable el objeto del Anteproyecto, tal y como lo define su artículo 1:

> "Esta ley establece requisitos de seguridad para el despliegue y la explotación de redes de comunicaciones electrónicas y la prestación de servicios de comunicaciones electrónicas basados en la tecnología 5G".

11. Tampoco hay nada que objetar a la intensidad de la intervención administrativa que el Anteproyecto contempla con el fin de proteger el trascendental objetivo que persigue, la ciberseguridad de las redes 5G. Téngase presente que en otro campo acaso no tan directamente ligado a la seguridad nacional, como es la ordenación del sistema bancario, tanto la normativa comunitaria como la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito otorgan a las autoridades administrativas, españolas y europeas, amplísimas facultades de actuación sobre entidades y actividades privadas, como son las bancarias. Lo mismo cabe decir, por ejemplo, en materia de seguridad nuclear, de la Ley 33/2007, de 7 de noviembre, que reconoce al Consejo de Seguridad Nuclear amplísimas facultades de intervención administrativa en ese sector de actividad.

12. El verdadero peligro que suscita el Anteproyecto es, como luego se expondrá, que, por la forma imprecisa en que está redactado su artículo 11 (y otros concordantes), permitiría un desarrollo reglamentario y aplicación por el Gobierno y por el Ministerio de Asuntos Económicos y Transformación Digital que desnaturalizara el bien jurídico que el proyecto dice proteger -la ciberseguridad de las redes 5G- y, bajo ese teórico manto protector, persiguiera otros objetivos distintos, como:

    - La adopción de medidas de protección a favor de los dos grandes suministradores europeos de equipos 5G, señalados por la Memoria del Anteproyecto (esto es, la sueca

[2] "*Joint Communication to the European Parliament and the Council*", European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, Brussels, 16.12.2020, JOIN (2020) 18 final, p.1.

Ericsson y la finlandesa Nokia), en apoyo del principio de "soberanía digital" de la UE, concepto que, ya enunciado por la Comisaria Vestager en la estrategia Digital para Europa presentada en febrero de 2020[3], ha vuelto a ser reiterado el pasado 16 de diciembre de 2020 en la presentación que la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores hicieron de "La estrategia de Ciberseguridad de la Unión Europea para la década digital"[4].

- La adopción de medidas de discriminación comercial o presión política contra la República Popular China (en adelante, RPC), que aprovecharían que es el país en el que tiene su sede la compañía líder internacional en tecnología 5G, Huawei, explotarían ciertos prejuicios culturales y psicológicos sobre ese país y buscarían, en coordinación con los Estados Unidos, frenar deliberadamente el liderazgo tecnológico de las empresas chinas.

13. Antes de formular comentarios detallados sobre el citado artículo 11 del Anteproyecto, se expondrá en más detalle el peligro mencionado.

3. Ciberseguridad vs. discriminación comercial y política

14. En el Dictamen del 4 de julio de 2020 analicé en detalle la finalidad y naturaleza de la Caja de Herramientas o Toolbox de la UE y el peligro de que los riesgos políticos (R5) y la medida estratégica contemplada para mitigarlos (SM 03) pudieran servir de coartada para, bajo el respetable manto de la protección de la ciberseguridad de las redes 5G, esconder medidas injustificadas objetivamente contra la empresa china Huawei que persiguieran otros objetivos distintos al de la ciberseguridad.

15. En efecto, las conclusiones primordiales del Dictamen fueron:

I. La Toolbox de la UE es un instrumento de "*soft law*" preparado por expertos en ciberseguridad, en el marco del Grupo de Cooperación NIS. Por tanto, por su propia naturaleza y origen, la Toolbox guarda silencio respecto a los criterios jurídicos que deben aplicar los Estados miembros al realizar la evaluación de riesgos recomendada en la medida estratégica 3 (SM 03).

Aunque la Toolbox hace referencia a que las medidas adoptadas deben ser "adecuadas" y "proporcionales", no entra a dilucidar o debatir las posibles limitaciones jurídicas y constitucionales que los Estados miembros como España tendrían que respetar al aplicar algunas de las medidas estratégicas que recomienda.

II. Las normas y jurisprudencia de la Organización Mundial del Comercio sobre la "excepción de seguridad nacional" (artículo XXI del GATT), de la Unión Europea sobre el "principio de precaución" y españolas sobre medidas públicas restrictivas para

[3] https://ec.europa.eu/commission/presscorner/detail/es/ip_20_273
[4] https://ec.europa.eu/commission/presscorner/detail/es/IP_20_2391

proteger los intereses nacionales, de la Administración Pública o de los ciudadanos, establecen que las autoridades públicas no pueden:

(i) basar tales restricciones en meras suposiciones o especulaciones, sino que deben basarlas en una evaluación adecuada y completa del riesgo que tenga en cuenta las circunstancias concretas de cada caso (incluidas las medidas ya en vigor para mitigar los riesgos y el coste potencial de la medida restrictiva);

(ii) adoptar medidas restrictivas que no sean adecuadas o idóneas para alcanzar el objetivo de ciberseguridad que persiguen ("test de idoneidad"); ni

(iii) adoptar medidas más restrictivas que otras que logren el objetivo público perseguido -esto es, la ciberseguridad- con la misma o mayor eficacia ("test de proporcionalidad").

Así pues, la invocación del objetivo de la ciberseguridad no puede ser un "conjuro mágico" (*incantation*) o un "comodín" que proporcione al Gobierno y al Ministerio de Asuntos Económicos y Transformación Digital "carta blanca" para aplicar restricciones sin limitación, sin respetar los tests de adecuación y proporcionalidad, ni llevar a cabo una evaluación adecuada y completa del riesgo que tome en cuenta las circunstancias específicas de cada caso.

III. En consecuencia, la evaluación del riesgo de suministradores individuales, como Huawei, no puede llevarse a cabo mediante métodos de "perfilado" (*profiling*) basados en su nacionalidad, sino que requiere considerar sus características concretas y, en particular, su trayectoria específica y prioridad otorgada a la mitigación y prevención de riesgos de ciberseguridad.

IV. Lo anterior resulta muy relevante, pues a lo largo de los años Huawei se ha esforzado de manera continua en cooperar con sus clientes y con las autoridades públicas a fin de garantizar que sus equipos y productos son seguros y no vulnerables frente a riesgos de ciberseguridad. Como parte de este esfuerzo, ha establecido voluntariamente:

- Un laboratorio interno independiente de ciberseguridad (ICSL), que es una unidad de verificación de seguridad certificada por la ISO e independiente de los equipos comerciales y de los departamentos de I+D.

- Tres Centros de Transparencia en Europa, que permiten a los clientes verificar e inspeccionar los equipos de Huawei, incluyendo su código fuente, sin comprometer la propiedad intelectual de Huawei. El centro más antiguo y activo es el del Reino Unido, que, presidido por la autoridad de ciberseguridad más importante del Reino Unido, se encarga de revisar los equipos y procesos de Huawei, y está tutelada por un Comité de Supervisión (*Oversight Board*). Este último ha confirmado la estrecha participación de Huawei en el proceso de verificación de sus equipos y en el trabajo de corrección necesario para solucionar los problemas técnicos detectados. También ha confirmado que las vulnerabilidades detectadas en el *software* no eran resultado de la interferencia de ningún Estado.

Según la información pública existente, ningún otro proveedor de equipos de telecomunicaciones ha aceptado un control externo tan riguroso.

- Una Oficina Mundial de Ciberseguridad (GSPO) robusta, de alto nivel y autónoma, con su máximo responsable con línea directa jerárquica y de comunicación con el presidente rotatorio, a través del Comité Global de Ciberseguridad y Protección de la Privacidad de los Usuarios (GCSPC).

  A pesar de que aún no existe una práctica internacional ni una norma sobre los *Chief Information Officers* ("CIO", o delegados de Información), el lugar que ocupa el *Global Cyber Security and Privacy Officer* (GSPO) de Huawei en la estructura corporativa de la compañía evidencia la importancia clave que se atribuye a su papel, lo que está en línea con las prácticas de otras empresas de telecomunicaciones líderes a nivel mundial (como Telefónica o Apple).

- El nombramiento de un delegado europeo de protección de datos independiente, de conformidad con lo dispuesto en el artículo 37 del RGPD -que, según ha confirmado, no recibe instrucciones sobre el ejercicio de sus funciones, no puede ser destituido ni penalizado por el desempeño de sus tareas y mantiene una línea jerárquica directa con el más alto nivel directivo -el presidente rotatorio- a través del GCSPC, resulta plenamente conforme con las exigencias del artículo 38 del RGDP.

Esta actitud cooperativa y proactiva de Huawei al tratar los riesgos de ciberseguridad, y la prioridad que Huawei ha venido atribuyendo a limitarlos, no concuerda con las acusaciones de que podría colaborar a que las redes de 5G sean vulnerables a intentos de espionaje o sabotaje promovidos por China.

V. Las especulaciones de que los equipos de Huawei están especialmente expuestos a un riesgo de interferencia por parte de las autoridades chinas -presumiblemente mediante la colocación de puertas traseras (*backdoors*), dispositivos de escucha (*eaversdropping devices*) o programas espía (*spyware*), o de mecanismos de sabotaje (como *kill switches*) parecen infundadas.

Esas especulaciones pasan por alto, además, que una parte significativa de la cadena de suministro de todos los proveedores de 5G, incluidos Ericsson y Nokia, incluyen actividades de fabricación llevadas a cabo en China.

VI. Huawei es una empresa privada, no muy diferente de una gran cooperativa europea, y no es de propiedad estatal. No hay ni el más mínimo indicio de que Huawei esté "controlada por el Estado". El riesgo de que Huawei o algunos de sus empleados se vean obligados a incorporar dispositivos ilegales en sus equipos o programas de 5G es extremadamente remoto y no superior al de otros fabricantes. Además, la trayectoria de Huawei en materia de ciberseguridad es excelente.

VII. Imponer medidas restrictivas a Huawei, y no digamos una prohibición total, como proveedor de equipos 5G para los operadores españoles, además de ser jurídicamente

cuestionable, implicaría también un alto coste económico para España y retrasaría el desarrollo del 5G. Así, como ha estimado la consultora británica *Oxford Economics*, en el escenario central la ausencia de Huawei en las redes 5G españolas provocaría a los operadores un aumento de costes cercano al 19%, lo que se traduciría en un aumento anual de costes de unos 292 millones de euros, en 5 millones menos de potenciales clientes con acceso a las redes en 2023 y una pérdida anual de PIB que en 2035 llegaría a los 3.700 millones de euros.[5]

VIII. Los potenciales riesgos de ciberseguridad de las redes de 5G no están relacionadas con la nacionalidad del proveedor de los equipos, sino con las medidas de ciberseguridad utilizadas en su diseño, fabricación, control, verificación e inspección, cualquiera que sea su proveedor o la nacionalidad de este.

Tanto Ciaran Martin, director del *National Cybsecurity Center* (NCSC) del Reino Unido, como el Comité de Inteligencia y Seguridad del Parlamento del Reino Unido han confirmado que "el pabellón de origen de los equipos de telecomunicaciones no es el elemento crítico a la hora de determinar su ciberseguridad".[6]

IX. Por eso, los riesgos de ciberseguridad resultantes de la interferencia de Estados de fuera de la Unión (R5, en la terminología de la Toolbox) podrían abordarse de manera más eficaz mediante un sistema general de verificación y/o inspección obligatoria de todos los equipos relevantes de 5G, junto con estrictos controles en las posteriores actividades de mantenimiento o actualización de equipos. Cualquiera de estas inspecciones o de estos controles deberían ser de aplicación para todos los proveedores, independientemente de su nacionalidad o del lugar de fabricación, adquisición o desarrollo de esos equipos.

X. En suma, la ciberseguridad de las futuras redes 5G constituye un objetivo público esencial, que las autoridades europeas y españolas deberán mitigar con las medidas técnicas idóneas descritas por la propia *Toolbox*, entre las que destaca la 9 (TM09): Uso de certificaciones UE para los componentes de la red de 5G, equipos de cliente y/o procesos de proveedores. Como ventaja adicional, eso protegería a la red 5G española contra posibles interferencias políticas de cualquier país, incluidas las agencias de seguridad e inteligencia de Estados Unidos. Por el contrario, aplicar a Huawei, por ser empresa china, restricciones como proveedor de 5G en aplicación de la "medida estratégica" 3 (SM03) constituiría una arbitrariedad política sin base jurídica.

4. Crítica del artículo 11 del Anteproyecto

16. Estas Observaciones no se dirigen contra el Anteproyecto en su conjunto o contra sus objetivos. Muy al contrario.

[5] Ver Dictamen, párrafos 270-277, especialmente el 274.
[6] Comité de Inteligencia y Seguridad del Parlamento del Reino Unido, 2019, 19 de julio). *Statement on 5G suppliers*. Ver Dictamen, párrafos 253 y 254.

17. El Anteproyecto contiene muchos preceptos que son perfectamente congruentes con el elogiable objetivo que marca el artículo 1. Tal ocurre, a título ilustrativo y no exhaustivo, con:

    - El artículo 4, cuando no limita el ámbito de aplicación a los operadores de redes, sino que lo extiende también a los suministradores y fabricantes de equipos.

    - Los artículos 6 y 7, sobre análisis de riesgos de los operadores y prácticas de seguridad de los suministradores.

    - El artículo 10, cuando contempla el desarrollo reglamentario de la Ley mediante el llamado "Esquema de seguridad para las redes y servicios 5G", así como los artículos 12 ("Tratamiento integral de la seguridad para las redes y servicios 5G"), 13 ("Priorización de riesgos") o 15 ("Certificación en elementos de redes 5G y requisitos esenciales").

    - El capítulo IV, sobre potestades administrativas de control y sanción, aunque su artículo 20 no tenga toda la precisión que debiera.

18. El Anteproyecto no es meridianamente claro sobre los pasos que serían precisos para su efectiva aplicación. En efecto, el articulo 10 prevé la aprobación por Real Decreto de un Esquema de seguridad para las redes y servicios 5G, lo que parecería el habitual desarrollo reglamentario de las previsiones legales. Pero, al mismo tiempo, el artículo 11.2 contempla que mediante un acto administrativo, con forma de acuerdo de Consejo de Ministros, se califique el riesgo de cada suministrador y la Disposición Transitoria contempla que el Ministerio de Asuntos Económicos y Transformación Digital, antes de que se apruebe el citado Esquema de seguridad, pueda establecer las obligaciones para los operadores relacionadas con el perfil de riesgo de sus suministradores (como serían las prohibiciones o restricciones previstas en el artículo 14.1 c). Todo ello sugiere que, en aplicación directa del Anteproyecto, sin esperar tampoco a la aprobación del citado Esquema de seguridad, el propio Gobierno llevaría a cabo, en virtud de acuerdo de Consejo de Ministros, la evaluación del riesgo de los suministradores, y que las consecuencias prácticas para las operadoras de tales calificaciones se definirían por el Ministerio de Asuntos Económicos y Transformación Digital, previsiblemente mediante una Orden Ministerial de desarrollo directo del Anteproyecto.

19. Si la anterior interpretación fuera acertada y estuviera previsto que, por razones de urgencia, el Anteproyecto, en la práctica, se aplicara en virtud de meros acuerdos del Consejo de Ministros y de una Orden del Ministerio de Asuntos Económicos y Transformación Digital, sin un desarrollo reglamentario previo completo a través de Real Decreto, resultaría todavía más imperativo que se subsane la extraordinaria vaguedad de la que adolece, como enseguida se dirá, el artículo 11 del Anteproyecto.

20. En efecto, el verdadero "agujero negro" del Anteproyecto está en los apartados 1 y 2 de un artículo clave del Anteproyecto, el artículo 11, cuyos efectos se despliegan a través de otros preceptos íntimamente relacionados con él, como son los artículos 8.3, 14.1 c), 14.4, 19.1 y la Disposición Transitoria. Por eso, al análisis de los apartados 1 y 2 del artículo 11 se dedicarán los siguientes epígrafes.

4.1. Análisis del artículo 11 (apartados 1 y 2)

21. La lectura del artículo 11 revela que "transpone" a la legislación española no una norma imperativa de la UE, sino el primer inciso del apartado 2 (*Supplier-specific vulnerabilities*) del Anexo 2 de la Toolbox (*Summary of the findings of the EU coordinated risk assessment*).[7]

22. Para comprobarlo, recordemos aquí ese apartado de la Toolbox, en su inglés original:

    "The likelihood of the supplier being subject to interference from a non-EU country. This is one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks. Such interference may be facilitated by, but not limited to, the presence of the following factors:

    - *A strong link between the supplier and a government of a given third country;*
    - *The third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country;*
    - *The characteristics of the supplier's corporate ownership; and*
    - *The ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.*

23. Si se compare ese texto en inglés con el segundo párrafo del art. 11.1 del Anteproyecto se advierte que son muy parecidos, aunque hay varias diferencias:

    - El "*fuerte* (*strong*) vínculo entre el suministrador y el Estado (*government*) de un tercer país" se ha convertido en la letra a) en "los vínculos de los suministradores y de su cadena de suministro con los gobiernos de terceros países", de forma que ha desaparecido el adjetivo "fuerte" y ahora se habla de "vínculos", en plural, tanto del suministrador como de su propia cadena de suministro con los gobiernos de terceros países.

    - Las características de su estructura de propiedad (*corporate ownership*) del suministrador se han transformado en la letra b) en "la composición de su capital social y la estructura de sus órganos de gobierno"

    - La expresión "*the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment*" se ha transformado en la letra c) en poder para "ejercer presión sobre la actuación o ubicación de la empresa", en vez de "ejercer cualquier forma de presión, incluso en relación con el lugar de fabricación del equipo", diferencia que bien pudiera deberse a una traducción inexacta al confundirse "ubicación de la empresa" (que parece referirse más bien al domicilio social de la empresa suministradora) con "lugar de fabricación de un equipo" dentro de una gran empresa multinacional.

[7] Ver el ya citado "*Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*", NIS Cooperation Group, CG Publication, 01/2020, Annex 2, página 42.

- Finalmente, el contenido de la segunda bola del Toolbox se ha plasmado en tres letras distintas, las d), e) y f), que ya no se refieren solo a la legislación del tercer país (especialmente cuando no tiene contrapesos democráticos o no tiene acuerdos sobre protección de datos con la UE), sino también a las características de su régimen político.

24. Así pues, el artículo 11.1 del Anteproyecto no solo pretende transponer a la legislación española la recomendación elaborada por los expertos europeos en ciberdefensa, sino que la ha hecho todavía más genérica y amplia y ha reducido incluso más el nexo causal o relación de los "aspectos" que menciona con el objetivo de ciberseguridad que el Anteproyecto persigue.

25. Debe señalarse, sin embargo, que la referencia del Anteproyecto a la "cadena de suministros" del propio suministrador, aunque no se mencione en la Toolbox, puede resultar acertada, por el motivo que ya se expuso en mi Dictamen: la cadena de suministro de todos los proveedores mundiales de equipos 5G (incluidos Ericsson y Nokia) es global y lo relevante para el riesgo de interferencia maliciosa de un Estado puede ser más el lugar en que se fabrican que el domicilio social de la empresa suministradora.[8]

26. En su intento por "transponer" lo previsto en la Toolbox, el Anteproyecto parece haber ignorado el tenor de una norma europea, esta sí imperativa, que, acaso por haber sido elaborada por juristas y no meros expertos en seguridad, regula con mayor precisión el ejercicio por los Estados de facultades de control relacionadas con la seguridad nacional: el artículo 4.2 del Reglamento (UE) 2019/452, de 19 de marzo de 2019, para el control de las inversiones extranjeras directas en la Unión. A tenor de ese precepto, "para determinar si una inversión extranjera directa puede afectar a la seguridad o al orden público, los Estados miembros y la Comisión también podrán tener en cuenta, especialmente:

    a) Si el inversor extranjero está controlado directa o indirectamente por el gobierno (incluidos los organismos públicos o las fuerzas armadas) de un tercer país, en particular mediante una estructura de propiedad o una financiación significativa;

    b) Si el inversor extranjero ya ha participado en actividades que afecten a la seguridad o al orden público en un Estado miembro, o

    c) Si existe un riesgo grave de que el inversor extranjero ejerce[9] actividades delictivas o ilegales.

27. Pues bien, la calificación del perfil de riesgo de los suministradores que el artículo 11.1 prevé, junto con las consecuencias que otros preceptos clave atribuyen a esa calificación, se traducen en unas medidas restrictivas del principio de libre empresa y del comercio internacional en cuya configuración legal no se han tomado en cuenta varias exigencias:

    - Las derivadas del principio de reserva de ley que contempla el artículo 53.1 de la Constitución española y de la jurisprudencia del Tribunal Constitucional que lo

[8] Ver Dictamen, párrafos 330-335.

[9] El uso del presente de indicativo "ejerce" en la versión española del Reglamento parece un claro error, pues debiera haberse usado el subjuntivo "ejerza".

interpreta, que no permiten redacciones tan genéricas y ambiguas en esas leyes que priven de contenido real a esa reserva.

- Las derivadas de los tests de idoneidad y proporcionalidad principios que exigen las normas constitucionales y de Derecho Internacional para la aplicación de medidas restrictivas de derechos, incluso cuando persiguen un objetivo de seguridad nacional. .

28. A continuación se analizan las críticas que merece la redacción del artículo.

4.2. Indeterminación

29. Con una llamativa parquedad, el artículo 11.1, tras hablar de las garantías técnicas de funcionamiento de las redes y su protección frente a ataques, se refiere a "su exposición a injerencias externas". Y acto seguido se limita a afirmar que para valorar ese riesgo de "injerencias externas" se valorarán, como mínimo, los siguientes "aspectos":

a) Los vínculos de los suministradores y de su cadena de suministro con los gobiernos de terceros países.

b) La composición de su capital social y la estructura de sus órganos de gobierno.

c) El poder de un tercer Estado para ejercer presión sobre la actuación o ubicación de la empresa.

d) Las características del régimen político y de su política de ciberdefensa, de ese tercer Estado.

e) Los acuerdos de cooperación en materia de seguridad, ciberseguridad, delitos cibernéticos o protección de datos firmados con el país tercero de que se trate, así como los tratados internacionales en esas materias de que sea parte dicho Estado.

f) El grado de adecuación de su normativa de protección de datos personales al Reglamento General de Protección de Datos adoptada por la Unión Europea.

30. En su afán por "no pillarse los dedos" y dar al Anteproyecto toda la flexibilidad necesaria para que su desarrollo reglamentario pueda regular cualquier riesgo imaginable, el Anteproyecto no se molesta siquiera en definir qué entiende por "injerencia" *(interference*) de un Estado o en precisar, aunque sea de forma aproximada, cuáles son los riesgo no-técnicos para la ciberseguridad de las redes 5G españolas que le preocupan y deberán ser tomados en cuenta en su desarrollo reglamentario y aplicación.

31. Es cierto que cualquiera que haya seguido los debates internacionales e iniciativas de los Estados Unidos sobre esta materia y las medidas que ha adoptado contra la compañía Huawei sabe bien que esas referencias veladas a "interferencias" aluden a las acusaciones de que un Estado no occidental (y, en particular, China), gracias a su hipotética influencia sobre algún suministrador de equipos 5G, pudiera introducir en las redes 5G de los países occidentales como España, con propósitos de espionaje o potencial sabotaje, mecanismos de los conocidos como "puertas traseras" (*backdoors*), dispositivos de escucha

(*eaversdropping devices*), programas espía (*spyware*) o mecanismos de sabotaje (*kill switches*). Las autoridades americanas siempre han dado esa explicación para justificar sus medidas contra Huawei.[10]

32. El Anteproyecto, sin embargo, no hace referencia alguna a tales riesgos, en el entendido de que el Gobierno y el Ministerio de Asuntos Económicos y Transformación Digital sabrán descifrar las abstractas referencias del Anteproyecto a "injerencias" y "gobiernos de terceros países". Así pues, tanto el Anexo 2 del Toolbox como el artículo 11.1 del Anteproyecto que lo "transpone" constituyen un refinado ejemplo de la técnica que un prestigioso periodista y lingüista, Alex Grijelmo, ha llamado "la información del silencio":

> "Todo mensaje se expresa tanto por lo que contiene como por aquello que omite pero se deja disponible para que el receptor lo perciba".[11]

33. Ahora bien, habida cuenta de que el artículo 11.2 contempla que, tras la valoración de su perfil de riesgo, el Gobierno pueda calificar a un suministrador como de riesgo alto y que, a tenor del artículo 14.c), esa calificación puede entrañar la prohibición de uso de sus equipos e incluso la eliminación de los ya instalados, resulta inevitable concluir que el artículo 11.1 otorga al Gobierno y al Ministerio de Asuntos Económicos y Transformación Digital verdadera "carta blanca" para prohibir a un operador que utilice como suministrador a cierta empresa (por ejemplo, Huawei) y deposita ciegamente su confianza en que el Poder Ejecutivo no abuse de la discrecionalidad absoluta que el Anteproyecto le otorga.

34. Confirma esa aseveración la propia Memoria del Anteproyecto, que reconoce que, como el mundo de la tecnología cambia con rapidez, la verdadera regulación de la evaluación de los suministradores de equipos y servicios 5G la hará el "Esquema de seguridad para las redes y servicios 5G" previsto en el artículo 10 del Anteproyecto.

35. Nótese que, dada la parquedad y vaguedad del artículo 11, el Anteproyecto no entrañaría cortapisa alguna a que el desarrollo reglamentario de la futura Ley por el Gobierno o su aplicación provisional directa por el Ministerio de Asuntos Económicos y Transformación Digital prohibieran la presencia en las redes 5G españolas de equipos procedentes de suministradores:

    - Que hayan suministrado equipos a Gobiernos de terceros países (lo que podría considerarse un "vínculo" de los señalados en la letra a).

    - Que no coticen en Bolsa o tengan naturaleza cooperativa (lo que podría considerarse aspecto decisivo de la composición de su capital y de su estructura de órganos de gobierno, según la letra b).

    - Que estén domiciliados en un país cuyo régimen político no sea democrático (como indica la letra d).

[10] Puede verse, como ilustración muy reciente, el artículo del embajador americano en Túnez, Donald Blome, del pasado 20 de diciembre de 2020, disponible en https://tn.usembassy.gov/smart-5g-decisions-today-can-preserve-the-security-and-privacy-of-all-tunisians/

[11] Alex Grijelmo, "La información del silencio. Cómo se miente contando hechos verdaderos", Taurus, 2012, p.17-18.

- Que estén domiciliados en un país cuya normativa de protección de datos no se adecúe al Reglamento General de Protección de Datos de la UE (como señala la letra f). Tengamos presente, a ese respecto, que hasta ahora la Comisión Europea solo ha reconocido que proporcionan una protección adecuada de datos Japón, Canadá (para organizaciones comerciales), Suiza, Nueva Zelanda, Israel, Argentina y Uruguay, así como Andorra, islas Fároe, isla de Man, Guernsey y Jersey.[12]

36. Tal y como está redactado el Anteproyecto, para un observador ingenuo y poco informado que no sepa "de qué va la película", constituirá un insondable misterio saber qué uso podría hacer el Gobierno y el Ministerio de Asuntos Económicos y Transformación Digital de esos "aspectos" que deberá valorar, e incluso de otros que el Anteproyecto no menciona, pero no excluye, porque la lista es de mínimos.

37. Pues bien, esa radical indeterminación del artículo 11.1 viola frontalmente la jurisprudencia constitucional sobre el principio de "reserva de ley" que el artículo 53.1 de la Constitución española establece para aquellas normas que regulan los derechos reconocidos en el Capítulo Segundo de su Título I, entre los que se encuentra el de "libertad de empresa" del artículo 38 de la Constitución.

38. Nada habría que reprochar a la previsión de desarrollo reglamentario mediante Real Decreto si el propio Anteproyecto delimitara con suficiente precisión los motivos por los que un suministrados puede ser declarado de "alto riesgo" y, en consecuencia, su actuación en las redes 5G españolas restringida o incluso prohibida. Pero, como el Anteproyecto no contiene ni siquiera atisbo de esa delimitación, la conclusión inevitable es que "deslegaliza" su precepto esencial -el artículo 11, que determina el presupuesto para que puedan aplicarse las limitaciones a la "libertad de empresa"- y, al hacerlo, viola la reserva de ley exigida por el artículo 53.1 de la Constitución.

39. En efecto, según señaló el Tribunal Constitucional en el Fundamento Jurídico 5 de su sentencia 76/2019, de 22 de mayo:

> "Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal "ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica", esto es, "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención" (STC 49/1999, FJ 4)".

40. En suma, la indeterminación y vaguedad del artículo 11.1, pieza esencial del Anteproyecto, lo hace inconstitucional, por ignorar, *de facto*, la reserva de ley que consagra el artículo 53.1 de la Constitución.

[12] Ver "*Adequacy decisions. How the EU determines if a non-EU country has an adequate leve lof data protection*", disponible en https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

4.3. Arbitrariedad

41. Sin perjuicio de esa constatación inicial de que el artículo 11.1 es un precepto "en blanco" que no establece ni siquiera de forma remota cuándo un suministrador podría ser declarado de alto riesgo, la enumeración que hace de los "aspectos" que el Gobierno deberá valorar denota, además, que el precepto resulta inadecuado por dos motivos:

    - Parece basar la valoración del riesgo de una empresa suministradora en ciertas características del Estado en el que tiene su domicilio (aunque ni siquiera el Anteproyecto, al referirse a un "gobierno de terceros países", se refiera de forma expresa al país del que procede la compañía suministradora), como si una empresa privada pudiera ser juzgada por las características de su Estado.

    - Basa la valoración de los posibles riesgos para la ciberseguridad de un suministrador en aspectos cuya relación con dichos riesgos parece remota.

42. A continuación se analizan ambos aspectos.

4.3.1 Indebida equiparación entre empresa y Estado

43. El artículo 11.1 tácitamente equipara a una empresa suministradora con el Estado de su nacionalidad o en el que tiene su domicilio social, incluso aunque la empresa no sea de propiedad del Estado ni esté controlada por este, pues prevé que para evaluar el riesgo para la ciberseguridad que puede entrañar un suministrador de equipos 5G deben tomarse en cuenta ciertas características de ese Estado (como su régimen político o su normativa interna sobre protección de datos).

44. Por ilustrarlo con una metáfora: siguiendo un enfoque similar al del Anteproyecto, para enjuiciar si un coche fabricado por una empresa británica reúne en las carreteras españolas las condiciones idóneas de seguridad sería un "aspecto" relevante, y acaso decisivo, constatar que en el Reino Unido se conduce por la izquierda y los vehículos suelen tener el volante a la derecha. Ese ejemplo es, efectivamente, absurdo, pero sirve para ilustrar los despropósitos a los que puede llevar la confusión entre la valoración de la conducta de una empresa exportadora y la legislación del país en que tiene su sede social.

45. Tengamos presente que esa tendencia a predicar ciertas características de un Estado o de alguna de sus instituciones o principales grupos sociales al conjunto de ciudadanos o empresas que tienen esa nacionalidad o lugar de residencia está en el origen de muchos "estereotipos sociales".

46. Aunque el Diccionario de la Real Academia de la Lengua Española define ese término como "imagen o idea aceptada comúnmente por un grupo o sociedad con carácter inmutable", el *Oxford English Dictionary*, más preciso lo define como "imagen o idea aceptada comúnmente, pero fija y demasiado simplificada (*fixed and oversimplified*), de un tipo particulsr de persona o cosa".

47. Los estereotipos, por desgracia, no son neutros y pueden alteran la percepción no solo de los ciudadanos en su vida social, sino también la de las autoridades públicas, que pueden sucumbir a ellos, de forma inconsciente, cuando redactan normas o toman decisiones que, influidas por esos estereotipos, tienen un efecto discriminatorio contra aquellos colectivos que los padecen. Así, en el caso de la represión de los delitos en Estados Unidos, algunos autores han señalado:[13]

> "Los estadounidenses deducen muchas cosas de los rasgos corporales asociados a la raza, como color de la piel, tipo de pelo, y forma de los ojos, y saben que todos los demás están haciendo inferencias previsibles a partir de esos rasgos (…) De forma consciente o inconsciente, atribuimos a los individuos ciertas características de los grupos a los que imaginamos que pertenecen. Estereotipamos. (…) Sin examinar el papel de los estereotipos en las interacciones más delicadas, nos parece imposible entender el castigo de los delitos en Estados Unidos. (…) Los estereotipos influyen en la actuación de los agentes del orden, los representantes elegidos que establecen el marco bajo el que actúan, y los votantes que eligen a esos representantes (…). La evidencia disponible sugiere que los controles policiales de peatones y vehículos responden a un "perfilado étnico" (*ethnic profiling*). Es decir, eso sugiere que algunos grupos son vistos como más sospechosos independientemente de cómo actúen cuando tienen contacto con los agentes de policía. Como resultado, un gran número de miembros inocentes de tales grupos son objeto de controles y cacheos".

48. El artículo 11 del Anteproyecto parece sucumbir a ese fenómeno de los estereotipos y amalgama íntimamente la nacionalidad de una empresa suministradora de equipos 5G con el Estado del que procede, de forma que el régimen político o la legislación sobre protección de datos en su país de origen pasan a ser aspectos determinantes del riesgo que esas compañías entrañan para la ciberseguridad de las redes 5G españolas. En suma, sin decirlo así de forma expresa, y aprovechando de nuevo la "información del silencio", el Anteproyecto da a entender que el que la RPC sea un régimen comunista arroja un estigma indeleble sobre todas las empresas suministradoras con sede social en ese país. Aunque, por motivos obvios, no lo diga, el Anteproyecto parece estar basado en que a las dos empresas suministradoras de equipos 5G que no son europeas les resulta aplicable un juicio similar al que el general estadounidense John De Witt expresó tras el ataque de Pearl Harbour sobre los japoneses residentes en Estados Unidos:[14] "Un chino es un chino. No hay forma de determinar su lealtad".

49. La indebida equiparación entre un Estado y las empresas domiciliadas en él ha sido objeto también de atención desde la perspectiva del Derecho Internacional y, en especial, de los acuerdos internacionales sobre arbitraje de inversiones, como el Acuerdo de Washington que dio origen al Centro Internacional para el Arbitraje de las Diferencias sobre Inversión (CIADI). La razón está en que tanto ese como otros tratados internacionales de protección de inversiones permiten a inversores privados extranjero demandar en arbitraje al Estado anfitrión en el que invirtieron cuando se consideran víctimas de alguna medida lesiva atribuible a dicho Estado. En esos llamados "arbitrajes de inversión" el Demandado es

[13] Brenadan O'Flaherty y Rajiv Sethi, "*Shadows of Doubt. Stereotypes, Crime and the Pursuit of Justice*", Harvard University Press, 2019, p. Introduction y Chapter 1.
[14] Dictamen, Consideraciones finales, apartado II.

siempre un Estado, pero el demandante no puede serlo, porque no se trata de sistemas de arbitraje entre Estados, sino entre un inversor privado extranjero y un Estado anfitrión.

50. Pues bien, como se demostrará a continuación, a tenor del Derecho Internacional debe distinguirse nítidamente entre un Estado y las empresas en él domiciliadas no solo cuando, como ocurre en Huawei, no existe ninguna relación de propiedad o control entre el Estado y la empresa, sino incluso en aquellos casos en que la empresa es de propiedad estatal, lo que demuestra *a fortiori* la equivocación de equiparar Estados y empresas domiciliadas en ellos.

51. Así, el artículo 25.1 de la Convención del CIADI establece que "la jurisdicción del Centro se extenderá a las diferencias de naturaleza jurídica que surjan directamente de una inversión entre un Estado Contratante (o cualquiera subdivisión política u organismo público de un Estado Contratante acreditados ante el Centro por dicho Estado) y el nacional de otro Estado Contratante".

52. Esa disposición suscitó pronto la cuestión de si podrían iniciar arbitrajes de inversión contra el correspondiente Estado anfitrión las empresas extranjeras que estuvieran participadas accionarialmente por un Estado distinto, cuestión a la que el impulsor de la Convención del CIADI y primer Secretario-General del Centro, Aron Broches, dio en un célebre discurso esta respuesta:

> "En el mundo de hoy la clásica distinción entre inversión pública y privada, basada en la fuente del capital, ya no tiene significado, si es que no está pasada de moda. Hay muchas compañías que combinan capital de fuentes públicas y privadas y sociedades cuyas acciones sobre propiedad en su totalidad del Estado, pero que son prácticamente indistinguibles de una empresa completamente privada, tanto en sus características legales como en sus actividades. Parecería, pues, que a efectos de la Convención, una compañía mixta o sociedad de propiedad estatal no debiera ser excluida del concepto de 'nacional de otro Estado contratante' a menos de que esté actuando como agente del Estado o desarrollando una función esencialmente gubernamental".

53. Surgió así el llamado "test de Broches" (*Broches test*), que permite considerar como inversor privado, a efectos de arbitraje de inversiones, a una empresa de propiedad estatal, a menos que esté actuando como un mero agente o brazo instrumental del Estado.

54. Ese test ha sido utilizado por varios Tribunales arbitrales, como el del reciente caso *Beijing Urban Construction Group (BUCG) v. Republic of Yemen*[15], en el que el Tribunal consideró admisible la demanda de arbitraje presentada contra Yemen por la empresa constructora china BUCG, a pesar de que era propiedad al 100% del Estado chino, porque al actuar como constructora del aeropuerto de Sana no estaba desarrollando funciones gubernamentales en representación del Gobierno chino.

[15] ICSID Case No. ARB/14/30, Decision on Jurisdiction, 31 de mayo de 2017.

55. Mayor interés tuvo todavía, a los efectos de estas Observaciones, el caso *Emilio Agustín Maffezini c. Reino de España*,[16] en el que un ciudadano argentino reclamaba por una actuación de la Sociedad para el Desarrollo Industrial de Galicia (SODIGA), la antigua filial del Instituto Nacional de Industria creada para promover el desarrollo de Galicia. Pues bien, fue aquí el Reino de España el que, distinguiendo con nitidez entre el Reino de España y la empresa SODIGA, señaló que esta era una sociedad constituida según las leyes mercantiles privadas y su actividad era privada: "El hecho de que una parte de las acciones de SODIGA pertenezcan a entidades estatales no altera el carácter comercial privado de la sociedad ni transforma a SODIGA en un organismo estatal. Sus actos u omisiones, por consiguiente, no pueden ser imputables al Estado".

56. En este caso, sin embargo, el Tribunal arbitral admitió la demanda y rechazó el argumento del Reino de España, basándose en que, a la luz de la historia de SODIGA, había sido creada por el Gobierno de España para "llevar a cabo funciones gubernamentales en el ámbito del desarrollo regional". En consecuencia, el Tribunal arbitral se basó tanto en el ya citado "test de Broches" como en lo dispuesto en el párrafo 2 del Artículo 7 del Proyecto de artículos sobre responsabilidad de los Estados, que establece:

> "El comportamiento de un órgano de una entidad que no es parte de la estructura formal del Estado o de una entidad pública territorial, pero que está facultado por el derecho interno de ese Estado para ejercer prerrogativas de poder público, se considerará acción del Estado bajo el derecho internacional, cuando ese órgano haya actuado en tal capacidad en el caso de que se trate".

57. Como ya he indicado, en el caso de Huawei no existe, en mi opinión, el más mínimo indicio de que esté participada o controlada por la RPC o por ninguna otra institución pública. Y eso hace especialmente injustificada su amalgama con el Estado chino, a la vista de que el Derecho Internacional obliga a distinguir entre un Estado y una empresa filial y de que el propio Reino de España sostuvo en el caso *Maffezini* que una entidad pública participada accionarialmente por el Estado, SODIGA, no tenía nada que ver con el Reino de España.

58. Se observa, pues, que el enfoque que parecen sugerir las letras d), e) y f) del artículo 11.1 del Anteproyecto se aleja radicalmente de los estándares del Derecho Internacional y del "test de Broches: a la hora de valorar los riesgos de ciberseguridad de un suministrador no europeo (como, por ejemplo, Huawei), no pueden imputársele los juicios de valor que nos merezcan el régimen político y la legislación de su Estado de origen, salvo que demostremos que la empresa actúa como mero agente de ese Gobierno.

59. Obsérvese, finalmente, que, como ya se indicó, el Anteproyecto parece haber ignorado el tenor de una norma europea imperativa que regula el ejercicio por los Estados de facultades de control relacionadas con la seguridad nacional, el artículo 4.2 del Reglamento (UE) 2019/452, de 19 de marzo de 2019, para el control de las inversiones extranjeras directas en la Unión, que para determinar si una inversión extranjera directa puede afectar a la seguridad o al orden público, pone énfasis, en primer lugar, en si el inversor extranjero está controlado directa o indirectamente por un Estado extranjero.

[16] Caso No. ARB/97/7, Decisión del Tribunal sobre Excepciones a la Jurisdicción, 25 de enero de 2000, párrafos 71 a 89.

4.3.2 Ausencia de correlación entre ciberseguridad y "aspectos" descritos

60. La deficiente formulación del artículo 11.1 puede observarse también si analizamos cuál es la conexión entre el bien jurídico que el Anteproyecto protege -esto es, la ciberseguridad de las redes y servicios 5G españoles- y los "aspectos" que prevé que el Gobierno tome en cuenta para valor el riesgo que un suministrador entraña para ese bien jurídico.

61. En efecto, como ya se indicó en el Dictamen[17], las normas y jurisprudencia de la Organización Mundial del Comercio sobre la "excepción de seguridad nacional" (artículo XXI del GATT), de la Unión Europea sobre el "principio de precaución" y españolas sobre medidas públicas restrictivas para proteger los intereses nacionales, de la Administración Pública o de los ciudadanos, establecen que las autoridades públicas no pueden:

    (i) basar tales restricciones en meras suposiciones o especulaciones, sino que deben basarlas en una evaluación adecuada y completa del riesgo que tenga en cuenta las circunstancias concretas de cada caso (incluidas las medidas ya en vigor para mitigar los riesgos y el coste potencial de la medida restrictiva);

    (ii) adoptar medidas restrictivas que no sean adecuadas o idóneas para alcanzar el objetivo de ciberseguridad que persiguen ("test de idoneidad"); ni

    (iii) adoptar medidas más restrictivas que otras que logren el objetivo público perseguido -esto es, la ciberseguridad- con la misma o mayor eficacia ("test de proporcionalidad").

62. Así pues, la invocación del objetivo de la ciberseguridad no puede ser un "conjuro mágico" (*incantation*) o un "comodín" que proporcione al Gobierno y al Ministerio de Asuntos Económicos y Transformación Digital "carta blanca" para aplicar restricciones sin limitación, sin respetar los tests de adecuación y proporcionalidad, ni llevar a cabo una evaluación adecuada y completa del riesgo que tome en cuenta las circunstancias específicas de cada caso.

63. En el campo del Derecho Internacional y del arbitraje inversiones la existencia de esa "idoneidad" del medio utilizado para alcanzar el fin público perseguido resulta también crucial para determinar si una intervención pública es injustificada o arbitraria, si bien suele expresarse no con el término "idoneidad", sino con la idea de "correlación".

64. En el caso *Electrabel S.A. v. Hungary*,[18] el Tribunal arbitral sintetizó así la doctrina ya establecida sobre el concepto de "arbitrariedad" (*arbitrariness*):

> "Este Tribunal está de acuerdo con los de los casos *Saluka*, *AES* y *Miluka* en que una medida no será arbitraria si está razonablemente relacionada con una política racional. Como subrayó el tribunal del caso AES, esto exige dos elementos: 'la existencia de una política racional; y la razonabilidad del acto del Estado en relación con la política. Una política racional se adopta por un Estado siguiendo una explicación lógica (buen sentido)

[17] Para más detalle, ver Dictamen, apartado 7.2, párrafos 162 a 202.
[18] ICSID Case No. ARB/07/19, de 25 de noviembre de 2015, párrafo 179.

y con el objetivo de abordar una cuestión de interés público. Sin embargo, una política racional no basta para justificar todas las medidas tomadas en su nombre por un Estado. Una medida cuestionada debe también ser razonable. Es decir, tiene que haber una correlación adecuada entre el objetivo de política pública del Estado y la medida adoptada para alcanzarlo. Esto tiene que ver con la naturaleza de la medida y la forma en que es instrumentada'".

65. Esa doctrina en Derecho Internacional y, en particular, en el arbitraje de inversiones de las condiciones precisas para que una medida pública de restricción de derechos de un inversor -como sería una hipotética declaración de Huawei como suministrador de alto riesgo, en base a los "aspectos" señalados en el artículo 11.1- no pueda ser calificada de "arbitraria" o "injustificada" debiera llevar a una redacción más cuidadosa del Anteproyecto, en la medida en que:

- España y China suscribieron el 14 de noviembre de 2005 un Acuerdo para la Promoción y Protección Recíproca de Inversiones, por el que ambos países se comprometieron a que los inversores de la otra parte disfrutaran de protección y seguridad constantes en su territorio y a que no se tomarían medidas injustificadas o discriminatorias contra la gestión, mantenimiento, uso, disfrute y enajenación de las inversiones de inversores de la otra parte.

- Huawei ha efectuado inversiones en España directamente relacionadas con su actividad de suministrador de equipos de telecomunicación.

66. El citado Acuerdo para la Promoción y Protección Recíproca de Inversiones contiene varias disposiciones clásicas en este tipo de Acuerdos (conocidos internacionalmente como *Bilateral Investment Treaties*, BITs):

- El artículo 2.3 establece que "Ninguna de las Partes Contratantes tomará medidas injustificadas o discriminatorias contra la gestión, mantenimiento, uso, disfrute y enajenación de las inversiones de inversores de la otra Parte Contratante.

- El artículo 3.1 establece que "a las inversiones de los inversores de cada Parte Contratante se les concederá, en todo momento, un tratamiento justo y equitativo en el territorio de la otra Parte Contratante".

- El artículo 3.3 establece que "ninguna de las Partes Contratantes someterá las inversiones y actividades asociadas con dichas inversiones de inversores de la otra Parte Contratante a un tratamiento menos favorable que el concedido a las inversiones y actividades asociadas de inversores de cualquier tercer Estado" (salvo lo dispuesto en el artículo 3.4 sobre uniones aduaneras o uniones económicas y monetarias).

- El artículo 4.1 establece que "ninguna de las Partes Contratantes podrá expropiar, nacionalizar o tomar otras medidas semejantes de efecto equivalente a la nacionalización o expropiación (en adelante denominadas «expropiación») contra las inversiones de inversores de la otra Parte Contratante en su territorio, a menos que se cumplan los requisitos siguientes:

a) por causa de utilidad pública.

b) con arreglo a un procedimiento legal interno.

c) de manera no discriminatoria.

d) y mediante indemnización.

67. No resulta preciso efectuar aquí un análisis pormenorizado de la interpretación por sucesivos tribunales arbitrales del contenido de tales principios, pero sí poner énfasis en que del citado Acuerdo hispano-chino se desprende con claridad que cualquier medida que pudiera afectar de forma grave a la inversión que Huawei ya ha efectuado en España -como sería una severa restricción de la venta de equipos 5G para las redes españolas- deberá adoptarse en el marco de un procedimiento que no deje a Huawei en indefensión.

4.4. Indefensión de suministradores

68. Pues bien, el artículo 11 no regula con claridad la naturaleza del procedimiento que el Gobierno y el Ministerio de Asuntos Económicos y Transformación Digital seguirán para valorar los riesgos de ciberseguridad que pueden suscitar los suministradores de equipos y servicios 5G.

69. En efecto, el artículo 20 del Anteproyecto señale, de forma muy escueta, que "los órganos competentes darán audiencia a los titulares de derechos e intereses legítimos que resulten afectados por las instrucciones técnicas, guías orientativas y resoluciones que dicten", pero no está claro que tan sucinta previsión permita a los operadores y a los propios suministradores que pudieran verse afectados por una decisión amparada en los artículos 11 y 14.1 c) la adecuada defensa de sus intereses. Tampoco se señala expresamente que la decisión que adopte el Consejo de Ministros, especialmente cuando resulte desfavorable para un suministrador, deba ser motivada.

70. La vaguedad de esa previsión del Anteproyecto contrasta con el cuidado con el que las normas imperativas sobre ciberseguridad, como el Reglamento (UE) 2019/881 del Parlamento europeo y del Consejo sobre ciberseguridad y, en particular, su artículo 64, reconocen el derecho a la tutela judicial efectiva de los afectados por las decisiones de expedición (o denegación) de los certificados europeos de ciberseguridad.

71. Resultaría, pues, preciso que la evaluación de riesgo prevista en el artículo 11 se instrumente mediante un procedimiento administrativo en el que el suministrador afectado tenga la condición de interesado y cuya resolución final, si resultara perjudical para algún interesado, fuera motivada.

5. Propuestas de mejora del artículo 11 (apartados 1 y 2)

72. La conclusión general de todo lo que antecede es que el Anteproyecto persigue objetivos elogiables y muchos de sus preceptos son perfectamente congruentes con ellos. Tampoco hay nada que objetar, dada la importancia del objetivo de la ciberseguridad, a la amplitud

de las facultades de intervención administrativa que el Anteproyecto contempla para la consecución de ese objetivo.

73. El verdadero "agujero negro" del Anteproyecto está en los apartados 1 y 2 de un artículo clave del Anteproyecto, el 11 (puestos en relación con otros preceptos íntimamente relacionados con ellos, como los artículos 8.3, 14.1 c), 14.4, 19.1 y la Disposición Transitoria), cuya indeterminación e inadecuación dejan el contenido efectivo del Anteproyecto al albur de lo que puedan establecer el Gobierno o el Ministerio de Asuntos Económicos y Transformación Digital en su desarrollo reglamentario y aplicación.

74. Por eso, parecerían aconsejables diversas mejoras en la redacción de los apartados 1 y 2 del artículo 11.

75. En primer lugar, debiera especificarse y aclararse la naturaleza de los "riesgos no técnicos", y hacerse referencia expresa, en aras de los principios de seguridad jurídica y reserva de ley, al segundo de los dos potenciales peligros que justifican en gran medida el Anteproyecto, pero que este paradójicamente silenciado: el riesgo de que algún suministrador de equipos o servicios pudiera ser obligado o inducido a cometer actividades ilegales relacionadas con la ciberseguridad de las redes y servicios 5G en España -tales como espionaje, sabotaje, vulneración de protección de datos o cualesquiera otros delitos cibernéticos-. Esa definición más precisa de la segunda preocupación a la que responde el Anteproyecto acotaría automáticamente el margen de actuación del Gobierno y del Ministerio de Asuntos Económicos y Transformación Digital al desarrollar reglamentariamente y aplicar administrativamente sus preceptos.

76. En segundo lugar, debiera tenerse presente que las medidas técnicas de control de la ciberseguridad de los equipos y servicios que usen las redes 5G pueden mitigar de forma efectiva los hipotéticos "riesgos políticos" de injerencia maliciosa de un Estado extranjero dirigidos a espiar a través de dichas redes o sabotear su funcionamiento y los servicios esenciales que dependan de ellas. Así pues, las medidas técnicas de control tienen un papel decisivo, pues pueden hacer extremadamente remoto el peligro derivado de hipotéticos "riesgos políticos".

77. En tercer lugar, los "aspectos" que menciona el articulo 11.1 no debieran presentarse como factores indiciarios o determinantes de riesgo, sino como una relación ilustrativa de las informaciones que las autoridades españolas podrían recabar de los suministradores para poder formarse un juicio. Y al hacer esa enumeración el Anteproyecto debiera:

    - Corregir aquellas expresiones del artículo 11.1 que pudieran obedecer a una traducción defectuosa de algunas previsiones de la Toolbox.

    - Incorporar algunas expresiones tomadas del Reglamento (UE) 2019/452, de 19 de marzo de 2019, para el control de las inversiones extranjeras directas en la Unión, que resultan más precisas y menos ambiguas que las utilizadas por el Anteproyecto.

    - Añadir algunas informaciones adicionales que pudieran considerarse relevantes (como la relativa a eventuales incidentes previos en materia de ciberseguridad).

78. En cuarto lugar, el Anteproyecto debiera señalar expresamente que la evaluación de riesgos prevista en el artículo 11 y la decisión final del Consejo de Ministros se efectuarán en el marco de un expediente administrativo, de acuerdo con lo que con carácter general establece la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el que el suministrador evaluado tendrá la consideración de interesado y en el que la resolución final del Consejo de Ministros, si limitara los derechos del suministrador, deberá ser motivada. Esa previsión procedimental sería importante no solo desde el punto de vista del escrupuloso respeto de los principios que consagra la Constitución española, sino también para asegurar que el Anteproyecto resulta conforme con el Acuerdo para la Promoción y Protección Recíproca de Inversiones que España suscribió con China.

79. Finalmente, como cuestión terminológica menor, puesto que la calificación de un suministrador como de riesgo "bajo", en la terminología del Anteproyecto, carecerá previsiblemente de trascendencia, parecería preferible que el Anteproyecto se refiera solo a aquellos supuestos en los que una evaluación desfavorable podrá dar origen a medidas limitativas. Además, siguiendo la terminología utilizada por el ya citado Reglamento (UE) 2019/452, de 19 de marzo de 2019, para el control de las inversiones extranjeras directas en la Unión, que es concordante con la utilizada tradicionalmente por las leyes españolas, parecería preferible sustituir las expresiones "riesgo medio" y "riesgo alto" por las de "riesgo grave" y "riesgo muy grave". De esa forma, el Gobierno solo necesitaría determinar si un suministrador -o alguno de sus equipos o servicios- entraña un riesgo grave o muy grave para las redes 5G españolas y, en caso afirmativo, motivar adecuadamente esa decisión.

6. Conclusiones

80. El Anteproyecto objeto de estas Observaciones afirma ser una norma concebida en defensa del bien jurídico de la ciberseguridad, como bien indican su título, su exposición de motivos y buena parte de su articulado.

81. Pero a la vista de extraordinaria vaguedad de uno de sus artículos capitales, el articulo 11; de las graves consecuencias que contempla para aquellos suministradores que el Gobierno declare de "alto riesgo"; del hecho, reconocido por la Memoria del Anteproyecto, que de los cuatro grandes suministradores de equipos 5 G dos tienen su sede en la Unión Europea y otros dos en la República Popular China; y del contexto político en el que la UE elaboró su Toolbox, en plena campaña de la Administración Trump contra la empresa china Huawei, no es descabellado temer que el Anteproyecto, tal y como está redactado, pudiera permitir un desarrollo reglamentario y aplicación por el Gobierno y por el Ministerio de Asuntos Económicos y Transformación Digital que desnaturalizaran el bien jurídico que pretende proteger -la ciberseguridad de las redes 5G españolas- y, so capa de ese objetivo, persiguieran otros objetivos distintos, como la protección comercial de las compañías europeas suministradores de equipos 5G -como paso para lograr la "soberanía digital" de la UE- o la adopción de medidas injustificadas, por motivos culturales o políticos, contra suministradores basados en la República Popular China

82. Si, por el contrario, se diera al artículo 11 del Anteproyecto una redacción mucho más precisa, de acuerdo con los cambios que se han sugerido, permanecerían intactas las extraordinarias facultades de intervención pública en las redes 5G que, en aras de la

seguridad nacional, el Anteproyecto justificadamente contempla, pero su aplicación respetaría tanto las garantías de seguridad jurídica y reserva de ley que nuestra Constitución contempla como las obligaciones que para España dimanan del Acuerdo para la Promoción y Protección Recíproca de Inversiones suscrito entre España y China de 14 de noviembre de 2015.

Madrid, 14 de enero de 2021

Manuel Conthe Gutiérrez

Datos profesionales

NIF: 00666887F
Serrano 26, 4º dcha
28001 Madrid
manuel.conthe@mconthe.com
móvil: 697 801 570

Domicilio particular

Comunidad de Madrid 19, 1º B
28.231 Las Rozas Madrid

APÉNDICE

Manuel Conthe
Serrano, 26 – 4
28001 Madrid
España

Dictamen sobre el riesgo de interferencia estatal (o R5) en Huawei como proveedor de 5G

4 de julio de 2020

Índice

Abreviaturas

AEPD	Agencia Española de Protección de Datos
APD	Autoridades de Protección de Datos
APPRI	Acuerdo de Promoción y Protección Recíproca de Inversiones
ARN	Autoridad Reguladora Nacional
BCP	Plan de Continuidad del Negocio
BSIMM	Modelo de Madurez para el Desarrollo de Software Seguro o "Building Security in Maturity Model"
CCN	Centro Criptológico Nacional
CE	Comisión Europea
CEOE	Confederación Española de Organizaciones Empresariales
CERT	Equipo de Respuesta a Emergencias Informáticas
CGCP	Comité Global de Ciberseguridad Cibernética y de Protección de la Privacidad
CISL	Laboratorio independiente de seguridad
CNMC	Comisión Nacional de los Mercados y la Competencia
CSEM	Metodología de evaluación de la ciberseguridad
CSIRT	Equipo de Respuesta a Incidentes de Seguridad Informática
DDoS	Denegación general de servicio o "Distributed Denial-of-Service"
DPO	Delegado de protección de datos o "Data Protection Officer"
EECC	Código Europeo de Comunicaciones Electrónicas
EIPD	Evaluación de impacto de protección de datos
ENISA	Agencia Europea de Ciberseguridad
GATT	Acuerdo General sobre Aranceles Aduaneros y Comercio
GSPO	Responsable global de privacidad y ciberseguridad" (Global Cyber Security & Privacy Officer)
HCSEC	Centro de evaluación de ciberseguridad de Huawei
IC	Infraestructura crítica
ICE	Infraestructura crítica europea
IED	Inversión extranjera directa
INCIBE	Instituto Nacional de Ciberseguridad
NCSC	UK National Cyber Security Centre o Centro Nacional de Ciberseguridad del Reino Unido
NEI	Redes y sistemas de información o "Networks and information systems"
OMC	Organización Mundial del Comercio
OMV	Operador móvil virtual
PIB	Producto interior bruto
RGDP	Reglamento General de Protección de Datos
RPC	República Popular China
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la información y la comunicación
TJUE	Tribunal de Justicia de la Unión Europea
VAB	Valor Agregado Bruto

7. Introducción

83. He redactado este dictamen profesional (en adelante, el "Dictamen") por encargo de Huawei España, para dar mi opinión sobre las siguientes cuestiones:

    - Si existe riesgo de interferencia por parte de las autoridades públicas chinas sobre Huawei como proveedor de red 5G en España, y

    - Si, en base a su perfil de riesgo, sería adecuado aplicar a Huawei alguna de las restricciones previstas en la medida estratégica 03 (SM 03) del documento "Conjunto de instrumentos de la UE para la seguridad de las redes 5G" (en adelante, la "Toolbox") aprobada por el Grupo de Cooperación NIS en enero de 2020.

84. El presente Dictamen está basado en la información, documentos, respuestas y explicaciones, tanto verbales como por escrito, que me han sido proporcionados por Huawei, junto con la información, las publicaciones y textos jurídicos pertinentes sobre la materia que se encuentran a disposición pública.

85. He supuesto que los documentos que Huawei me ha proporcionado son copias fieles y completas de los originales y, en el caso de las leyes chinas, que su traducción al inglés también es correcta.

86. Mi currículum está disponible públicamente en www.manuelconthe.com. Mi cualificación para escribir este Dictamen se basa en la experiencia que ahí se expone y en particular en mi trabajo como abogado y árbitro internacional desde 2009, y mi experiencia previa como alto funcionario en la Comisión Nacional del Mercado de Valores y en el Ministerio de Economía y Hacienda, así como en el Banco Mundial.

87. Quiero expresar mi agradecimiento a Carmen Ruiz Lorente, directora de la Asesora Jurídica de Huawei España, quien de la manera más amable y efectiva me brindó toda la información y organizó todas las entrevistas que solicité para la elaboración de este Dictamen.

88. El presente Dictamen ha sido elaborado conforme a la legislación española y la interpretación o referencias a las leyes de cualquier otra jurisdicción se han realizado asimismo conforme a la legislación española.

8. Huawei: aspectos generales

8.1. Una historia de éxito

89. Huawei fue fundada originalmente en 1987 por el Sr. Ren Zhengfei y otros cinco inversores como una modesta empresa con sede en Shenzen, un área de China donde las empresas privadas podían expandirse por tratarse de una zona económica especial. Hoy en día es un proveedor global líder de soluciones de Tecnología de la Información y la Comunicación ("TIC"), con alrededor de 194.000 empleados, que opera en más de 170 países y regiones, y da servicio a más de tres mil millones de personas en todo el mundo.

90. Como parte de sus actividades TIC, Huawei se dedica tanto en China como en el resto del mundo no sólo a la investigación, diseño, fabricación y comercialización de equipos de redes de telecomunicaciones, sino que también desarrolla muchas otras actividades y servicios, como tecnología y servicios en la nube, servicios de Internet móvil y fabricación de *smartphones* y otros dispositivos para empresas y consumidores. Sin embargo, este Dictamen se centrará exclusivamente en la actividad de Huawei como proveedor de equipos de 5G para los operadores de red móvil ("ORMs") europeos y españoles.

91. En 2019, los ingresos por ventas de Huawei alcanzaron los 858,8 mil millones de yuan chinos (aproximadamente 123 mil millones de dólares estadounidenses), con un beneficio neto de 62,7 mil millones de yuan chinos (aproximadamente 8,97 millones de dólares estadounidenses) y un *cash flow* operativo de 91,4 mil millones de yuan chinos (aproximadamente 13,1 millones de dólares).

92. Aunque esté concentrada en China, la cadena de suministro de Huawei se extiende por otras partes del mundo, y cuenta con centros de fabricación en Hungría (Budapest), Alemania (Múnich), India (Chennai) y, en el futuro inmediato, también en Francia.

93. Si bien Huawei tiene competidores en todos los segmentos de mercado en los que opera (por ejemplo, la estadounidense Apple, o la china ZTE), como proveedor de equipos de 5G para ORMs europeos, cuenta esencialmente con dos competidores principales:

- Ericsson, proveedor global TIC para operadores de telecomunicaciones, con sede en Estocolmo (Suecia); y

- Nokia, proveedor global de infraestructura de red y de IP, software y mercado de servicios relacionados, con sede en Espoo (Finlandia).

8.2. I+D

94. Es muy probable que el notable crecimiento y el éxito comercial de Huawei se haya visto impulsado por su enorme esfuerzo en I+D. Así, según el Informe Anual de 2019 de Huawei, en ese ejercicio invirtió en I+D más del 10 % de sus ingresos (es decir, alrededor de 18 900 millones de dólares). Y durante la última década, el gasto acumulado en I + D superó los 86.000 millones de dólares. En 2019, tenía 96 000 empleados (es decir, casi la mitad de su plantilla total) dedicados a I+D.

95. Si comparamos los gastos de en I+D por compañías, en el periodo 2018/2019, según el ranking del "*EU Industrial R&D Investment Scoreboard*" Huawei, con un gasto aproximado en I+D de 12.700 millones de euros, ocupó el quinto lugar en el mundo, justo por delante de las estadounidenses Apple e Intel, con Nokia (4.000 millones de euros, en la 36ª posición) y Ericsson (3.400 millones de euros, en la 46ª posición) muy por detrás[19].

[19] *Vid*. *The 2019 Industrial R&D Investment Scoreboard*. (2019, 18 diciembre). Web oficial de la Comisión Europea. https://iri.jrc.ec.europa.eu/scoreboard/2019-eu-industrial-rd-investment-scoreboard.

96. Huawei sostiene que, al no contar con accionistas externos y no cotizar en bolsa, puede centrarse en invertir en I+D+i a medio y largo plazo, en lugar de en los beneficios a corto plazo o en la cotización de la acción.

97. Huawei está pasando de innovar en tecnología, ingeniería, productos y soluciones a llevar a cabo avances en teoría básica y desarrollo de nuevas tecnologías básicas.

98. Como consecuencia de ese enorme esfuerzo en I+D, Huawei cuenta con más de 85.000 patentes activas (entre ellas, más de 40.000 concedidas en Europa y Estados Unidos).

8.3. Estructura corporativa y gobernanza

99. Conforme a sus documentos y declaraciones oficiales, Huawei es una empresa privada propiedad de sus empleados.

100. A través del *Sindicato de Huawei Investment & Holding co., Ltd.* (en adelante y, para abreviar, el "Sindicato") la compañía implementa un "Plan de Titularidad de Acciones para Empleados" (ESOP, según sus siglas en inglés) que involucra a 104.572 empleados. Sólo los empleados de Huawei pueden participar en dicho plan. Ninguna agencia gubernamental u organización externa posee acciones de Huawei. El único otro accionista directo o "registrado" como tal es el Sr. Ren, fundador de la empresa, que cuenta con una participación directa del 1,01 % de Huawei (y una combinada de cerca del 1,14 %, incluida su participación indirecta a través del ESOP).

101. Huawei recuerda que la Ley de Sociedades de China establece un límite de 50 socios para cualquier sociedad de responsabilidad limitada. Por eso, para permitir la participación de una cantidad tan grande de empleados en su capital, Huawei, como muchas otras empresas chinas, tuvo que canalizar la participación de sus empleados a través del Sindicato, una entidad jurídica registrada en la Federación Sindical Shenzen. El Sindicato de Huawei tiene, pues, un doble papel: como "sindicato", tal y como se define esa figura en la Ley de sindicatos de China, por una parte, y como accionista o socio, tal y como se define en la Ley de sociedades de China, por otra, a cuyo efecto actúa como una plataforma colectiva que permite a los empleados de Huawei poseer "acciones virtuales" de la compañía. Estos dos roles están separados y son totalmente independientes entre sí, siendo el primero gestionado por un "comité sindical" y el segundo por una "Comisión de representantes".

102. Huawei se muestra orgulloso de su sólido sistema de gobierno corporativo[20]. Los empleados propietarios de acciones eligen, a razón de un voto por acción, a 115 representantes para que por períodos de 5 años formen la Comisión de Representantes, el máximo órgano de toma de decisiones de Huawei. Dicha Comisión es quien toma decisiones sobre los asuntos de mayor importancia para la compañía, como la distribución de beneficios o los aumentos de capital.

103. Huawei destaca que, a pesar de que sus empleados no poseen "acciones directas" de Huawei -es decir, no están "inscritos" como accionistas de Huawei-, son propietarios, a través del Sindicato de Huawei de "acciones virtuales restringidas", que les otorgan

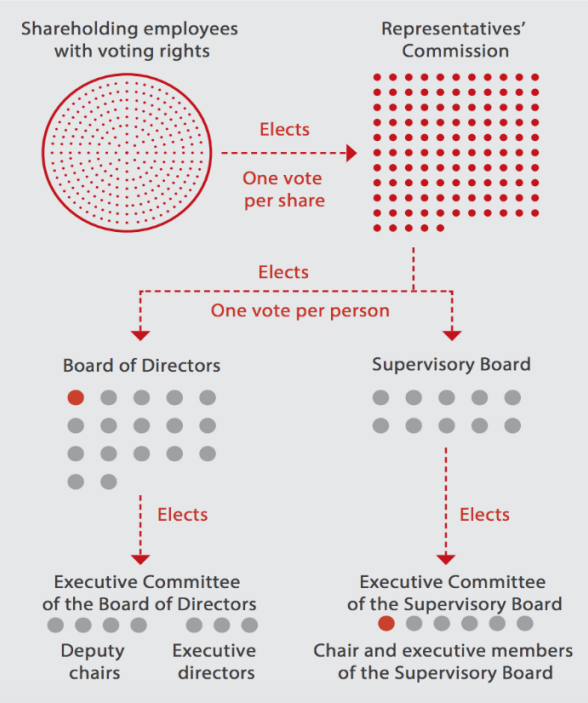
[20] *Cf*. https://www.huawei.com/en/about-huawei/corporate-information.

derechos políticos y económicos y, por lo tanto, no son un mero esquema de participación en beneficios. Según Huawei, actualmente solo los empleados chinos pueden participar en el ESOP, debido a los controles de cambios en China, pero Huawei está estudiando la posibilidad de permitir que los empleados no chinos puedan participar también en el ESOP.

104. La Comisión de Representantes elige al presidente del Consejo de Administración -quien también actúa como presidente de la Comisión de Representantes- y a los otros 16 miembros de dicho Consejo. El Consejo de Administración elige, a su vez, a cuatro vicepresidentes y a tres consejeros ejecutivos. Tres de tales vicepresidentes se turnan para desempeñar el cargo de presidente del Comité Ejecutivo (por lo tanto, el "presidente rotatorio" desempeña un papel similar al del Primer Ejecutivo de una compañía occidental, aunque sólo sea por períodos de seis meses).

105. Cada presidente rotatorio ejerce tales funciones durante un periodo de seis meses. Este peculiar sistema rotatorio refleja el "modelo de liderazgo colectivo" de la compañía, que garantiza que el destino de Huawei no está ligado a ningún individuo. Huawei explica que este sistema de presidencia rotatoria imita los patrones de migración oceánica de ciertas aves, que cambian de posición y se relevan como guías de la bandada.

106. El siguiente diagrama, tomado del Informe Anual de 2019 de Huawei, resume el sistema de gobierno descrito:



107. El presidente rotatorio dirige el Consejo de Administración y su Comité Ejecutivo. El Consejo es el responsable de la estrategia corporativa, la gestión de operaciones y la satisfacción de los clientes.

108. Como fundador de Huawei, el Sr. Ren tiene reconocido derecho de veto sobre ciertos asuntos, para preservar los valores y la dirección a largo plazo de la compañía, derecho que nunca ha ejercido y que no se extiende a decisiones rutinarias o de mera gestión.

109. Como se explicará en la sección 8.1.1 de esta Opinión, algunos analistas externos han cuestionado esta versión oficial de Huawei sobre la estructura de su estructura de propiedad y gobernanza.

8.4. Cumplimiento (*compliance*)

110. Huawei se muestra orgullosa de actuar como empresa con integridad, y respetar los Tratados internacionales y todas las leyes y normas aplicables en los países y regiones donde opera.

111. De acuerdo con la documentación revisada, Huawei ha puesto en práctica un sistema integral de cumplimiento normativo o "*compliance*" en línea con las mejores prácticas internacionales y ha creado equipos que, dedicados a tareas de cumplimiento y supervisión, refuerzan aún más la gestión y supervisión de sus operaciones comerciales globales. Ha elaborado manuales para garantizar el cumplimiento de las leyes y normas TIC locales en los más de 100 países en los que tiene presencia comercial, que toman en cuenta tanto esas normas locales como las exigencias establecidas por las asociaciones de la industria. Huawei tiene responsables de cumplimiento en todas sus filiales europeas, incluida España[21].

8.4.1. La Oficina Global de Protección de la Privacidad y la Ciberseguridad

112. Como parte de su esfuerzo por cumplir las normas más estrictas de protección de la ciberseguridad y la privacidad, y disipar cualquier temor sobre esa materia de sus clientes de fuera de China, Huawei ha creado una Oficina Global de Protección de la Ciberseguridad y la Privacidad (la "Oficina GSPO") dirigida por un Responsable Global de Protección de la Ciberseguridad (GSPO), que depende directamente del Presidente Rotatorio. El actual GSPO es el Sr. John Suffolk, que está basado en el Reino Unido.

113. La Oficina GSPO es la responsable de crear mecanismos integrales de ciberseguridad y protección de la privacidad para los clientes; impulsar la incorporación, por parte de los departamentos pertinentes, de los requisitos de ciberseguridad y protección de la privacidad en los sistemas de gestión de procesos y toma de decisiones empresariales; y de llevar a cabo las correspondientes auditorías.

114. Entre las funciones de la Oficina GSPO se incluyen también las siguientes:

- El funcionamiento del Laboratorio Independiente de Ciberseguridad ("ICSL").

  El ICSL es un centro de verificación de seguridad, independiente de las áreas de negocio y de los departamentos de I + D, creado en 2012 y certificado conforme a la ISO 17025. Utiliza la Metodología de evaluación de la ciberseguridad ("CSEM") que se guía por las amenazas y riesgos de seguridad de los productos de Huawei para someterlos a pruebas de seguridad independientes. El informe de evaluación de un producto por el ICSL sirve para tomar decisiones sobre su lanzamiento. Así, si la prueba

[21] *Cf*. https://www.huawei.com/en/about-huawei/sustainability/win-win-development/develop_honesty.

llevada a cabo por el ICSL detecta que un producto tiene altos riesgos de seguridad, la GSPO puede vetar su lanzamiento. El ISCL actúa de forma transparente para sus clientes, pues estos pueden solicitar acceso a sus plataformas de pruebas, herramientas, métodos de evaluación y resultados.

- Prestar los servicios de verificación de código fuente. Para ello, Huawei ha establecido varios centros de transparencia para que los clientes puedan inspeccionar en ellos el código fuente de los productos de Huawei, como se explica a continuación.

8.4.2. Mecanismos de certificación por terceros

115. De acuerdo con la documentación proporcionada por Huawei, Huawei ofrece garantías de seguridad al cliente no solo a través de pruebas y evaluaciones independientes de sus productos por el propio ICSL de Huawei, sino también a través de laboratorios externos de pruebas de seguridad y de entidades externas de certificación.

116. Como se explicará con más detalle a continuación, Huawei afirma que "es la empresa TIC más abierta, más evaluada y más transparente del mundo, y está sujeta a verificaciones exhaustivas por parte de equipos de expertos de gobiernos, clientes y terceros. Huawei es también la única empresa del sector de telecomunicaciones que está dispuesta a que se revise su código fuente".

117. En el caso específico de España, desde 2010 Huawei cuenta con certificaciones del Centro Criptológico Nacional (CCN) y sus laboratorios acreditados. Actualmente, 25 productos de Huawei han pasado las certificaciones *Common Criteria* España, incluyendo la solución de RAN de 5G, y 10 productos se encuentran en proceso de evaluación, incluyendo la solución Core de 5G. Además, dos centros de desarrollo de Huawei también han sido certificados como centros de desarrollo seguros desde 2013.

8.5. Huawei en Europa

8.5.1. El papel de Huawei en las redes europeas de 4 G

118. Huawei consiguió en 2004 su primer contrato significativo en Europa, con el operador de telefonía móvil holandés Telfort. Un año después, Huawei fue seleccionado como uno de los proveedores estratégicos para el programa de red del siglo XXI de British Telecom. A finales de 2007, Huawei ya había sido concluido contratos con los principales operadores de redes de Europa. En 2014, Vodafone anunció que había adjudicado a Huawei el contrato para actualizar sus redes en 15 países de Europa y África. Actualmente, Huawei forma parte del despliegue de redes de 5G en Italia, Mónaco, Países Bajos, Finlandia, Reino Unido, Suiza, España y otros países.

119. En febrero de 2020, Huawei anunció la construcción de una fábrica de equipos 4G/5G en Francia. Se espera que esta instalación requiera una inversión de más de 200 millones de euros.

120. Al igual que en otros países, los países europeos y los ORMs tienen previsto crear sus redes de 5G no partiendo de cero y creando redes 5G independientes ("*Stand Alone*"), sino

aprovechando las redes de 4G ya existentes (es decir, como redes 5G "*Not Stand Alone*" o NSA).

121. Así, en el caso de la mayoría de los países europeos, incluida España, Huawei ya ha suministrado equipos que están integrados en las redes 4G existentes, de tal manera que cualesquiera restricciones a la participación de Huawei en el desarrollo de las redes 5G europeas podrían representar un importante revés para los operadores, como se indicará más adelante.

8.5.2. Los Centros de Transparencia de Huawei

122. Para asegurarse que sus clientes confían en la fiabilidad y ciberseguridad de sus productos, Huawei ha creado en Europa Centros de Transparencia, que están abiertos a los clientes y a las organizaciones independientes externas, y facilitan pruebas y verificaciones de seguridad objetivas e independientes, de acuerdo con las normas de ciberseguridad y las prácticas reconocidas como idóneas por la industria.

123. Existen tres Centros de Transparencia:

- El primero fue el "Huawei Cyber Security Evaluation Centre" o Centro de Evaluación de la Ciberseguridad de Huawei ("HCSEC"), establecido en el Reino Unido en noviembre de 2010.

  Como se expondrá más abajo, el HCSEC nació de los acuerdos entre Huawei y el Gobierno del Reino Unido para mitigar los riesgos que se percibían en la participación de Huawei en ciertas partes de la infraestructura nacional crítica del Reino Unido. El HSCEC efectúa evaluaciones de seguridad de toda la gama de productos utilizados en el mercado de telecomunicaciones del Reino Unido. A través del HCSEC, el Gobierno del Reino Unido recibe información sobre las estrategias de Huawei en el Reino Unido y su catálogo de productos allí.

- En noviembre de 2018 se estableció un segundo Centro en Bonn (Alemania).

  Dicho centro trabaja en estrecha colaboración con clientes, socios, instituciones de investigación y autoridades gubernamentales y supervisoras de Alemania. Eso permite una cooperación estrecha y regular entre la Oficina Federal de Seguridad de la Información de Alemania y Huawei, centrada en las nuevas tecnologías (especialmente la inteligencia artificial de 5G), el internet de las cosas (IoT) y las Ciudades Inteligentes, los trabajos de estandarización (como los 3GPP) y la verificación de la seguridad de los productos.

  El objetivo del centro alemán es explorar y estandarizar las normas y especificaciones de seguridad de la industria, discutir conceptos innovadores de seguridad para futuras tecnologías y facilitar la colaboración y el diálogo de Huawei con la Oficina Federal Alemana de Seguridad de la Información y los socios de la industria.

- El Centro más reciente se estableció en Bruselas (Bélgica) en marzo de 2019.

Este Centro ofrece una plataforma de verificación y evaluación técnica para los clientes de Huawei, que permite la verificación del código fuente. Su finalidad es responder a los objetivos y necesidades europeos, así como compartir información técnica importante sobre las soluciones de Huawei para hacer frente a las amenazas y vulnerabilidades en materia de ciberseguridad. Además, este Centro también colabora con organizaciones industriales y de estandarización para promover y desarrollar normas de seguridad y mecanismos de verificación. Asimismo, colabora e innova conjuntamente con las organizaciones de verificación de la ciberseguridad de la UE.

8.5.3. Cumplimiento por Huawei del RGPD

124. Uno de los instrumentos normativos europeos en materia de ciberseguridad es, como se expondrá más adelante, el Reglamento (UE) 2016/ 679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, para la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos ("Reglamento General de Protección de Datos" o "RGDP").

125. El RGDP no es sólo el principal instrumento legislativo que regula en la Unión el derecho fundamental de protección de las personas físicas respecto al tratamiento de sus datos personales, sino que se ha convertido en un estándar normativo internacional sobre actividades de tratamiento de datos y su seguridad.

126. El Reglamento General de Protección de Datos adopta el llamado "enfoque basado en el riesgo", de conformidad con el principio de "responsabilidad proactiva", que exige la aplicación de medidas técnicas y organizativas apropiadas en función de la probabilidad y gravedad de los riesgos para los derechos y libertades de las personas físicas (artículo 24 en relación con el artículo 5 del RGPD).

127. Huawei ha implementado un esquema integral de cumplimiento del RGPD basado en los estándares de la industria, que abarca todos los elementos relevantes, incluida la metodología de Evaluación de Impacto de Privacidad ("EIPD") establecida en el artículo 35 del RGPD en todos sus procesos comerciales. De esta manera, a través de tales EIPDs, Huawei incorpora los requerimientos de protección de privacidad desde el diseño de cada proceso comercial.

128. En cuanto a las medidas organizativas, una de las medidas clave establecidas para los operadores de red y proveedores de servicios digitales de comunicación tanto en el RGDP como en la Ley española de Protección de Datos es el nombramiento de un delegado de protección de datos ("DPO") capaz de desempeñar sus funciones de manera independiente.

129. Durante la preparación de este Dictamen, Huawei confirmó que ha implementado las medidas organizativas de "responsabilidad proactiva" ("*accountability*") requeridas por el RGPD, y que ha nombrado un delegado de protección de datos independiente para la Unión Europea ("EU DPO"), como exigen los artículos 37 y 38 del RGPD. La Oficina del EU DPO de Huawei se encuentra ubicada en Düsseldorf (Alemania) y está dirigida en la actualidad por el Sr. Joerg Thomas.

130. El Sr. Thomas ha confirmado que, conforme a las exigencias del RGPD, el DPO no recibe instrucción alguna en cuanto al ejercicio de sus funciones, que no puede ser destituido ni penalizado por el desempeño de sus funciones y que rinde cuentas al más alto nivel directivo (el Presidente Rotatorio) a través del Comité Global de Ciberseguridad y Protección de la Privacidad o "Global Cyber Security and Privacy Protection Committee" ("GCSPC").

131. La competencia de su DPO abarca el tratamiento por Huawei de datos personales procedentes de la Unión, tanto dentro como fuera de ella, en aquellos casos en los que el RGDP resulta de aplicación. Sus funciones incluyen, conforme al art. 39 del RGPD:

- Ser el punto de contacto de las autoridades europeas de control de la protección de datos ("APDs").
- Aprobar una comunicación proactiva con las APDs.
- Monitorizar y auditar el cumplimiento de las normas sobre protección de datos.
- Monitorizar el resultado de las evaluaciones de impacto de protección de datos ("EIPDs").
- Monitorizar la gestión y comunicación de los casos de violación de la seguridad de datos personales.
- Proporcionar orientación y asesoramiento en materia de protección de datos.
- Mantener un buzón de correo del DPO y una línea directa de denuncias ("*whistleblowring hotline*").
- Mantener informada a la Alta Dirección.
- Apoyar en materia de comunicación externa.

8.5.4. El Centro del Reino Unido de evaluación de la ciberseguridad de Huawei

8.5.4.1. El HSCEC

132. Como ya se expuso, el HSCEC nació en noviembre de 2010, fruto de los acuerdos entre Huawei y el Gobierno del Reino Unido para mitigar los riesgos que se percibían por la participación de Huawei en ciertas partes de la infraestructura nacional crítica del Reino Unido.

133. El Centro, propiedad de Huawei Technologies (UK) Co. Ltd, tiene sus instalaciones en Banbury, Oxfordshire, y durante los últimos diez años ha venido proporcionando conocimientos e instrumentos de seguridad técnica a los operadores del Reino Unido y al Centro Nacional de Ciberseguridad de Reino Unido (el "NCSC").

134. Como señaló el último informe presentado por el NCSC al Consejo de Supervisión, el HSCEC sigue "aportando conocimientos únicos y de categoría mundial en materia de

ciberseguridad para ayudar al Gobierno a ejecutar el programa de gestión de riesgos en relación con el uso de equipos de Huawei por los operadores del Reino Unido".

135. El objetivo de la NCSC es exigir al HSCEC que evalúe cada producto de relevancia en el Reino Unido con una frecuencia de, al menos, cada dos años.

136. Las prioridades del HSCEC se fijan de mutuo acuerdo por los operadores del Reino Unido, el NCSC y el HSCEC, sin dejar que ningún operador, por presiones comerciales, tenga un peso indebido en su programa de trabajo, cuya versión final es aprobada por el Director Técnico de Telecomunicaciones del NCSC en nombre del Consejo de Supervisión y sujeta a revisión durante el año por el HSCEC.

137. El proceso de evaluación del HCSEC ha puesto de manifiesto en algunas ocasiones tanto vulnerabilidades puntuales como cuestiones más estratégicas de arquitectura o procesos que debían ser corregidas por Huawei. Sin embargo, como se señalará más abajo, el Consejo de Supervisión del HCSEC ha confirmado la activa participación de Huawei en el proceso de verificación de sus equipos y en los trabajos de corrección necesarios para solucionar los problemas técnicos descubiertos. Las conclusiones transmitidas por el HCSEC a los operadores del Reino Unido, al NCSC y al departamento de I+D de Huawei I+D han ayudado a estos últimos en sus trabajos de corrección.

8.5.4.2. El Consejo de Supervisión (*Oversight Board*)

138. El Consejo de Supervisión del HCSEC se estableció a principios de 2014 y su función es supervisar y garantizar la independencia, competencia y eficacia general del HCSEC como parte de la estrategia global de mitigación en vigor para gestionar los riesgos presentados por la presencia de Huawei en el Reino Unido, así como, sobre esa base, informar al Jefe de Seguridad Nacional (*National Security Advisor*). Este deberá garantizar a los ministros, al Parlamento y, en última instancia, al público en general que los riesgos se están gestionando correctamente.

139. El Consejo de Supervisión está presidido por Ciaran Martin, Consejero Delegado del NCSC, y miembro ejecutivo del Consejo del "*Government Communication Headquarters*" (comúnmente conocido como "GCHQ"), responsable en materia de ciberseguridad. El Consejo de Supervisión tiene como Vicepresidente a un alto directivo de Huawei, y en él participan también altos representantes de la Administración y del sector de telecomunicaciones del Reino Unido.

140. El Consejo de Supervisión se ocupa de las cuestiones más relevantes desde la perspectiva de la seguridad nacional del Reino Unido, como son:

i) La evaluación por el HCSEC de los productos de Huawei instalados o en trance de serlo en el Reino Unido y que, según el criterio absolutamente discrecional del NCSC, son relevantes para el riesgo de seguridad nacional del Reino Unido.

ii) La independencia, competencia y consiguiente eficacia global del HCSEC en el desempeño de sus funciones.

141. El Consejo de Supervisión debe presentar un Informe Anual al Jefe de Seguridad Nacional, que lo trasladará al Consejo de Seguridad Nacional y al Comité de Inteligencia y Seguridad del Parlamento. Los cuatro objetivos de alto nivel del Consejo de Supervisión para el HCSEC han permanecido invariables y son:

- Asegurarse de que, de acuerdo con el programa anual de evaluación del HCSEC, se evalúa la seguridad de los equipos de Huawei utilizados por sus clientes en el Reino Unido.

- Seguir proporcionando confianza al Gobierno del Reino Unido respondiendo de forma clara, transparente y rápida a las inquietudes sobre seguridad del Gobierno o de los clientes del Reino Unido.

- Acreditar una mejora constante de la capacidad técnica, ya sea mediante el resultado de mejoras en la calidad de las evaluaciones o mediante el desarrollo de instrumentos, técnicas o procesos específicos sobre seguridad.

- Que el HCSEC apoye al desarrollo y mejora por el departamento de I+D de Huawei de la capacidad de la compañía en ingeniería de software y ciberseguridad.

142. En su informe más reciente, el Comité de Supervisión efectúa varias declaraciones importantes:[22]

- "3.8 La NCSC sigue pensando que la estrategia de mitigación del Reino Unido, que incluye como componentes la ejecución de trabajos técnicos por el HCSEC y la supervisión de su calidad por el Consejo de Supervisión, es la mejor manera de gestionar el riesgo de que Huawei participe en el sector de las telecomunicaciones del Reino Unido. El descubrimiento de los problemas expuestos en este informe constituye un indicador de que el modelo funciona adecuadamente. Huawei sigue en la actualidad comprometido en ese proceso".

- "3.10 El HCSEC sigue teniendo investigadores sobre seguridad de nivel mundial que están creando nuevas herramientas y técnicas que permiten a la comunidad del Reino Unido comprender la ingeniería de software e implicaciones en materia de ciberseguridad de la singular ingeniería de software y procesos de ciberseguridad de Huawei en la compleja esfera de las telecomunicaciones".

- "3.13 Los operadores del Reino Unido seguirán teniendo que gestionar el significativo riesgo que conllevan los equipos de Huawei para la infraestructura de telecomunicaciones del Reino Unido y se requerirá un trabajo significativo, a lo largo del tiempo, de todas las partes involucradas para reducir ese riesgo en los equipos existentes. El NCSC y los operadores de Reino Unido continuarán trabajando con Huawei para crear un plan de reparaciones de los equipos en el Reino Unido creíble y sostenible . Huawei está de acuerdo en que la reparación de los equipos en el Reino

[22] *Vid*. *Cabinet Office*. (2019, 28 marzo). *Huawei cyber security evaluation centre oversight board: annual report 2019*. GOV.UK. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019.

Unido es independiente de cualquier otro trabajo que Huawei pueda realizar y que se llevará a cabo en tiempo oportuno".

- "3.15 El NCSC considera que el HCSEC sigue siendo competente en los ámbitos de seguridad técnica necesarios para asesorar a los operadores, al NCSC y al Consejo de Supervisión sobre los riesgos de producto y de solución que han sido aceptados al utilizar los productos de Huawei en la infraestructura de telecomunicaciones del Reino Unido. El NCSC manifiesta al Consejo de Supervisión que el HSEC sigue proporcionando unos conocimientos únicos y de primera categoría en materia de ciberseguridad que ayudan al programa en marcha del Gobierno de gestión de los riesgos del uso de equipos de Huawei por los operadores del Reino Unido".

143. Con posterioridad a ese informe, en su "Análisis de la seguridad para el sector de las telecomunicaciones del Reino Unido", el NCSC destacó una vez más la importancia del papel desempeñado por el HCSEC:[23]

> "La existencia del HCSEC proporciona al NCSC y al Gobierno de Su Majestad pruebas claras e imparciales sobre los riesgos que plantea para el Reino Unido el uso de los productos de Huawei por los operadores del Reino Unido. Garantiza que es factible que si se introdujese [en ellos] una funcionalidad maliciosa podría ser detectada, si existiera. El HCSEC despliega una gama de herramientas y de inteligencia artificial para poder escanear los productos de Huawei en el Reino Unido, lo que es complementado con analistas expertos.
>
> Debido a la estrategia de mitigación del Reino Unido, que incluye al HCSEC como un elemento esencial, nuestra evaluación es que el riesgo de presencia de funcionalidades troyanas en los equipos de Huawei sigue siendo manejable. Colocar "puertas traseras" (*backdoors*) en un equipo de Huawei con destino al Reino Unido no sería para el Estado chino el medio de menor riesgo y más fácil si quisiera llevar a cabo un gran ciberataque contra las redes de telecomunicaciones del Reino Unido".

8.6. Huawei en España

8.6.1. El negocio de Huawei en España

144. Huawei comenzó sus operaciones en España en el año 2001, a través de una oficina de representación comercial, para ampliar su negocio como proveedor clave de TICs. Poco después, como muestra de su intención de expandirse en el mercado español, creó una filial con personalidad jurídica propia, "Huawei Technologies España, S.L." (en adelante, "Huawei España").

145. Huawei España cuenta con cerca de 1.000 empleados, de los que el 80% españoles, un 5% chinos y un 15% de todo el mundo. Su sede central se encuentra en Madrid, y tiene otras cinco oficinas en Barcelona, Valencia, Sevilla, La Coruña y Bilbao.

[23] *Vid*. NCSEC. (2020, enero). *Security analysis for the UK telecoms sector. Summary of findings*. https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf.

146. Huawei trabaja con todos los principales operadores de red de España, y ha suministrado equipos o servicios móviles (3G, 4G, etc.), red fija (acceso de fibra, transporte, etc.) y equipos o servicios TIC a, entre otros, Telefónica, Vodafone, Orange y MásMovil.

147. Como parte de su negocio de consumo, ha abierto dos grandes tiendas en Madrid y Barcelona.

148. Huawei tiene también como clientes en España a muchas empresas privadas y, entre ellas, a compañías cotizadas como Banco Santander, BBVA, Caixa Bank, Repsol, Cepsa y Naturgy, y a El Corte Inglés.

149. Huawei también cuenta en España con varios centros de innovación conjunta con Telefónica y Vodafone, respectivamente.

150. Huawei participa en varios comités y asociaciones del sector de TIC, como la Confederación Española de Organizaciones Empresariales[24] ("CEOE") o DIGITALES.

151. Huawei ha participado activamente en la construcción de la red 4G de España, suministrando antenas pasivas y activas, estaciones base, redes de transporte ópticas e IP, soluciones de núcleo de red (tradicionales y virtualizadas), equipos IT (servidores de cómputo, almacenamiento, *switches* de red) para el núcleo de red virtualizado y soluciones de *Edge Computing*, sistemas de soporte y operaciones o servicios asociados, entre otros.

152. Huawei no solo ha participado en España en el establecimiento de las redes de 4G, sino que ha tomado la iniciativa en el desarrollo del 5G, y ha sido el único proveedor que, hasta mayo de 2020, ha contribuido en los dos proyectos piloto de 5G seleccionados por Red.es: el liderado por Vodafone en Andalucía por importe de 24,4 millones de euros[25]; y el liderado por Telefónica en Galicia por importe de 11,5 millones[26]. En ambos proyectos Huawei suministró soluciones integrales.

153. En junio de 2019, Vodafone anunció el lanzamiento del despliegue comercial de 5G en 15 ciudades de España, con Huawei como principal colaborador. Vodafone España también comercializa el Huawei Mate 20 en España, el primer dispositivo de Huawei para 5G.

8.6.2. Relaciones con las autoridades públicas

154. Huawei España y el Instituto Nacional de Ciberseguridad ("INCIBE") firmaron, en el marco del *Mobile World Congress* celebrado en Barcelona en 2016, un Memorando de Entendimiento en el que ambas organizaciones se comprometen a colaborar para promover la ciberseguridad en España. Fue el primer acuerdo de esa naturaleza que Huawei firmó en un país europeo[27].

---

[24] *Vid*. https://www.ceoe.es/en/contenido/huawei-spain-becomes-a-member-of-the-spanish-confederation-of-business-organizations-ceoe.

[25] *Cf*. https://www.red.es/redes/es/actualidad/magazin-en-red/redes-impulsa-la-puesta-en-marcha-del-proyecto-piloto-5g-en-andaluc%C3%ADa.

[26] *Cf*. https://www.telefonica.com/es/web/sala-de-prensa/-/se-pone-en-marcha-el-proyecto-piloto-5g-en-galicia-impulsado-por-red-es.

[27] *Cf*. https://www.huawei.com/en/press-events/news/2016/2/Huawei-Spain-and-INCIBE-sign-a-MoU.

155. Como hoja de ruta conjunta, Huawei España e INCIBE se fijaron en dicho Memorando los siguientes objetivos: crear mecanismos de intercambio periódico de información sobre cuestiones de ciberseguridad; fomentar el intercambio de metodologías para mejorar la ciberseguridad; fomentar la compartición de conocimientos en este ámbito y apoyar la formación y cualificación de las empresas y los profesionales españoles en este ámbito.

9. El Proyecto español 5G

9.1. Red actual de telecomunicaciones de España

156. España tiene uno de los mayores mercados móviles de Europa, con una competencia efectiva de cuatro ORMs y un buen número de revendedores y operadores de redes móviles virtuales. Esta competencia ha reducido el coste de los servicios móviles para el usuario final al tiempo que la inversión en infraestructura de red permitía también hacer frente al aumento continuo, año tras año, del tráfico móvil de datos. Vodafone España fue el primer operador en lanzar una red de 5G en junio de 2019.

157. España tiene cuatro ORMs principales: Telefónica, Vodafone, Orange y MasMóvil. Conforme a la información publicada por la CNMC, durante el primer trimestre de 2019, los tres principales operadores de telecomunicaciones representaron el 77,1 % de los ingresos del mercado minorista del sector[28].

9.2. La hoja de ruta de España en cuanto al 5G

158. Basándose en la información obtenida en la consulta pública llevada a cabo en julio de 2017, el Ministerio de Energía, Turismo y Agenda Digital elaboró el Plan Nacional 5G para el período 2018-2020. Dicho Plan pretende situar a España entre los países más avanzados en el desarrollo de esta tecnología.

159. En España se están llevando a cabo 31 pruebas piloto de 5G, más que en cualquier otro país europeo, incluidas las ya señaladas de Telefónica en Galicia y Vodafone en Andalucía. Ambas pruebas piloto comenzaron en mayo de 2019 y está previsto que finalicen en diciembre de 2020.

160. Para preparar el lanzamiento de las redes de 5G, la subasta del espectro de 3,6-3,8 GHz tuvo lugar en julio de 2018 -y recaudó 438 millones de euros-, pero, debido en parte al Covid-19, la subasta del espectro de 700 MHz -particularmente interesante, por su amplia cobertura, para cubrir territorios escasamente poblados-, prevista para el primer semestre de 2020, ha tenido que posponerse a 2021.

161. La banda de frecuencias de 470 a 790 Mhz iba a ser lanzada en los países miembros de la UE a más tardar el 30 de junio de 2020 para los servicios de comunicación electrónicas móvil de banda ancha. Sin embargo, dada la situación excepcional derivada del Covid-19, España comunicó a la Comisión Europea la necesidad de aplazar la fecha del 30 de junio para completar la liberación del segundo dividendo digital.

[28] Movistar el 42.6%, Orange el 17.7% y Vodafone el 16.8%.

9.3. Huawei como proveedor de 5 G

162. Huawei cuenta con la tecnología y la capacidad para suministrar estaciones base de 5G (antenas, tanto activas como pasivas), RU (*radio units*), unidades de banda base, soluciones de energía para los emplazamientos, transporte óptico, routers IP, elementos de núcleo de red virtualizado, infraestructura (computing, almacenamiento, conectividad), plataformas como el MEC, soluciones de cobertura para interior de edificios, soluciones de *small cells*, infraestructuras de centros de datos (refrigeración, energía, soluciones de alimentación…), dispositivos de usuario de equipos en las instalaciones del cliente, etc.

163. Huawei también cuenta con capital humano para proveer

- servicios de asistencia posventa (es decir, resolución de incidentes y actualización de *hardware* y *software*);
- servicios de operación y mantenimiento (tanto en *hardware* como en *software)*; y
- servicios de despliegue (instalación, integración y optimización, entre otros).

10. Preocupaciones políticas sobre Huawei

10.1. La desconfianza occidental hacia las empresas chinas

164. El temor general surgido espontáneamente en países occidentales a raíz del ascenso económico de las empresas chinas se basa, según una investigadora estadounidense, Sophie Meunier, en dos factores principales:[29]

- El papel central del Estado chino en la economía.

  "*Incluso en el caso de las transacciones realizadas por inversores privados, persisten dudas sobre la influencia real del gobierno chino y del Partido Comunista. Esto ha sido un problema, por ejemplo, a la hora de realizar esfuerzos para invertir en Estados Unidos por parte de Huawei, una empresa privada, cuyo dueño se rumorea que mantiene vínculos muy estrechos con el gobierno chino*".

- China no es un aliado seguro.

  "*Los Estados Unidos y los países europeos no están acostumbrados a recibir inversiones de países que no son sus aliados en materia de seguridad. La Unión Soviética no invirtió en Occidente durante la Guerra Fría. China no es un enemigo, sino una superpotencia con declaradas ambiciones geopolíticas y objetivos de política exterior a menudo en contradicción con los de Estados Unidos y los de algunos países europeos, lo que plantea diversos motivos de preocupación acerca*

[29] *Cfr*. "Beware of Chinese Bearing Gifts: Why China's Direct Investment Poses Political Challenges in Europe and the United States", en el libro "China's International Investment Strategy", Chaisse, J. (Ed.). Oxford University Press, 2019. https://global.oup.com/academic/product/chinas-international-investment-strategy-9780198827450?cc=es&lang=en&.

del motivo último de la inversión, incluidas las cuestiones relativas a la tecnología de doble uso e influencia estratégica".

10.2. Preocupaciones geopolíticas relacionadas con el 5G

165. En el caso específico de Huawei, los temores políticos de los países occidentales se han visto agravados por el liderazgo de la empresa en el desarrollo del 5G, junto con el enorme potencial de esta tecnología.

166. El 5G puede ser, desde luego, un elemento decisivo que puede traer consigo nuevas aplicaciones y oportunidades aún inimaginables. Las principales ventajas de la tecnología 5G son una mayor velocidad en las transmisiones y una menor latencia y, por tanto, una mayor capacidad de ejecución a distancia, un mayor número de dispositivos conectados y la posibilidad de implementar redes virtuales, proporcionando una conectividad más ajustada a necesidades concretas.

167. Si bien no hay pruebas de que el 5G sea en general menos seguro que las redes actuales de 4G, la complejidad de las redes de 5G representa un reto en materia de seguridad. Desde una perspectiva política, se han descrito dos riesgos principales de ciberseguridad:

- La colocación malintencionada en equipos y programas 5G de mecanismos de espionaje *(spyware*), troyanos o "puertas traseras" (*backdoors*) con fines de espionaje político.

  El *spyware* es un *software* no deseado que se infiltra en el dispositivo y roba datos de uso de Internet e información sensible. El *spyware* se utiliza para muchos propósitos. Generalmente, su objetivo es rastrear y vender datos de uso de Internet, capturar datos de tarjetas de crédito o información de la cuenta bancaria, o robar la identidad personal.

  Los troyanos de hardware, también conocidos como circuitos troyanos, son modificaciones de circuitos integrados en chips de ordenador que pueden proporcionar a terceros acceso a datos.

  Una "*backdoor*" o "puerta trasera", en términos de ciberseguridad, es un método para eludir los controles de seguridad para acceder a un sistema informático o datos cifrados. Aunque las puertas traseras pueden ser comunes en algunos equipos de red y software porque los desarrolladores los crean para gestionar los equipos, pueden ser explotadas por eventuales atacantes.

- La colocación malintencionada de dispositivos de sabotaje ("*kill switches*", en el expresivo término popular) para ocasionar interrupciones y cortes intencionados de servicio de las redes de 5G, incluida la denegación masiva de servicios distribuidos (DDos).

168. Las inquietudes políticas se extienden no sólo a la fabricación y diseño iniciales de equipos y programas, sino también a su posterior mantenimiento, actualizaciones y *patches* (parches).

169. El hecho de que Huawei sea una empresa china con sede en China, no cotizada en los mercados internacionales de capital y propiedad de nacionales chinos -empleados de Huawei- ha aumentado en los Estados Unidos y en otros países occidentales, particularmente en aquellos que pertenecen a la llamada alianza de inteligencia "*Five Eyes*" (es decir, Australia, Nueva Zelanda, Canadá y el Reino Unido) la preocupación respecto a quién controla a Huawei y si es, o podría convertirse, en una herramienta que pudieran controlar o utilizar las autoridades políticas chinas o el Partido Comunista Chino (PCC), y convertirse en un instrumento de la política exterior de China.

10.3. Temores especiales de Estados Unidos sobre Huawei

170. En el caso de Huawei y los Estados Unidos, independientemente de cualquier temor sobre nuevos riesgos de ciberseguridad en relación a las redes de 5G, existe probablemente una preocupación mucho más profunda sobre su capacidad tecnológica y liderazgo, debido a que "Huawei ha tomado la delantera en el desarrollo de la próxima generación de tecnología móvil, el 5G, con su promesa de un salto cualitativo en cuanto a conectividad. En caso de que Huawei mantenga y amplíe esa ventaja al mismo tiempo que avance en otros frentes, por extensión, China puede ser el primero en producir una nueva generación de sistemas militares sensibles, redes inteligentes, vehículos de transporte autónomos y otros productos y procesos cruciales. A Estados Unidos le preocupa que tal cambio en el equilibrio de poder entre este país y China amenace su seguridad nacional"[30].

171. En otras palabras, las preocupaciones políticas de los Estados Unidos sobre Huawei no están relacionadas exclusivamente con los riesgos de la tecnología 5G: probablemente son un reflejo de la ventaja tecnológica de China sobre los países occidentales, y el desafío que esto puede entrañar, a medio plazo, a la primacía de los Estados Unidos en las relaciones internacionales.

172. Probablemente como consecuencia de esos temores, la Administración Trump se ha centrado en limitar la actividad internacional de Huawei, en un episodio de lo que algunos académicos han descrito como una versión moderna de la llamada "Trampa de Tucídides ", es decir, el conflicto centenario entre las dos principales ciudades-estado griegas de Esparta y Atenas que el historiador Tucídides explicó así: "Fue el ascenso de Atenas y el miedo que esto inculcó en Esparta lo que hizo inevitable la guerra"[31].

173. Entre las medidas adoptadas por la Administración de Trump contra Huawei se incluyen las siguientes:

- Acusar a la directora financiera de Huawei, la Sra. Meng Wanzhou, la hija de Ren Zhengfei, por fraude y violación de sanciones contra Irán, y solicitar su extradición desde Canadá.

[30] *Cfr*. Pearlstine, Pierson, Dixon, Cloud, Su, Hao Lu (2019, 10 abril). *The Man behind Huawei*. Los Angeles Times. https://www.latimes.com/projects/la-fi-tn-huawei-5g-trade-war/.
[31] *Cfr*. Allison, G. (2017). *Destined for War: Can America and China Escape Thucydides's Trap?* Scribe.

- Prohibir no solo a empresas estadounidenses, sino también a empresas de otros países con proveedores estadounidenses, realizar ciertos tipos de negocios con Huawei.

- Exigir que los gobiernos y empresas de todo el mundo dejen de comprar o utilizar productos y equipos de Huawei y amenazar a aquellos aliados occidentales que no lo hagan con consecuencias adversas, como dejar de compartir información de inteligencia o retirar fuerzas militares.

174. A modo de ilustración de las presiones políticas de Estados Unidos sobre sus aliados, el senador estadounidense Tom Cotton se expresó en estos términos en su reciente testimonio ante el Parlamento del Reino Unido:[32]

> "*Entiendo que se ha aconsejado al gobierno del Reino Unido que la amenaza de Huawei puede ser contenida si se mantiene alejada a esta de instalaciones sensibles en el llamado 'núcleo' de la red. No me adentraré demasiado en ese debate técnico, pero observaré que nuestros propios expertos técnicos no están de acuerdo con esto, al igual que los expertos de otras democracias aliadas como Australia y Japón. Estos mismos expertos también advierten que Huawei podría ayudar a China a obtener una gran cantidad de información dañina, desde detalles sobre cómo combaten nuestras tripulaciones aéreas, hasta información personal intrusiva sobre nuestros propios aviadores. Advierten de escenarios en los que el partido comunista chino podría llegar a hacerse con detalles comprometidos sobre las fuerzas americanas que se encuentran en vuestro país.*
>
> *(..)*
>
> *China es una amenaza más grave a largo plazo para la paz y la estabilidad internacionales que Rusia, así que, en los próximos años, Estados Unidos planea aumentar nuestra postura de defensa en el Pacífico. Ese fortalecimiento puede requerir que desplacemos activos desde otras zonas. Por qué desplegábamos recursos de nuestras fuerzas aéreas en Inglaterra en vez de, digamos, en Alaska, Hawai, Guam o Japón ya fue cuestionado en nuestros debates en Washington. Ahora, los altos cargos estadounidenses se están dando cuenta de que nuestras tropas estarán expuestas a un riesgo operacional de seguridad en el Reino Unido al que no quedarían expuestas en el Pacífico*."

175. Cuando el diputado británico Kevan Jones le respondió que "no hay pruebas de ello. El GCHQ y nuestras agencias de seguridad ha dejado claro que no hay forma de que los equipos de Huawei ni siquiera se acerquen a nuestras señales de inteligencia, o a impactar en las [de Estados Unidos]", el Senador Cotton respondió:

> "*La tecnología de 5G es un salto tecnológico respectos las tecnologías 3G y 4G. Tendrá un papel tan clave en cómo las economías funcionarán en el futuro y en la seguridad de nuestros países que creo que utilizar la tecnología de Huawei, de ZTE o de cualquier otra compañía sometida al Partido Comunista Chino sería como*

[32] *Cfr*. *The Security of 5G,* testimonio del Senador de los Estados Unidos, Tom Cotton. (2020). https://committees.parliament.uk/oralevidence/448/html/.

durante la Guerra Fría hubiéramos confiado en naciones rivales para construir nuestros submarinos o tanques: ni nos lo habríamos planteado. Hay ciertas tecnologías que son tan sensibles y esenciales y vitales para nuestra prosperidad y seguridad que nunca usaríamos la tecnología de una nación rival".

176. El economista estadounidense Jeffrey D. Sachs ha criticado el enfoque de la Administración Trump hacia Huawei y lo ha bautizado como una nueva ilustración de lo que él llama la "doctrina Cheney ":[33]

> "*En el período previo a la Guerra de Irak, el vicepresidente estadounidense Richard Cheney declaró que incluso aunque el riesgo de que las armas de destrucción masiva cayeran en manos terroristas fuera pequeño, digamos del 1 %, deberíamos actuar como si estuviéramos seguros y llevar a cabo la invasión. Los Estados Unidos vuelven a hacer lo mismo, exagerando riesgos ínfimos para crea pánico sobre las tecnologías chinas.*
>
> *El problema con la Doctrina Cheney no es sólo que obliga a tomar medidas basándose en pequeños riesgos sin considerar sus elevados costes potenciales. Es que los políticos se ven tentados a suscitar temores para conseguir otros fines.*
>
> *Esto es lo que los líderes estadounidenses están haciendo de nuevo: crear pánico sobre las empresas de tecnología chinas al plantear, y exagerar, riesgos diminutos. El caso más pertinente (pero no el único) es el ataque del gobierno estadounidense contra la compañía de banda ancha inalámbrica Huawei. Estados Unidos está cerrando sus propios mercados a la compañía y tratando con ahínco de impedir que haga negocios en el resto del mundo. Al igual que en Irak, Estados Unidos podría terminar creando un desastre geopolítico sin razón alguna*".

10.4. La postura del Reino Unido respecto de Huawei

177. En enero de 2020, el gobierno del Reino Unido anunció que Huawei podría suministrar equipos para partes "*no core*" de la red 5G y que su presencia se limitaría al 35 % de la cuota de mercado en acceso por radio.

178. Sin embargo, el 26 de mayo de 2020 la CNBC informó de que el NCSC del Reino Unido había lanzado una revisión de emergencia sobre el papel de Huawei en el Reino Unido después de que los Estados Unidos introdujeran nuevas sanciones a la compañía." [34]

179. Según el *Financial Times*, Vodafone ha advertido de que la ambición del Reino Unido de liderar el mundo en tecnología 5G sufrirá un duro golpe si el gobierno excluye a Huawei de la infraestructura de telecomunicaciones del país. Además, el *Financial Times* también informa de que, a pesar de que los equipos de Huawei en el Reino Unido son fundamentales

[33] *Cfr*. Sachs, J. D. (2019, 7 noviembre). *America's War on Chinese Technology*. Leaders. https://leaders.economicblogs.org/project-syndicate/2019/d-sachs-america-war-chinese-technology-2/.
[34] *Vid*. https://www.cnbc.com/2020/05/26/huawei-5g-ncsc.html.

para lograr el 5G, Boris Johnson se enfrenta a una creciente presión desde Washington y desde su propio gobierno para excluir a Huawei[35].

180. Excede del alcance del presente Dictamen enjuiciar esos acontecimientos políticos, pero se mencionan con el propósito de indicar la gran apuesta política de los EE.UU. contra Huawei y para ayudar a entender su impacto en el enfoque de la UE sobre Huawei.

10.5. Las relaciones UE-China y las aspiraciones de «soberanía digital» de la UE

181. Aunque las relaciones políticas de la UE con China tradicionalmente no habían reflejado contraposición de intereses, en marzo de 2019 la creciente preocupación política por China quedó de manifiesto en la Comunicación presentada al Parlamento y al Consejo por la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, la Sra. Federica Mogherini, sobre la revisión estratégica de las relaciones entre la UE y China[36].

182. Así, en su capítulo IV ("Consecución de una relación comercial y de inversión más equilibrada y recíproca"), dicha comunicación decía:[37]

> "*Las políticas industriales y económicas chinas, proactivas e impulsadas por el Estado, como la de 'Made in China 2025', tiene como objetivo desarrollar campeones nacionales y ayudarles a convertirse en líderes mundiales en sectores estratégicos de alta tecnología. China preserva sus mercados internos para sus campeones, protegiéndolos de la competencia mediante la apertura selectiva del mercado, la concesión de licencias y otras restricciones a la inversión; fuertes subvenciones tanto a empresas estatales como del sector privado; cierre de sus mercados de compras; requisitos relativos a la localización, incluidos los datos; ventajas a los operadores nacionales en la protección y aplicación de derechos de propiedad intelectual y otras leyes nacionales; y limitando a las empresas extranjeras su acceso a programas financiados por el gobierno. Los operadores de la Unión Europea deben cumplir condiciones muy onerosas como condición previa para poder acceder al mercado chino, tales como la creación de filiales conjuntas con empresas locales o la transferencia de tecnologías clave a las contrapartes chinas*".

183. Con este espíritu, la Comunicación hacía un llamamiento a "reforzar la competitividad de la Unión, y garantizar iguales reglas del juego" y sostenía que "la UE debería fomentar la cooperación industrial transfronteriza, con agentes europeos fuertes, con cadenas de valor estratégicas que son clave para la competitividad industrial y la autonomía estratégica de la UE".

---

[35] *Vid*. https://www.ft.com/content/c2fd1c70-3eaa-4e80-8ad3-e88e7bec7d12.

[36] *Vid*. https://ec.europa.eu/commission/publications/eu-china-strategic-outlook-commission-contribution-european-council-21-22-march-2019_en.

[37] *Cfr*. Comisión Europea. (2019, 12 marzo). *EU-China Strategic Outlook: Commission and HR/VP contribution to the European Council*, p. 5. https://ec.europa.eu/commission/publications/eu-china-strategic-outlook-commission-contribution-european-council-21-22-march-2019_en.

184. En el mismo sentido, el capítulo V ("Reforzar la competitividad de la Unión y garantizar las mismas reglas del juego") sostiene que "para garantizar la competitividad a largo plazo de los operadores de la UE, incluso en ámbitos en los que las empresas de la UE no disfrutan de un acceso recíproco al mercado, la UE necesita un ambicioso programa Horizonte Europa abierto a terceros países y organizaciones internacionales a fin de mantenerse a la vanguardia de la investigación y la innovación mundiales, que incluya normas claras sobre la explotación de los resultados y permita un acceso recíproco efectivo a la financiación de la investigación y el desarrollo".

185. Tras estos dos capítulos, el capítulo VI final pasa a centrarse en el "refuerzo de la seguridad de las infraestructuras críticas y la base tecnológica" y afirma que "cualquier vulnerabilidad en las redes 5G podría explotarse para poner en peligro tales sistemas e infraestructuras digitales, lo que podría causar daños muy graves. Toda una serie de instrumentos normativos de la Unión Europea, incluida la Directiva sobre seguridad de las redes y de la información, la recientemente aprobada ley de ciberseguridad y el Código Europeo de Comunicaciones Electrónicas permitirán reforzar la cooperación para hacer frente a los ciberataques y permitir a la UE actuar colectivamente para proteger su economía y su sociedad".

186. El capítulo concluye recomendando como Acción 9 que "como salvaguarda frente a posibles graves implicaciones para la seguridad de las infraestructuras críticas digitales, se necesita un enfoque común de la UE sobre seguridad de las redes 5G. Para ello, la Comisión Europea emitirá una Recomendación después del Consejo Europeo".

187. Este último anuncio fue el prolegómeno de la Recomendación de la Comisión sobre la ciberseguridad de las redes 5G, a la que nos referimos ahora.

11. La "Toolbox" de la UE

11.1. La evaluación coordinada de riesgos de la UE

188. Pocos días después de que se presentara la referida Comunicación sobre la revisión estratégica de las relaciones UE-China, la Comisión adoptó el 26 de marzo de 2019 una Recomendación sobre las amenazas a la ciberseguridad para las redes 5G [38]. La Recomendación solicita a los Estados miembros que realicen análisis nacionales de riesgos, que serán la base de un conjunto común de medidas de mitigación de los riesgos de seguridad del 5G, basándose en el sólido marco legislativo que la UE ya posee sobre protección de las redes de comunicaciones electrónicas. El considerando 24 de la Recomendación hacía un llamamiento para crear una "caja de herramientas" ("*toolbox*") que "ayude a la Comisión en el desarrollo de unos requerimientos mínimos que aseguren un alto nivel de ciberseguridad de las redes 5G en toda la Unión".

189. Sobre la base de estas evaluaciones nacionales de riesgos, el 9 de octubre de 2019 el Grupo de Cooperación NIS, formado por representantes de los Estados miembros, la Comisión y la

[38] Recomendación (UE) 2019/534 de la Comisión, de 26 de marzo de 2019, Ciberseguridad de las redes 5G OJ L 88, 29.3.2019. Esta Recomendación siguió la solicitud que realizó el Consejo Europeo en sus conclusiones de 21 de marzo de 2019, en las que pedía a la Comisión que adoptara una recomendación sobre un enfoque concertado de la seguridad de las redes 5G.

Agencia Europea de Ciberseguridad ("ENISA"), publicó un informe sobre la evaluación coordinada de riesgos de la UE en materia de ciberseguridad en las redes 5G (la "evaluación coordinada de riesgos de la UE")[39] que identifica las principales amenazas y actores que pueden suponer una amenaza, los activos más sensibles y las vulnerabilidades principales (de carácter técnico y de otra naturaleza) que afectan a las redes 5G. Sobre esta base, la evaluación coordinada de riesgos de la UE también identificó una serie de categorías de riesgos de importancia estratégica desde una perspectiva de la UE ilustradas por escenarios de riesgo concretos, que reflejan combinaciones relevantes de los diferentes parámetros (vulnerabilidades, amenazas y agentes que suponen amenazas) en relación a los diferentes activos.

190. Para complementarlo y como aportación adicional a la Toolbox, ENISA llevó a cabo un mapeo específico sobre el panorama de las amenazas[40], consistente en un análisis detallado de determinados aspectos técnicos y, en particular, en una identificación de los activos de la red y de las amenazas que los afectan.

191. La evaluación coordinada del riesgo de la UE sirvió de base para determinar las medidas de mitigación que pueden aplicarse a nivel nacional y europeo.

11.2. Los principales elementos de la Toolbox

192. El 29 de enero de 2020, el Grupo de Cooperación NIS publicó el conjunto de medidas de la UE para la mitigación de riesgos relativos al 5G, la llamada "Toolbox"[41].

193. La Toolbox comienza recordando que, como principal facilitador de futuros servicios digitales, el 5G desempeñará en los próximos años un papel clave en el desarrollo de nuestra economía y sociedad digital. Desde medicina personalizada a agricultura de precisión, desde redes energéticas inteligentes a movilidad conectada, la tecnología 5G puede afectar prácticamente a todos los aspectos de la vida de los ciudadanos de la UE. Al mismo tiempo, debido a su arquitectura menos centralizada, a su capacidad de computación inteligente en la periferia (*edge computing*), a la necesidad de más antenas y a su mayor dependencia del *software*, las redes 5G ofrecen más puntos de entrada potenciales para los atacantes. Garantizar la seguridad de las futuras redes de 5G de la UE es de suma importancia.

194. Si bien los operadores son en gran medida responsables del despliegue seguro del 5G, y los Estados miembros son responsables de la seguridad nacional, la seguridad de las redes es una cuestión de importancia estratégica para toda la UE. Un enfoque coordinado basado en medidas de seguridad sólidas a nivel nacional y de la UE ayudará a Europa a seguir siendo una de las regiones líderes en el despliegue del 5G.

[39] *Vid*. https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.
[40] *Vid*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.
[41] *Vid*. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

11.2.1. Riesgos

195. La Toolbox identifica nueve categorías de riesgo (abreviando, "R") conforme aparecen en la evaluación coordinada de riesgos de la UE, incluida una categoría específica que es el centro de atención del presente dictamen:

- **R5 Interferencia estatal en la cadena de suministro del 5G**

11.2.2. Medidas

196. Tras una larga descripción de los instrumentos jurídicos de la UE disponibles para abordar estos riesgos, que se expondrán más adelante, la Toolbox describe un conjunto de medidas estratégicas y técnicas que los gobiernos de la UE podrían utilizar para hacerles frente. En su anexo 1 profundiza en la descripción de tales medidas, basándose en algunos casos en los criterios previamente establecidos en la evaluación coordinada de riesgos de la UE.

197. Las "medidas estratégicas" ("SM", abreviadamente) más relevantes a los efectos del presente Dictamen son las siguientes:

- SM01 Fortalecer el papel de las autoridades nacionales

- SM02 Realizar auditorías sobre los operadores y solicitarles información

- **SM03** Evaluar el perfil de riesgo de los proveedores y aplicarles restricciones a los considerados de alto riesgo para activos clave -incluida su exclusión si fuera necesaria para mitigar eficazmente los riesgos-.

  A tal fin, se espera que los Estados miembros

  - Establezcan un marco con criterios claros, que tome en cuenta los factores de riesgo identificados en el punto 2.37 de la evaluación coordinada de riesgos de la UE y añada información específica del país (por ejemplo, evaluación de amenazas por parte de los servicios de seguridad nacional, etc.), de forma que las autoridades nacionales competentes y los ORM puedan:

    - Realizar evaluaciones rigurosas del perfil de riesgo de todos los proveedores relevantes, ya sea a nivel nacional y/o de la UE (por ejemplo, evaluaciones conjuntas con otros Estados miembros u otros ORM).

    - Sobre la base de la evaluación del perfil de riesgo, establecer restricciones -incluidas las exclusiones que sean necesarias para mitigar eficazmente los riesgos- para los activos clave considerados críticos o sensibles en la evaluación coordinada de riesgos de la UE (por ejemplo, funciones de núcleo de red, funciones de gestión y orquestación de la red y funciones de acceso a la red);

  - Adopten medidas para garantizar que los ORM dispongan de controles y procesos adecuados para gestionar los posibles riesgos residuales, como auditorías periódicas de la cadena de suministro y evaluaciones de riesgos, una sólida gestión

de riesgos y/o requisitos específicos para los proveedores en función de su perfil de riesgo.

Según el punto 2.37 de la evaluación coordinada del riesgo de la UE, el perfil de riesgo de un proveedor puede evaluarse sobre la base de varios factores, en particular:

- La probabilidad de que el proveedor esté sujeto a interferencias de un país no comunitario. Este es uno de los aspectos clave en la evaluación de las vulnerabilidades no técnicas de las redes 5G. Esas interferencias pueden verse facilitadas, sin carácter exhaustivo, por los siguientes factores:

  - Un fuerte vínculo entre el proveedor y el gobierno de un determinado país tercero;

  - La legislación del ese país tercero, especialmente cuando no existen controles o contrapesos legislativos o democráticos, no hay de acuerdos de seguridad o protección de datos entre la UE y el país tercero (en este contexto, varios Estados miembros atribuyen un perfil de riesgo más elevado a los proveedores sujetos a la autoridad de países terceros que llevan a cabo una política cibernética agresiva);

  - Las características de la estructura corporativa de propiedad del proveedor;

  - La capacidad del país tercero para ejercer cualquier forma de presión, como respecto al lugar de fabricación de los equipos.

- La calidad global de los productos y prácticas de ciberseguridad del proveedor, incluido el grado de control sobre su propia cadena de suministro y si da la prioridad adecuada a las prácticas de seguridad.

- SM05 Garantizar la diversidad de proveedores para los distintos ORMs a través de estrategias adecuadas de proveedores múltiples ("*multi-vendor strategies*").

  Garantizar que cada operador móvil cuenta con una estrategia adecuada de varios proveedores teniendo en cuenta las limitaciones técnicas y los requisitos de interoperabilidad de las diferentes partes de una red 5 G:

  - Evitar o limitar cualquier dependencia importante de un único proveedor (o proveedores con un perfil de riesgo similar);

  - Evitar la dependencia de proveedores considerados de alto riesgo en el sentido de la SM03.

198. Como se indicó en la Introducción, el presente Dictamen se centra exclusivamente en la medida estratégica 3 (SM 03), y no abordará la cuestión de la diversidad de proveedores (SM 05).

199. Entre las "medidas técnicas" ("TM") recomendadas, hay una que también es pertinente para el presente dictamen:

- TM09 Uso de certificaciones UE para los componentes de la red de 5G, equipos de cliente y/o procesos de proveedores.

Con arreglo al marco común de certificación de ciberseguridad de la UE, la Comisión deberá publicar antes de julio de 2020 el Programa Continuo de Trabajo de la Unión para el desarrollo de los sistemas de certificación a escala de la UE. La Comisión deberá considerar la posibilidad de incluir dentro del marco de certificación de la UE sistema(s) relevante(s) a escala de la UE de certificación de componentes críticos de la red usados en las redes 5G y/o de equipos 5G de clientes (por ejemplo, eSIMs y material criptográfico relacionado).

En una fase posterior deberá también examinarse si la certificación de procesos de proveedores podría igualmente añadirse al referido Programa de Trabajo Continuo de la Unión.

11.2.3. Recomendaciones:

200. Las principales recomendaciones de la Toolbox son las siguientes:

i. Todos los Estados miembros deben asegurarse que disponen de medidas (incluidas facultades de las autoridades nacionales) para responder de forma adecuada y proporcional a los riesgos ya identificados y a los futuros, y garantizar, en particular, que, en atención de un abanico de motivos relacionados con la seguridad, pueden restringir, prohibir y/o imponer requisitos o condiciones específicas, siguiendo un enfoque basado en el riesgo, al suministro, despliegue y funcionamiento de los equipos de la red de 5G.

En particular, deberán:

- Reforzar los requisitos de seguridad para los operadores de redes móviles (por ejemplo, controles estrictos de acceso, normas de funcionamiento seguro y supervisión, limitaciones a la externalización de funciones específicas, etc.);

- Evaluar el perfil de riesgo de los proveedores; y, en consecuencia, aplicar las restricciones pertinentes a los proveedores considerados de alto riesgo - incluidas las exclusiones necesarias para mitigar eficazmente los riesgos-, para los activos clave definidos como críticos y sensibles en la evaluación coordinada de riesgos de la UE (por ejemplo, funciones de núcleo de red, gestión de red y funciones de orquestación, y funciones de acceso a la red);

- Asegurarse de que cada operador tiene una estrategia adecuada de proveedores múltiples que evite o limite cualquier dependencia importante de un único proveedor (o de proveedores con un perfil de riesgo similar), garantice un equilibrio adecuado de proveedores a nivel nacional y evite la dependencia de proveedores considerados de alto riesgo; esto también requiere evitar situaciones de vinculación tecnológica (*lock-in*) con un único proveedor, fomentando una mayor interoperabilidad de los equipos;

ii. La Comisión Europea, junto con los Estados miembros, deberá contribuir a:

- Mantener una cadena de suministro de 5G diversa y sostenible que evite una dependencia a largo plazo, y, a tal fin:

  - Hacer pleno uso de los instrumentos y herramientas de la UE, en particular analizando las posibles inversiones extranjeras directas que afecten a activos clave de 5G y evitando distorsiones en el mercado de suministros del 5G provocadas por posibles prácticas de dumping o subvenciones; y

  - Continuar reforzando las capacidades de la UE en tecnologías 5G y posteriores, utilizando a tal fin los programas y financiación pertinentes de la UE.

- Facilitar la coordinación entre los Estados miembros en materia de estandarización, a fin de alcanzar objetivos específicos de seguridad y desarrollar sistemas de certificación pertinentes a escala de la UE que promuevan productos y procesos más seguros.

11.2.4. Naturaleza Legal

201. La Toolbox podría describirse en general como un instrumento de "soft law" sobre riesgos para la ciberseguridad, destinado a guiar a los Estados miembros de la UE, mediante recomendaciones, en la aplicación de la extensa legislación comunitaria ("hard law") sobre el sector de las telecomunicaciones.

202. La Toolbox reconoce que será responsabilidad de los respectivos gobiernos decidir qué medidas consideran apropiadas:

> "*Al seleccionar las medidas que es necesario adoptar, cada Estado miembro decidirá sobre la idoneidad de dicha medida*"[42].

> "*Cómo utilizar la Toolbox. Paso 3: el Estado miembro estudia las medidas recomendadas y los planes de mitigación, selecciona la(s) medida(s) que tendrán mayor efecto y tendrá en cuenta los potenciales factores de su aplicación, ya sea individualmente o con otros Estados miembros alineados*"[43].

203. La respuesta de la Comisión Europea a la pregunta "¿son obligatorias las medidas de la Toolbox?", aunque no es particularmente esclarecedora y es un poco asimétrica, confirma que la caja de herramientas no contiene reglas de obligado cumplimiento:[44]

> "*La Toolbox de la UE sobre ciberseguridad del 5G es un documento elaborado y acordado por el Grupo de Cooperación NIS, formado por representantes de las instituciones de todos los Estados miembros, de la Comisión y de la Agencia Europea*

[42] Toolbox, párrafo 5.2.
[43] Toolbox, cuadro 4, *How to use the toolbox*.
[44] *Cfr*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127.

de la Ciberseguridad. El desarrollo por la UE de un enfoque coordinado en materia de ciberseguridad del 5G se basa en el firme compromiso tanto de los Estados miembros como de la Comisión de utilizar y aplicar plenamente un conjunto clave de medidas recomendadas. La Toolbox establece una metodología precisa y objetiva para afrontar los riesgos identificados en la evaluación de riesgos europea de octubre de 2019, pero respeta las competencias nacionales en este ámbito.

Al mismo tiempo, el despliegue y funcionamiento de las redes 5G es una cuestión de seguridad nacional. Los Estados miembros pueden ir <u>más allá</u> de lo que se propone en la Toolbox cuando constaten la necesidad de hacerlo".

204. La Toolbox, al igual que los documentos en los que se basa, es un documento básicamente acordado por las autoridades nacionales de ciberseguridad, en el que se describen de manera extensa los riesgos relativos al 5G que se han identificado, así como las posibles medidas estratégicas y técnicas para hacerles frente, pero sin intentar dilucidar o debatir las posibles limitaciones jurídicas y constitucionales que los Estados miembros como España tendrían que respetar al tomar en consideración algunas de las medidas estratégicas recomendadas (y en particular, al llevar a cabo la evaluación de proveedores descrita como SM03).

12. El marco jurídico de las redes 5G

205. En esta sección se llevará a cabo un análisis jurídico de las normas imperativas, tanto europeas como nacionales, aplicables a las redes españolas de telecomunicaciones.

206. La conclusión clave del análisis será que España dispone de un sólido marco jurídico y reglamentario que dota a las autoridades españolas de todas las competencias sugeridas por la Toolbox de la UE. Sus amplias facultades para hacerlas cumplir -en caso necesario mediante imposición de multas o medidas correctoras-, pueden ser un instrumento muy eficaz para mitigar riesgos.

12.1. Los tres marcos normativos básicos

207. Como se indica tanto en la evaluación coordinada de riesgos de las redes 5G a nivel de la UE como en la Toolbox, las normas de obligado cumplimiento sobre requisitos de seguridad del ecosistema de redes de 5G y sistemas críticos conexos se contienen en los siguientes tres grandes marcos reglamentarios de la UE:

- El marco de las telecomunicaciones de la UE.
- La Directiva NIS.
- La Ley de Ciberseguridad de la UE (Reglamento sobre ENISA).

208. Para apoyar la puesta en práctica de estas obligaciones e instrumentos, la Unión ha creado una serie de organismos de cooperación:

- El Grupo de Cooperación NIS creado por la Directiva NIS, que reúne a las autoridades competentes y apoya y facilitar la cooperación entre ellas, en particular mediante orientación estratégica.

- La red de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT), que reúne a esos equipos nacionales de los Estados miembros de la UE y facilita el intercambio de información operativa.

  ENISA, la Comisión, los Estados miembros y las autoridades nacionales de reglamentación - en España, principalmente la Comisión Nacional de los Mercados y la Competencia (CNMC) y la Agencia de Protección de Datos (AEPD)- han elaborado directrices técnicas para las autoridades nacionales de reglamentación sobre notificación de incidentes, medidas de seguridad, amenazas y activos.

209. Aunque la Toolbox no incluye la normativa sobre protección de datos y privacidad entre los marcos "principales", sino que lo considera solo un marco regulatorio "relevante" o "potencialmente relevante", lo analizaremos más adelante, teniendo en cuenta, en particular, que las competencias legales y de ejecución con las que ya cuenta la AEPD constituyen un importante factor de reducción del riesgo. De hecho, la Recomendación de la Comisión sobre la ciberseguridad de las redes 5G subraya que asegurar un alto nivel de protección de datos y de privacidad es un elemento importante para garantizar la seguridad de las redes 5G. [45]

12.2. El marco de telecomunicaciones de la UE

210. Según el marco de las telecomunicaciones de la UE, los Estados miembros en los que un operador de telecomunicaciones presta servicios pueden imponerle obligaciones.

211. A tenor del artículo 13 bis de la Directiva marco[4647], los Estados miembros deben garantizar el mantenimiento de la integridad y la seguridad de las redes públicas de comunicaciones, y asegurarse de que las empresas que suministran redes públicas de comunicaciones o servicios de comunicación electrónica accesibles al público adoptan las medidas técnicas y organizativas apropiadas para gestionar adecuadamente los riesgos de la seguridad de las redes y los servicios.

212. El marco regulatorio asimismo exige que las autoridades nacionales competentes cuenten con competencias para dictar instrucciones vinculantes y garantizar su cumplimiento. Además, en virtud de la Directiva 2002/20/CE ("Directiva autorización"), los Estados miembros pueden añadir a una autorización general las condiciones relativas a la seguridad de las redes públicas contra accesos no autorizados. La Toolbox también recuerda las obligaciones de protección de la confidencialidad de las comunicaciones que establece el

[45] Considerando (16) de la Recomendación de la Comisión sobre Ciberseguridad de las redes 5G.
[46] Artículo 13a sobre la seguridad e integridad de las redes y los servicios de la Directiva 2002/21/CE, modificado por la Directiva 2009/140/CE; y los artículos 40 y 41 de la Directiva 2018/1972.
[47] *Vid*. para más información sobre el artículo 13a, la página web del grupo de expertos del artículo 13a disponible en https://resilience.enisa.europa.eu/article-13.

artículo 4 de la Directiva 2002/58/CE, sobre privacidad y comunicaciones electrónicas[48], a la que haremos referencia más adelante.

213. El futuro Código Europeo de Comunicaciones Electrónicas ("EECC"), que sustituirá al marco normativo actual a partir del 21 de diciembre de 2020, mantiene las disposiciones de seguridad de este (artículos 40 y 41 del título V) e introduce asimismo definiciones sobre la seguridad de las redes y los servicios[49].

214. A efectos del presente Dictamen, conviene destacar que, como se indica en la Toolbox, ni el marco actual ni el futuro EECC contienen disposiciones directamente aplicables a los fabricantes de equipos de red y otros proveedores de servicios, ya que no entran en su ámbito de aplicación.

215. En España, al igual que en la mayoría de los países europeos, la legislación vigente ya otorga a las autoridades las competencias previstas en la Toolbox, debido a que la Ley 9/2014, de 9 de mayo (la "Ley General de Telecomunicaciones") traspuso la Directiva 2009/140/CE, de 25 de noviembre, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicos.

216. Así, el artículo 44 de la ley General de Telecomunicaciones establece las obligaciones en materia de integridad y seguridad de las redes públicas de comunicaciones, y otorga a la autoridad española competente en telecomunicaciones (actualmente, la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales) la facultad de dictar instrucciones vinculantes para los operadores y exigirles que:

- Proporcionen información para evaluar la integridad y seguridad de sus redes, incluidas sus políticas de seguridad.

- Permitan que organismos independientes o autoridades competentes realicen, a cargo del operador, auditorías de seguridad y notifiquen sus resultados al Ministerio.

217. Dicho esto, esas facultades no contemplan el establecimiento de un mecanismo de selección de proveedores ni la imposición de límites a las cuotas de mercado.

218. En el ejercicio de las facultades descritas, la Autoridad de Telecomunicaciones de España actuará de acuerdo con ENISA, la Secretaría de Estado del Ministerio de Interior (en lo que respecta a infraestructuras críticas) y la CNMC (respecto a sus facultades reguladoras y de competencia en el mercado de las comunicaciones).

[48] Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

[49] El apartado 21) del artículo 2 define la 'seguridad de las redes o servicios' como 'la capacidad de las redes y servicios de comunicaciones electrónicas de resistir, con un determinado nivel de confianza, cualquier acción que comprometa la disponibilidad, autenticidad, integridad y confidencialidad de dichas redes y servicios, de los datos almacenados, procesados o transmitidos y la seguridad de los servicios conexos que dichas redes y servicios de comunicaciones electrónicas ofrecen o hacen accesibles'.

219. Al margen de esos aspectos puramente reglamentarios, la Ley 9/2014 consagra en varias ocasiones el principio de libre competencia en la prestación de servicios de comunicaciones electrónicas, por ejemplo:

- como objetivo y principio general (artículo 3 bis);
- como principio rector para los operadores del mercado (apartado 5.1);
- como principio rector para las administraciones públicas (artículo 9.2); y
- como principio rector de la regulación *ex ante* del mercado (artículos 13 a 18), la definición de las obligaciones de servicio público y servicio universal (artículos 23 y 25), la ocupación de la propiedad pública y privada o las condiciones que deben cumplir las instalaciones y los instaladores (artículo 59).

12.3. La Directiva NIS[50]

220. La Directiva NIS establece requisitos de seguridad y notificación de incidentes para los operadores de servicios esenciales en infraestructuras digitales y otros sectores (energía, finanzas, asistencia sanitaria, transporte) y para los proveedores de servicios digitales (servicios de *cloud computing* y de mercados en línea y motores de búsqueda).

221. La Directiva NIS fue traspuesta en España por el Real Decreto-ley 12/2018, de 7 de septiembre y, al igual que la Directiva, no resulta de aplicación a las empresas proveedoras de redes públicas de comunicación o servicios de comunicación electrónica accesibles al público, excepto cuando sean considerados "operadores críticos" en virtud de la normativa sobre Infraestructuras Críticas (Ley 8/2011, de 28 de abril, por la que se establecen medidas protección de las infraestructuras críticas). Dicha exclusión obedece a que las disposiciones de seguridad para los operadores de redes públicas de comunicación o servicios de comunicación electrónica accesibles al público ya están reguladas bajo el marco de las telecomunicaciones.

222. Para cumplir lo previsto en la Directiva NIS sobre Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT)/Equipo de Respuesta a Emergencias Informáticas (CERT), España creó, para el sector público, el CCN-CERT del Centro Criptológico Nacional, que actúa como coordinador principal, el INCIBE-CERT del Instituto Nacional de Ciberseguridad para entidades del sector no público y particulares y, finalmente, el ESPDEF-CERT del Ministerio de Defensa para los servicios esenciales o de defensa nacional. La legislación española refuerza también la coordinación entre los Estados miembros en caso de incidentes transfronterizos que afecten a operadores.

[50] Directiva (UE) 2016/1148, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

12.4. El Reglamento europeo de ciberseguridad[51]

223. La denominada "Ley de ciberseguridad" de la UE es un Reglamento de la Unión Europea que entró en vigor en junio de 2019, pero que contiene varios artículos que no entrarán en vigor hasta el 28 de junio de 2021. Como reglamento comunitario, tiene efecto directo en España. Crea un marco para los esquemas europeos de certificación de la ciberseguridad y las declaraciones de conformidad UE para los productos, procesos y servicios TIC.

224. El Reglamento aborda específicamente el denominado riesgo de "dependencia", entendido como la dependencia e integración de productos y sistemas modernos TIC con una o más tecnologías y componentes de terceros, como módulos de software, *libraries* o *application programming interfaces*. El Reglamento reconoce que esta "dependencia" podría plantear riesgos adicionales de ciberseguridad, ya que las vulnerabilidades detectadas en componentes de terceros también podrían afectar a la seguridad de los productos, servicios y procesos TIC.

225. Una vez que el Reglamento se aplique plenamente, los esquemas de certificación también permitirán a los fabricantes o proveedores demostrar que han incluido características específicas de seguridad en las primeras etapas del diseño de los productos y a los usuarios cerciorarse del nivel de garantía de seguridad, a escala de la UE. Tal y como se reconoce en la Toolbox, el marco constituye un instrumento de apoyo esencial para promover niveles consistentes de seguridad.

226. El Reglamento permite el desarrollo de esquemas de certificación de ciberseguridad que respondan a las necesidades de los usuarios de equipos y programas informáticos relacionados con 5G, y asimismo prevé que los Estados miembros puedan adoptar normativa técnica a nivel nacional que exija la certificación obligatoria en el marco de un sistema europeo de certificación de ciberseguridad y que se sirva de tales esquemas en la contratación pública.

12.5. Normas de protección de datos y privacidad

12.5.1. El Reglamento general de protección de datos (RGPD)[52]

227. El RGPD no es sólo el principal instrumento legislativo que regula en la UE el derecho fundamental de protección de las personas físicas en relación con el tratamiento de sus datos personales, sino que también se ha convertido en el estándar internacional de cumplimiento en materia de tratamiento de datos y de seguridad de dicho tratamiento.

228. Aunque los proveedores de equipos 5G y otros proveedores de servicios no llevan a cabo actividades de procesamiento de datos sujetas al RGDP, este resulta aplicable a la mayoría de las amenazas a la ciberseguridad y en algunas situaciones a los proveedores de equipos 5G.

[51] Reglamento (UE) 2019/881, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación.

[52] Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

229. Para los proveedores de equipos 5G, como Huawei, sirven de mitigadores de riesgos:

- La necesidad de llevar a cabo evaluaciones de impacto relativas a la protección de datos (EIPD), como se exigen el artículo 35 del RGPD y el artículo 28 de la Ley española de Protección de Datos;

- La adopción de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad acorde con los riesgos (artículo 32 del RGPD), sobre todo porque no hacerlo puede considerarse una infracción grave en virtud del artículo 73 d) de la Ley española de protección de datos;

- La adhesión a los mecanismos de certificación y cumplimiento de los principios de protección de datos, desde el diseño y por defecto, establecidos en el artículo 25 del RGDP.

12.5.2. Normativa española sobre protección de datos

230. España era desde 1992, antes de la aprobación del Reglamento General de Protección de Datos de la UE, uno de los países de la UE con la normativa más estricta y exhaustiva en materia de protección de datos (incluida la seguridad informática del tratamiento).

231. Posteriormente, a partir de 1999, España exigió a todas las empresas que contaran con protocolos de seguridad y que nombraran a un responsable de seguridad, y que realizaran auditorías bianuales de seguridad, encriptaran datos sensibles cuando se transmitieran a través de redes de comunicaciones e identificaran los incidentes de seguridad. Dichas medidas fueron posteriormente reforzadas en 2007 cuando las nuevas normas exigieron a los fabricantes de *software* que empleasen "medidas de privacidad desde el diseño", con la imposición por la AEPD de fuertes multas a los incumplidores.

232. Por todas estas razones históricas, la AEPD ha contribuido decisivamente a garantizar la integridad y seguridad de la red de comunicaciones, y ha ido mucho más allá de asegurarse de que se cumplían las obligaciones en materia de tratamiento de datos y privacidad electrónica (período de conservación de datos de tráfico, *cookies*, etc.).

233. Por lo tanto, el efecto directo del RGDP en España y su estricto régimen de aplicación, así como las multas administrativas, son importantes factores de reducción de riesgos ya en vigor.

12.5.3. La posición inicial de la AEPD sobre el 5G

234. No es sorprendente, dado el papel proactivo de la Protección de Datos española (AEPD) en seguridad IT, que el 13 de mayo de 2020 difundiera la nota “Introducción a las tecnologías 5G y sus riesgos para la privacidad”[53].

235. En su nota, la AEPD pide:

[53] *Vid*. https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-recomendaciones-5G.

- Criterios homogéneos de seguridad IT para todos los participantes en las redes 5G, basados en un análisis de riesgos EIPD, como exige el RGDP.

- Auditoría independiente de servicios y mecanismos de certificación de infraestructuras.

- El uso de cifrado de extremo a extremo en el modelo de cómputo en la periferia (*edge computing*).

12.6. La Directiva sobre infraestructuras críticas

236. España traspuso la Directiva de infraestructuras críticas de 2008[54] mediante la ley 8/2011, de 28 de abril, relativa a las medidas para la protección de las infraestructuras críticas.

237. La identificación y designación de infraestructuras críticas ("IC") e infraestructuras críticas europeas ("ICE") y su inclusión en el correspondiente Catálogo del Ministerio de Interior es información secreta.

238. Como se indica en la Toolbox, los requisitos establecidos en este instrumento legislativo para identificar las infraestructuras críticas pueden funcionar como una medida de mitigación eficaz.

13. Evaluación del riesgo de interferencia de la República Popular China en Huawei (R5): principios jurídicos clave

239. La Toolbox puede considerarse un conjunto de recomendaciones acordadas en común por los Estados miembros de la UE sobre cómo ejercer una función preventiva específica: la protección de sus redes nacionales 5G frente a los importantes riesgos de ciberseguridad a los que estarán expuestas, dadas las complejas características técnicas de la nueva tecnología 5G y las funciones y servicios críticos que se basarán en el 5G y, en particular, en el "Internet de las cosas" (IoT).

240. Así pues, la Toolbox es esencialmente un documento técnico preparado por expertos y autoridades nacionales que se ocupan de una categoría específica de riesgos críticos -los riesgos de ciberseguridad de las futuras redes 5G- y podría por tanto compararse con otros conjuntos potenciales de recomendaciones relacionadas con riesgos, como las preparadas, hipotéticamente, por grupos de cooperación de:

- Autoridades sanitarias sobre prevención de pandemias;

- Autoridades del sector energético sobre cómo lograr la seguridad del suministro energético; o

[54] Directiva 2008/114/CE, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

- Las fuerzas de policía, los servicios de inteligencia y las fuerzas nacionales de seguridad nacional sobre prevención de ataques terroristas.

13.1. La Toolbox y el "Estado preventivo"

241. Como muestran las comparaciones anteriores, la Toolbox puede ser considerada como un ejemplo de lo que el jurista estadounidense Allan Dershowitz ha descrito como el tránsito hacia el "Estado preventivo", es decir, la adopción por las autoridades públicas de medidas *ex ante* destinadas a prevenir posibles conductas nocivas, particularmente aquellas con potenciales efectos devastadores. En 2006 escribió:[55]

> "*El mundo democrático está experimentando un cambio fundamental en su forma de controlar las conductas nocivas. Estamos dejando de confiar en nuestro tradicional enfoque disuasorio y reactivo y moviéndonos hacia enfoques más preventivos y proactivos. Este cambio tiene enormes consecuencias para las libertades civiles, los derechos humanos, la justicia penal, la seguridad nacional y la política exterior, y las implicaciones para el Derecho Internacional no están siendo suficientemente tenidas en cuenta. Se trata de un cambio conceptual de prioridades, desde una teoría de la disuasión a una teoría de la prevención, cambio que tiene enormes implicaciones sobre las acciones que una sociedad puede llevar a cabo para controlar el comportamiento humano peligroso, que van desde asesinatos selectivos de terroristas, a ataques preventivos contra armas nucleares y otras armas de destrucción masiva, prevención de la guerra, técnicas proactivas de prevención del crimen (operaciones encubiertas, informantes, escuchas telefónicas), métodos psiquiátricos o químicos de prevención de la depredación sexual, técnicas de perfilado ("profiling") basados en la raza, etnia u otras características, inoculación o cuarentena en casos de enfermedades infecciosas (ya sean transmitida de manera "natural" o inoculadas como armas), censura previa de discursos peligrosos u ofensivos, o, en fin, al uso de la tortura (u otras medidas extraordinarias) como medio de conseguir la información necesaria para prevenir actos inminentes de terrorismo*".

242. Terminó su libro de 2006 con una súplica desesperada:[56]

> "*Necesitamos desesperadamente en el mundo una jurisprudencia coherente y ampliamente aceptada sobre anticipación y prevención, tanto en el ámbito de la defensa propia como en la de los demás. También existe una necesidad apremiante de contar con un órgano neutral u otro mecanismo justo que aplique dicha jurisprudencia. A día de hoy faltan ambos. En ausencia de jurisprudencia y de mecanismos para aplicarla, las decisiones* ad hoc *se convierten en reglas* de facto".

[55] *Cfr*. Dershowitz, A. M. (2006). *Preemption: A Knife That Cuts Both Ways (Issues of Our Time)*, pgs. 2 y 3. W. W. Norton.
[56] *Ibid*. p. 237.

13.2. Los límites de la excepción de “seguridad pública” o “orden público”

243. Como ya se ha indicado, la Toolbox no contiene una sola referencia a las implicaciones jurídicas de la aplicación de algunas de las medidas estratégicas que recomienda, a pesar de que algunas se asemejan a técnicas de “perfilado” (*profiling*), en las que el riesgo se evalúa sobre la base de ciertas características externas del vendedor, con escasa consideración de sus circunstancias particulares.

244. Es innegable que la integridad de las redes 5G será considerado un problema de seguridad pública que afecta al interés nacional, sobre todo a la luz del papel fundamental que desempeñarán en el futuro desarrollo de muchos servicios clave. Pero eso no significa que, como se expresará en breve, las autoridades públicas puedan utilizar la referencia a los riesgos no técnicos de la ciberseguridad como un "conjuro mágico” o "comodín" que les permita adoptar medidas arbitrarias que no sean adecuadas o proporcionales para alcanzar los verdaderos objetivos de ciberseguridad.

245. Existe, sin duda, el riesgo de que el mecanismo de identificación de proveedores de alto riesgo (HRV, por sus siglas en inglés) pueda conducir a la exclusión de determinados proveedores no pertenecientes a la UE (en particular, los proveedores chinos). Esto iría en contra de los principios jurídicos fundamentales que constituyen el núcleo de la legislación de la UE, incluida la libre circulación de bienes y servicios, la libertad de empresa y la prohibición de trato discriminatorio en función de la nacionalidad o la tecnología. El mecanismo HRV puede también infringir las normas de la Organización Mundial del Comercio (OMC) y las obligaciones establecidas en los Tratados Bilaterales de Protección de Inversiones.

246. Cabe recordar que la apertura de los mercados a la competencia fue el objetivo principal de la liberalización de las redes y los servicios de comunicaciones iniciada en 1988, que llevó a la UE a abolir los derechos especiales y exclusivos de uso y suministro de equipos y servicios de telecomunicaciones y a garantizar el derecho de los operadores del sector privado a utilizar, importar, comercializar, conectar, poner en servicio y mantener los equipos de telecomunicaciones que libremente eligieran.

247. Por eso, en los párrafos siguientes trataré de esbozar parte de la “jurisprudencia” que los gobiernos europeos, como el de España, desearían probablemente respetar cuando lleven a cabo la evaluación de los proveedores de 5G en función de los riesgos no técnicos descritos en la Toolbox (más específicamente, el R5).

248. Esa evaluación requiere evaluar un riesgo muy difuso, de carácter político, que puede considerarse relacionado con la "seguridad nacional", lo que plantea la cuestión jurídica de cuánta discrecionalidad debe permitirse a las autoridades en esa evaluación, dado el temor de que bajo el noble manto de la “seguridad nacional” oculten intereses comerciales proteccionistas o intereses políticos estrechos o de que apliquen un enfoque “cautelar” carente de todo sentido de proporcionalidad.

249. Con el fin de analizar qué jurisprudencia existente podría aplicarse *mutatis mutandis* al novedoso ejercicio de evaluación de riesgos de la Toolbox, me basaré en los precedentes en tres ámbitos jurídicos diferentes:

- La adopción de medidas comerciales restrictivas por parte de los miembros de la OMC sobre la base del artículo XXI del GATT.

- La adopción de medidas restrictivas por los Estados miembro de la UE sobre la base del llamado "principio de precaución" en menoscabo de las libertades fundamentales del mercado interior consagradas en los Tratados.

- La jurisprudencia española sobre el ejercicio de poderes discrecionales por las autoridades públicas.

250. Como se demostrará más adelante, un principio común de la jurisprudencia en esos tres ámbitos es que la prevención de riesgos hipotéticos no proporciona a las autoridades "carta blanca" para aplicar restricciones sin limitación, sin respetar los tests de adecuación y proporcionalidad.

13.2.1. La normativa de la OMC y la excepción de seguridad

251. Como han indicado dos destacados especialistas en las normas de la OMC, las medidas que limitan el uso de componentes de un determinado proveedor o país extranjero (como Huawei o China), y no digamos si prohíben totalmente su uso, irían en contra de los principios del GATT de no discriminación (art. I: 1) y trato nacional (art. III: 4), a no ser que resultasen de aplicación las excepciones previstas en los artículos XX (a) ("moral pública") o XXI (b) ("seguridad nacional"), cosa a su juicio muy dudosa[57].

252. Estoy totalmente de acuerdo con su conclusión y, puesto que la aplicabilidad de la excepción del artículo XX me parece impensable, me centraré en la excepción relativa a la "seguridad nacional" del artículo XXI del Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT).

253. Según ese artículo XXI, "no deberá interpretarse ninguna disposición del presente Acuerdo en el sentido de que (b) impida a una parte contratante la adopción de todas las medidas que estime necesarias para la protección de los intereses esenciales de su seguridad" en relación con varias categorías de bienes o materias (es decir, materias fisionables o armas, municiones u otros bienes o materiales utilizados para abastecer a las fuerzas armadas) o medidas "aplicadas en tiempos de guerra o en caso de grave tensión internacional".

254. Hay una larga historia de casos en los que los gobiernos intentaron abusar de este artículo, como cuando en la década de 1970 Suecia, alegando motivos de seguridad nacional, impuso un sistema de cuotas para la importación de calzado, que fue posteriormente retirado.

255. Un ejemplo reciente fue la imposición en 2018 por el Gobierno de los Estados Unidos de contingentes arancelarios a las importaciones de acero y aluminio, una vez más por motivos de seguridad nacional. La UE, China, y muchos otros países se opusieron a la medida y solicitaron el establecimiento de un grupo especial de la OMC para tratar el asunto.

[57] *Vid*. Voland, T., & Petite, M. (2020, 24 marzo). *Cybersecurity measures and WTO Law -Especially regarding the 5G networks*, p. 224. EuZW 2020, 218.

256. Una de las cuestiones jurídicas más relevantes que se plantearon en la controversia fue hasta qué punto la excepción de seguridad era de "aplicación completamente discrecional" (*self-judging*) por el país miembro que invoca su utilización o si, por el contrario, esa invocación es susceptible de control externo (*justiciable*), de forma que su conformidad con las normas del GATT puede ser enjuiciada por un grupo especial de la OMC, como parte del procedimiento de resolución de disputas.

257. Si bien los Estados Unidos alegaron que el artículo XXI es de aplicación discrecional y que su uso no puede ser controlado por ningún grupo especial de la OMC, la Unión Europea se opuso enérgicamente a dicha opinión, como expresó la Declaración de apertura de la Unión Europea:[58]

> "*Queremos subrayar los siguientes tres puntos esenciales siguientes: en primer lugar, que las medidas en cuestión son medidas de salvaguardia. En segundo lugar, que no son verdaderas medidas de seguridad nacional. Tercero, que el artículo XXI es susceptible de ser invocado ante los tribunales".*
>
> *"Las medidas en cuestión no son auténticas medidas de seguridad nacional. No porque lo digamos nosotros, sino que debemos fijarnos en la estructura y el texto de las propias medidas, así como en las declaraciones del Presidente de los Estados Unidos, los departamentos del Gobierno de los Estados Unidos, y altos funcionarios. Todos ellos muestran claramente que un objetivo específico de las medidas es proteger la industria nacional del acero y el aluminio en sentido amplio, como fin en sí mismo. Recientemente, el presidente Trump tuiteó que, "al imponer un arancel del 25% sobre un acero objeto de "dumping", Estados Unidos tiene ahora una "industria grande y en crecimiento", lo que resulta importante, por ejemplo, para ayudar a la industria estadounidense de la automoción. También tuiteó que la industria siderúrgica ahora ha "revivido", que se crearán muchos puestos de trabajo y que eso producirá "billones" para el Tesoro de los Estados Unidos. Las medidas en cuestión entienden el término "seguridad nacional" como "definido con amplitud, de forma que incluye la economía, el impacto en el empleo y una gran variedad de asuntos*".

258. Aunque este caso está pendiente de resolución, el 5 de abril de 2019 otro grupo especial de la OMC se pronunció sobre las restricciones excepcionales de tránsito impuestas en 2014 por Rusia contra Ucrania por motivos de seguridad nacional, durante un periodo de tensiones políticas entre los dos países[59].

259. El grupo especial consideró que los grupos especiales de la OMC tienen competencia para examinar ciertos aspectos de la invocación del artículo XXI por un miembro, que Rusia

[58] *Cfr*. Declaración de apertura de la Unión Europea en el Caso DS548, Estados Unidos – Determinadas medidas relativas a los productos de acero y aluminio, en Ginebra el 4 de noviembre de 2019, disponible en https://trade.ec.europa.eu/doclib/docs/2019/november/tradoc_158427.pdf.

[59] *Cfr*. Caso DS512, Rusia – Medidas que afectan al tráfico en tránsito, disponible en https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds512_e.htm#:~:text=The%20Panel%20found%20that%20WTO,XXI(b)(iii)%20of.

cumplía con os requisitos para invocar el artículo y, por consiguiente, que las prohibiciones y restricciones de tránsito estaban cubiertas por el GATT.

260. El grupo, en particular, resolvió que, si bien la cláusula inicial del artículo XXI (b) permite a un Miembro adoptar las medidas "que considere necesarias" para la protección de sus intereses esenciales de seguridad, esta facultad discrecional se limita a circunstancias que objetivamente "se considere que cumplen los requisitos de alguno de los apartados enumerados en dicha disposición"[60]. El grupo rechazó el argumento jurisdiccional de Rusia de que el artículo XXI es de aplicación totalmente discrecional, y argumentó que "no hay base para considerar que la invocación del artículo XXII (b) del GATT de 1994 es un conjuro (*incantation*) que blinda frente a todo escrutinio a una medida impugnada"[61].

261. El grupo consideró que los "intereses esenciales de seguridad", un concepto evidentemente más restringido que "intereses de seguridad", pueden interpretarse en general como intereses relacionados con las funciones por excelencia del Estado, a saber, la protección de su territorio y su población contra amenazas externas, y el mantenimiento interno del orden público.

262. Los intereses específicos que se consideren directamente pertinentes para la protección de un Estado frente a esas amenazas externas o internas dependerán de la situación particular y de las percepciones del Estado en cuestión, y cabe esperar que varíen con las circunstancias cambiantes. Por dichos motivos, se deja, en general, a cada uno de los Estados miembros que definan lo que consideran que son sus intereses esenciales de seguridad.

263. Sin embargo, esto no significa que un Miembro sea libre para elevar cualquier preocupación a la categoría de "interés esencial de seguridad", sino que la facultad discrecional de un Miembro de calificar preocupaciones específicas como "intereses esenciales de seguridad" se ve limitada por su obligación de interpretar y aplicar de buena fe el artículo XXI (b)(iii) del GATT de 1994. El Grupo recuerda que la obligación de buena fe es un principio general del derecho y un principio del derecho internacional general en el que se basan todos los tratados (…) La obligación de buena fe exige que los Miembros no utilicen las excepciones del artículo XXI como un medio para esquivar sus obligaciones conforme al GATT de 1994. Un ejemplo evidente de ello sería que un Miembro pretendiera liberarse de la estructura de "acuerdos recíprocos y mutuamente ventajosos" que constituye el sistema de comercio multilateral simplemente aplicando a los intereses comerciales que había acordado proteger y promover dentro del sistema la etiqueta de "intereses esenciales de seguridad", para así dejarlos fuera del alcance de ese sistema".

264. En la práctica, la decisión del grupo especial implica que -si dejamos a un lado los materiales nucleares (es decir, el inciso i del artículo XXI b) y suministros militares (inciso ii))-, la excepción de seguridad nacional sólo puede invocarse en situaciones de emergencia en las relaciones internacionales o durante una guerra (inciso iii)".

[60] Párrafo 7.101.
[61] Párrafo 7.100.

13.2.2. Las pruebas de "idoneidad" y "proporcionalidad" de la UE

265. La posibilidad de que las autoridades adopten medidas restrictivas excepcionales para prevenir riesgos potencialmente catastróficos, incluso cuando siga habiendo cierto grado de incertidumbre en cuanto al alcance y prueba de tales riesgos, fue prevista por primera vez en Alemania en 1968 en su "Ley sobre la contaminación atmosférica"[62]. Ese *Vorsorgeprinzip* ("principio de precaución") se estableció posteriormente en 1987 en la Declaración Ministerial de Londres de la Segunda Conferencia Internacional sobre Protección del Mar del Norte y, por último, en 1992, se consagró en dos textos importantes:

- La Declaración de Río sobre el Medio Ambiente y el Desarrollo, a tenor de la cual "cuando existan amenazas de daños graves o irreversibles, la falta de plena certeza científica no se utilizará como razón para aplazar medidas eficientes (*cost-effective*) para prevenir la degradación ambiental"[63].

- El Tratado de Maastricht incluyó en el Tratado de la Unión los principios de que la política comunitaria en materia de medio ambiente se basará en el principio de precaución y en los principios de que deben tomarse medidas preventivas, que los daños al medio ambiente deben corregirse primordialmente en su fuente y que quien contamina, paga. Al elaborar su política medioambiental, la Unión tendrá en cuenta los datos científicos y técnicos disponibles (…) los beneficios y costes que puedan resultar de la acción o falta de acción (…)"[64].

266. Merece la pena señalar que el Tratado de Maastricht, al tiempo que consagró el principio de prevención en materia de política medioambiental, incluyó también en el Tratado otro principio importante:

> "*Los Estados miembros y la Unión actuarán respetando el principio de una economía de mercado abierta y de libre competencia, favoreciendo una eficiente asignación de recursos*"[65].

267. En la Unión Europea, el "principio de precaución", nacido originalmente como parte de su política medioambiental, ha ampliado posteriormente su alcance y se ha convertido en un principio jurídico más general, aplicable a las medidas políticas adoptadas para prevenir un riesgo potencialmente catastrófico (por ejemplo, intoxicación alimentaria) cuando no hay pruebas concluyentes de la existencia o gravedad del peligro potencial.

268. Esto se puso de manifiesto en 1996 cuando la Comisión Europea decidió prohibir las exportaciones de carne de vacuno del Reino Unido para reducir el riesgo de transmisión de la enfermedad de las "vacas locas" y el Reino Unido impugnó dicha medida. En su resolución

---

[62] *Vid*. 1974 *Bundesinmissionsschutsgesetz*, art. 5.2. "Las instalaciones sujetas a autorización se construirán y explotarán de manera que… se tomen precauciones contra los efectos ambientales perjudiciales".

[63] *Cfr*. Declaración de Rio sobre el Medio Ambiente y el Desarrollo (1992, 14 junio), Principio 15. Disponible en https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_CONF.151_26_Vol.I_Declaration.pdf.

[64] Actualmente, Artículo 191.2 del TFUE.

[65] Actualmente, Artículo 120 del TFUE.

de 1998[66], el Tribunal de Justicia de las Comunidades Europeas sostuvo que "cuando hay dudas sobre la existencia o alcance de los riesgos para la salud de las personas, las Instituciones pueden adoptar medidas de protección sin tener que esperar a que se demuestre plenamente la realidad y gravedad de tales riesgos (…) Corrobora este punto de vista el apartado 1 del artículo 130 R del Tratado CE, según el cual la protección de la salud de las personas forma parte de los objetivos de política de la Comunidad en el ámbito del medio ambiente. El apartado 2 de ese mismo artículo establece que dicha política, que tendrá como objetivo alcanzar un nivel de protección elevado, se basará, entre otros, en los principios de precaución y acción preventiva, y que las exigencias de la protección del medio ambiente deberán integrarse en la definición y la realización de las demás políticas de la Comunidad."

269. Poco después, el Consejo instó a la Comisión a "seguir en el futuro, con mayor determinación aún, el principio precaución en la preparación de propuestas legislativas y en sus demás actividades relacionadas con la política de los consumidores, y definir con carácter prioritario orientaciones claras y eficaces para la aplicación de este principio", lo que llevó a la Comisión a preparar en 2000 una completa "Comunicación de la Comisión sobre el principio de precaución"[67].

270. En la Comunicación, la Comisión argumentó que, si bien el principio de precaución se menciona en el Tratado únicamente en relación con el medio ambiente, "en la práctica, su ámbito de aplicación es mucho más vasto, y especialmente cuando la evaluación científica preliminar objetiva indica que hay motivos razonables para temer que los efectos potencialmente peligrosos para el medio ambiente y la salud humana, animal o vegetal puedan ser incompatibles con el alto nivel de protección elegido para la Comunidad. La Comisión considera que la Comunidad, al igual que otros miembros de la OMC, tiene derecho a establecer el nivel de protección que considere adecuado, en particular en lo que se refiere al medio ambiente y la salud humana, animal o vegetal. La aplicación del principio de precaución constituye un principio esencial de su política, y las decisiones que adopte a este fino seguirán afectando a las posiciones que defiende internacionalmente sobre cómo debe ser la aplicación de este principio."

271. Pero en la parte más directamente relevante a efectos del presente Dictamen, la Comisión reconoció que, cuando se considerara necesario adoptar medidas, las medidas basadas en el principio de precaución deberían ser, entre otras cosas:

- proporcionales al nivel de protección elegido;
- no discriminatorias en su aplicación;
- basadas en el examen de los posibles beneficios y costes de la acción o falta de acción (incluido un análisis económico coste/beneficio, cuando resulte apropiado conveniente y viable).

272. Para la Comisión:

[66] *Cfr*. Sentencia de 5 de mayo de 1998, casos C-157/96 y C-180/96.
[67] *Vid*. Comunicación [COM(2000) 1 final] sobre el recurso al principio de precaución (2000, 2 febrero).

- "Proporcionalidad significa adaptar las medidas al nivel de protección elegido. La reducción del riesgo hasta el nivel cero raramente es posible, pero una evaluación incompleta del riesgo puede reducir el abanico de opciones posibles para los gestores del riesgo. La prohibición total puede no ser siempre una respuesta proporcionada a un posible riesgo, pero en algunos es la única respuesta posible ante un riesgo dado."

- "No discriminación significa que las situaciones similares no deben tratarse de forma diferente, y que las situaciones diferentes no deben tratarse del mismo modo, a menos que haya razones objetivas para hacerlo."

- "Examinar los costes y los beneficios supone comparar el coste global para la Comunidad de la acción y de la inacción, tanto a corto como a largo plazo, lo que no se limita sencillamente a un análisis económico de rentabilidad, sino que abarca un ámbito mucho más amplio e incluye consideraciones no económicas, como la eficacia de las posibles opciones y su aceptabilidad para la población. Al llevar a cabo tal examen, deberá tenerse en cuenta el principio general y la jurisprudencia del Tribunal de que la protección de la salud tiene prioridad sobre las consideraciones económicas."

273. El TJCE tuvo la oportunidad de pronunciarse sobre la aplicación práctica del principio de precaución en 2003, en un asunto relativo a algunas restricciones comerciales:[68]

> "*Si no se quiere menoscabar la doble finalidad del Reglamento No. 258/97, consistente en garantizar, por una parte, el funcionamiento del mercado interior de los nuevos alimentos y, por otra parte, la protección de la salud pública frente a los riesgos que pueden generar, las medidas de protección que se adopten en virtud de la cláusula de salvaguardia no pueden basarse en una concepción del riesgo puramente hipotética, fundada en meras suposiciones aún no verificadas científicamente.*
>
> *Tales medidas de protección, pese a su carácter provisional y preventivo, sólo pueden adoptarse sobre la base de una evaluación de los riesgos lo más completa posible, dadas las circunstancias concretas, que indique que tales medidas son necesarias a fin de asegurar que los nuevos alimentos no suponen un peligro para los consumidores, conforme al primer guion del artículo 3(1) del Reglamento 258/97*".

274. Incluso aunque no esté directamente relacionado con el "principio de precaución" como tal, existe también abundante jurisprudencia del Tribunal de Justicia Europeo que aborda cuestiones similares e identifica las pruebas que debe superar cualquier medida restrictiva pública que, al tiempo que invoca el orden público, la seguridad nacional u otros objetivos públicos, choque con las libertades fundamentales consagradas en los Tratados de la UE.

[68] *Cfr*. Sentencia de septiembre de 2003, caso C-236/01 sobre el Reglamento (CE) n.º 258/97 del Parlamento Europeo y del Consejo, de 27 de enero de 1997, sobre nuevos alimentos y nuevos ingredientes alimentarios, párrafos 106 y 107.

275. Así, por ejemplo, en *Scientology*, el Tribunal abordó los límites aplicables al principio de "orden público" o "seguridad pública" y declaró:[69]

> "*En primer lugar, aunque los Estados miembro gozan, en principio, de libertad para definir las exigencias del orden público y de la seguridad pública a la luz de sus necesidades nacionales, dichas razones deben, en el contexto comunitario y, en particular, como excepciones al principio fundamental de libre circulación de capitales, interpretarse de forma restrictiva, de manera que cada Estado miembro no pueda determinar unilateralmente su alcance sin control por parte de las Instituciones de la Comunidad (…)*
>
> *Así pues, el orden público y la seguridad pública sólo pueden invocarse en caso de que exista una amenaza real y suficientemente grave que afecte a un interés fundamental de la sociedad (…). Además, esas excepciones no se pueden desnaturalizar y aplicarse, en realidad, con fines puramente económicos.*
>
> *En segundo lugar, procede señalar que las medidas restrictivas de la libre circulación de capitales sólo pueden estar justificadas por razones de orden público o de seguridad pública si son necesarias para la protección de los intereses que pretenden garantizar y sólo si dichos objetivos no pueden alcanzarse con medidas menos restrictivas*."

276. De manera similar, al determinar si las medidas nacionales restrictivas eran coherentes con el principio de libre comercio dentro del mercado interior de la UE, consagrado en el Tratado de la UE (en particular, el artículo 34 del TFUE sobre la libre circulación de mercancías), el Tribunal ha precisado que deben ser tanto "apropiadas" (es decir, bien diseñadas, de forma que sean capaces de alcanzar los objetivos perseguidos) como "proporcionales" (es decir, no deben existir medidas menos restrictivas que logren el mismo objetivo).

277. Así, por ejemplo, en el famoso asunto *Scotch Whisky Association* relativo a si el establecimiento de un precio mínimo de venta del alcohol en Escocia con el fin de proteger la vida y la salud humanas era coherente con la libre circulación de bienes, el Tribunal señaló:[70]

> "*Una medida restrictiva como la prevista en la normativa nacional objeto de la disputa debe respetar la jurisprudencia del Tribunal sobre proporcionalidad, es decir, debe ser adecuada para garantizar el cumplimiento del objetivo perseguido y no ir más allá de lo necesario para alcanzarlo*."
>
> "*Una medida fiscal que incrementa la tributación de las bebidas alcohólicas puede ser menos restrictiva del comercio de estos productos en el seno de la Unión que una medida que fija un precio mínimo por unidad (PMU)*."

[69] *Cfr*. Sentencia del Tribunal de Justicia de la Unión Europea de 14 de marzo de 2000, *Association Eglise de Scientologie de Paris* y *Scientology International Reserves Trust* contra *Premier ministre*, Caso C-54/99, párrafos 17 y 18.
[70] *Cfr*. Caso C-333/14 de 23 de diciembre de 2015, párrafos 28, 46 y 49.

"*Corresponde al órgano jurisdiccional remitente, que es el único que dispone de todos los elementos de hecho y de Derecho en juego en la disputa, determinar si una medida distinta de la prevista por la normativa nacional objeto de controversia, como una mayor tributación de las bebidas alcohólicas, puede proteger la salud y la vida de las personas tan eficazmente como esa normativa, y, al mismo tiempo, ser menos restrictiva del comercio de estos productos en el seno de la Unión*."

278. Del mismo modo, en el asunto Monsanto – sobre si Italia podía bloquear por motivos de salud, en virtud del Reglamento 258/97, la importación de alimentos genéticamente modificados-, el Tribunal afirmó:[71]

"*Las medidas de protección que se adopten en virtud de la cláusula de salvaguardia no pueden basarse en una concepción del riesgo puramente hipotética, fundada en meras suposiciones aún no verificadas científicamente. Tales medidas de protección, pese a su carácter provisional y preventivo, sólo pueden adoptarse sobre la base de una evaluación de los riesgos lo más completa posible, dadas las circunstancias concretas del caso de que se trate, que demuestre que dichas medidas son necesarias para garantizar, conforme al artículo 3, apartado 1, primer guión, del Reglamento n. 258/97, que los nuevos alimentos no presentan riesgo alguno para el consumidor, con arreglo al artículo 3, apartado 1, primer guión, del Reglamento no 258/97*".

13.2.3. Principios jurídicos españoles

279. El artículo 38 de la Constitución española reconoce la libertad de empresa en el marco de la economía de mercado. Asimismo, establece que los poderes públicos garantizarán y protegerán su ejercicio y la defensa de la productividad de acuerdo con las exigencias de la economía general y, en su caso, de la planificación.

280. La jurisprudencia del Tribunal Constitucional y del Tribunal Supremo españoles ha prestado atención a los límites de las facultades discrecionales administrativas cuando discriminan a personas en situaciones similares y ha establecido una clara distinción entre "arbitrariedad" y "poderes discrecionales", que en su sentencia de 21 de noviembre de 1985 el Tribunal Supremo declaró conceptos opuestos.[72] Esta jurisprudencia constante ha sido confirmada recientemente por el Tribunal Constitucional en su STC91/2019 que, de conformidad con la jurisprudencia del TJCE, se refiere a los tests de "adecuación" y "proporcionalidad"[73].

"*Para que un [trato diferente] resulte constitucionalmente lícito no basta con que lo sea el fin que con ella se persigue, sino que es indispensable además que las consecuencias jurídicas que resultan de tal distinción sean <u>adecuadas</u> y <u>proporcionadas</u> a dicho fin, de manera que la relación entre la medida adoptada, el resultado que se produce y el fin pretendido por el legislador superen un juicio de*

[71] *Cfr*. Caso C-236/01 de 9 de septiembre de 2003, párrafos 106 y 107.
[72] Un análisis detallado de esta jurisprudencia se encuentra en la obra de Fernández, T. R. (2016). *Arbitrario, arbitraire, arbitrary. Pasado y presente de un adjetivo imprescindible en el discurso jurídico*. Iustel.
[73] *Vid*. STC 91/2019, FJ 4.

proporcionalidad en sede constitucional, evitando resultados especialmente gravosos o desmedidos".

281. Ya en el ámbito específico de las telecomunicaciones, el artículo 34.3 de la Ley 9/2014 establece:

> "*La normativa elaborada por las administraciones públicas que afecte al despliegue de las redes públicas de comunicaciones electrónicas y los instrumentos de planificación territorial o urbanística deberán recoger las disposiciones necesarias para impulsar o facilitar el despliegue de infraestructuras de redes de comunicaciones electrónicas en su ámbito territorial, en particular, para garantizar la libre competencia en la instalación de redes y en la prestación de servicios de comunicaciones electrónicas y la disponibilidad de una oferta suficiente de lugares y espacios físicos en los que los operadores decidan ubicar sus infraestructuras*."

282. Además, fiel al principio de libre competencia, el artículo 59.2 dispone:

> "*La prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación se realizará en régimen de libre competencia sin más limitaciones que las establecidas en esta Ley y su normativa de desarrollo.*
>
> *Podrán prestar servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación las personas físicas o jurídicas nacionales de un Estado miembro de la Unión Europea o con otra nacionalidad, cuando, en el segundo caso, así esté previsto en los acuerdos internacionales que vinculen al Reino de España. Para el resto de personas físicas o jurídicas, el Gobierno podrá autorizar excepciones de carácter general o particular a la regla anterior.*
>
> *Mediante real decreto se establecerán los requisitos exigibles para el ejercicio de la actividad consistente en la prestación a terceros de servicios de instalación o mantenimiento de equipos o sistemas de telecomunicación relativos a la capacidad técnica y a la cualificación profesional para el ejercicio de la actividad, medios técnicos y cobertura mínima del seguro, aval o de cualquier otra garantía financiera. Los requisitos de acceso a la actividad y su ejercicio serán proporcionados, no discriminatorios, transparentes y objetivos, y estarán clara y directamente vinculados al interés general concreto que los justifique*".

283. Por último, en la medida en que Huawei opera en España a través de su filial Huawei España, cabe mencionar el Acuerdo Bilateral de Promoción y Protección de Inversiones en vigor entre España y China, de 14 de noviembre de 2005[74]. Este Acuerdo prevé protección y seguridad permanentes para las inversiones recíprocas, así como la prohibición de medidas injustas o discriminatorias y la competencia de un tribunal arbitral de inversiones en caso de conflicto entre un Estado y un inversor de la otra parte. En ese mismo sentido, existe también un convenio entre España y China sobre el desarrollo de la cooperación económica e industrial, de fecha 15 de noviembre de 1984[75].

[74] Publicado en el Boletín Oficial del Estado el 8 de julio de 2008.

[75] Publicado en el Boletín Oficial del Estado los días 9 de febrero y 17 de septiembre de 1985.

13.3. Conclusiones

284. El breve análisis realizado anteriormente de las normas y jurisprudencia de la OMC, de la Unión Europea y españolas sobre la adopción de medidas públicas restrictivas para proteger los intereses nacionales, de la Administración Pública o de los ciudadanos contra riesgos potenciales revela con claridad que las autoridades públicas:

- No pueden actuar sobre la base de meras suposiciones, sino que deben hacerlo sobre la base de una evaluación adecuada del riesgo que tenga en cuenta las circunstancias específicas de cada caso (incluidas las medidas ya en vigor para mitigar los riesgos y el coste potencial de la medida restrictiva);

- No pueden adoptar medidas restrictivas que no sean adecuadas para alcanzar el objetivo que supuestamente persiguen ("test de idoneidad");

- No pueden adoptar medidas más restrictivas que otras que logren los objetivos públicos con la misma o mayor eficacia ("test de proporcionalidad").

14. Evaluación del riesgo de interferencia de la RPC en Huawei (R5): cuestiones clave

285. Tras haber establecido en la sección anterior los dos tests jurídicos que debe superar cualquier medida restrictiva resultante de la aplicación de la Toolbox –como sería la declaración de un proveedor como de alto riesgo (High Risk Vendor o HRV) debido al temor de que el Estado de un tercer país interfiera en sus actividades (es decir, del riesgo que la Toolbox denomina "R5"), llega ahora el momento de analizar si, a la luz de las circunstancias concretas de Huawei, podría estar justificado que se le declare HRV.

14.1. El riesgo de interferencia política china en Huawei

286. Como se ha explicado anteriormente, de acuerdo con la evaluación coordinada de riesgos de la UE y con la Toolbox, los indicios de potencial interferencia por parte un país no perteneciente a la UE en un proveedor 5G (como China en Huawei) son un "vínculo fuerte" entre el proveedor y el Gobierno y el país, así como la estructura de la propiedad de la compañía y la legislación de dicho tercer país.

287. Por lo tanto, en lo que sigue se analizarán las siguientes cuestiones:

- ¿Es Huawei de propiedad estatal?

- ¿Está Huawei controlado por el Estado?

- ¿Podrían las leyes de seguridad chinas desplegar efectos extraterritoriales ilegales sobre las actividades de Huawei?

14.1.1. ¿Es Huawei de propiedad estatal?

288. Huawei afirma ser, como se ha indicado anteriormente, una "empresa privada propiedad al 100 % de sus empleados" (más de 100.000, que poseen sus acciones a través del "Sindicato"). Su Esquema de Acciones para Empleados (ESOP) "alinea de manera efectiva la contribución y el desarrollo del empleado con el desarrollo a largo plazo de la compañía".

289. Huawei insiste, más específicamente, en que:

- "No es una empresa de propiedad estatal. A diferencia de las empresas de propiedad estatal, ninguna agencia gubernamental ni organización externa, incluido el Partido Comunista de China, participa en la toma de decisiones o en las actividades comerciales de Huawei".

- "Huawei adopta un sistema empresarial moderno. La Junta de Accionistas es el órgano de mayor autoridad de la compañía. El Consejo de Administración es el órgano de toma de decisiones estratégicas, operativas y de gestión de la compañía. El Consejo de Supervisión supervisa el cumplimiento de las responsabilidades de los miembros del Consejo de Administración y la alta dirección, así como la estandarización de las operaciones del Consejo".

- El Artículo 19 del Capítulo I de la Ley de sociedades de la RPC establece:

  "*En una sociedad, se establecerá una organización del Partido Comunista de China para que lleve a cabo las actividades del partido de conformidad con la Carta del Partido Comunista de China. La sociedad proporcionará las condiciones necesarias para las actividades de la organización del partido".*

  Según la información a disposición pública, todas las empresas chinas y de capital extranjero han establecido organizaciones del PCC según lo estipulado en la Ley de sociedades, como por ejemplo Huawei, Walmart China, Nokia Shanghai Bell China Co., Ltd., y SAIC General Motors Corporation Limited.

  La organización del PCC de Huawei no participa en ninguna de las actividades comerciales de Huawei".

- "Las preferencias políticas de los empleados son irrelevantes para las operaciones comerciales de Huawei. La decisión de un empleado de unirse al Partido Comunista de China (PCC) es un asunto privado. Las operaciones comerciales de Huawei no tienen nada que ver con las actividades políticas del PCC."

290. Algunos autores han expresado su desacuerdo con esa afirmación oficial de Huawei de que es una empresa privada propiedad de sus empleados, y sugieren que, de hecho, es de propiedad estatal. Argumentan que:[76]

[76] *Cfr*. Balding, C., & Clarke, D. (2019, 17 abril). *Who Owns Huawei?* SSRN. https://ssrn.com/abstract=3372669 o http://dx.doi.org/10.2139/ssrn.3372669. Tim Rühlig expresa opiniones similares en https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf.

- *"Huawei Tech es una sociedad de responsabilidad limitada de un solo accionista (una de las dos formas corporativas básicas de conformidad con el derecho de sociedades de China) y es propiedad al 100 % de Huawei Holding, que a su vez cuenta con solo dos accionistas: Ren Zhengfei, el fundador, con casi el 1,14 %, y una entidad llamada Huawei Investment & Holding Company Trade Union Committee ("Huawei Holding TUC"), con el resto."*

- *"Los empleados del grupo Huawei no poseen acciones reales ni de Huawei Tech ni de Huawei Holding, sino que poseen, en virtud de contrato, un tipo de acción virtual que les permite participar en los beneficios. Pero esta acción virtual es un derecho contractual y no un derecho de propiedad; no otorga al titular poder de voto ni en Huawei Tech ni en Huawei Holding, no puede ser transferida y se cancela cuando el empleado abandona la empresa, sujeto a un pago de reembolso de Huawei Holding TUC a un precio fijo bajo. En la actualidad, esta propiedad virtual de acciones no tiene nada que ver con la financiación o el control, sino que es un plan de incentivos de participación en los beneficios".*

- *"Dado que Huawei Holding TUC es la única entidad (distinta a Ren Zhengfei) que posee acciones de Huawei Holding -el único propietario de Huawei Tech-, la clave para entender la propiedad del grupo de Huawei radica en entender Huawei Holding TUC. Esto es difícil de hacer".*

- *"El panorama del modelo de gobernanza corporativa se complica aún más por el hecho de que con arreglo a derecho –y habitualmente por la vía del hecho-, los responsables del Sindicato –aquellos que deciden lo que hará el Sindicato con sus activos, por ejemplo- deben lealtad y son responsables ante las organizaciones sindicales superiores, en cuya cúspide está la Federación Nacional Sindical China (ACFTU) a nivel central. El Partido Comunista controla la ACFTU, cuyo director es miembro del buró político de aquel. El aparato del Partido controla las organizaciones sindicales a todos los niveles administrativos y las organizaciones sindicales son órganos gubernamentales de facto. Los responsables del Sindicato que están por encima del nivel del sindicato de la compañía, aunque no sean técnicamente funcionarios públicos, son tratados como empleados estatales, sujetos a las mismas normas administrativas y escalafón salarial, y sus salarios son pagados con el Tesoro estatal. En resumen, la ACFTU no es un simple sindicato, sino que está organizada, tanto legalmente como en la práctica, como un apéndice del Estado que existe para apoyar y ejecutar directivas de políticas estatales".*

- *"Por lo tanto, si Huawei Holding es propiedad al 99 % de un sindicato de tipo chino que opera de la manera en que se supone que operan los sindicatos en China es, en un sentido no banal, propiedad del Estado".*

- *"Por último, cabe señalar que es indiscutible que, sea cual sea la decisión de los directores de Huawei Tech o Huawei Holding, Ren Zhengfei tiene un veto. Esto fue declarado públicamente por Ren como parte de una campaña de Huawei con medios de comunicación".*

- *"Independientemente de quién sea propietario y controle de forma efectiva Huawei, está claro que los empleados no".*

291. En mi opinión, es obvio que la estructura corporativa de Huawei no es la misma que la de Ericsson y la de Nokia, por mencionar a sus dos principales competidores como proveedores de equipos 5G, que son empresas que cotizan en bolsa en las bolsas de Estocolmo y Helsinki, respectivamente, pero sería exagerado argumentar que Huawei es "efectivamente de propiedad estatal".

292. Aunque la naturaleza jurídica de los derechos de los empleados de Huawei no es meridiana, es legítimo pensar que los empleados son accionistas "indirectos" de Huawei o, al menos, "beneficiarios" (*beneficial owners*) de las acciones de *Huawei Technology* mantenidas en fideicomiso por el *Sindicato de Huawei Investment & Holding Co Ltd*. Esta sociedad jugaría un papel parecido al que en España y otros países tienen las SICAV, instituciones de inversión colectiva en las que sus accionistas pueden controlar a la entidad que gestiona sus inversiones en sociedades cotizadas (aunque en nuestro caso *Huawei Technology* no lo sea). Los derechos de los empleados de Huawei también pueden asimilarse a los que en el mundo anglosajón se conocen como "*depositary receipts*", como los títulos que se negocian en la Bolsa de Nueva York representativos de acciones de empresas extranjeras que cotizan en dicho mercado.

293. Es cierto, desde luego, que la estructura de propiedad de Huawei no es la misma que la de la mayoría de las empresas privadas occidentales, ni de las que cotizan en Bolsa -como Ericcson o Nokia, sus competidoras-, ni de otras grandes empresas propiedad de un número limitado de accionistas significativos (como, por ejemplo, en España, El Corte Inglés o Mercadona).

294. Ahora bien, pueden advertirse grandes similitudes entre Huawei y algunas grandes empresas privadas cooperativas europeas, en las que la mayoría de los empleados (los miembros de la "cooperativa") tienen un interés económico en la empresa y tienen influencia -al menos teórica- sobre las decisiones importantes de las empresas, aunque están muy alejados de las decisiones empresariales cotidianas. Hay, desde luego, una serie de empresas europeas importantes que, a veces desconocidas por el público en general, no son corporaciones, sino cooperativas, como Crédit Agricole, Grupo BPCE o Covea en Francia, BVR o el Grupo REWE en Alemania, Rabo Bank en Holanda o, en España, Cajamar, Cooperativa Mondragón, Mutua Madrileña o Mapfre[77].

295. En suma, puede ser cierto que el derecho que poseen los empleados de Huawei no sea jurídicamente idéntico al concepto occidental de "acción", y no es preciso que este Dictamen indague en profundidad sobre esa cuestión. Pero resulta obvio que tales derechos tienen un estrecho parecido con los títulos de participación en ciertas instituciones de inversión colectiva (como las SICAV) y con los "recibos de acciones" (*depositary receipts*). Y que todo ello hace que, al ser tales derechos propiedad de los empleados de Huawei, la estructura de propiedad de Huawei se asemeje bastante a la de las grandes sociedades cooperativas europeas. Es cierto que Huawei no es una sociedad cotizada al uso occidental

[77] *Vid*. para más detalles *World Cooperative Monitor 2019*. (2020, 12 marzo). Euricse. https://www.euricse.eu/publications/world-cooperative-monitor-2019/.

(y, como se señaló más arriba, la propia Huawei señala que eso le permite dedicar muchos más recursos a I+D, al no ser esclava de objetivos de beneficio a corto plazo). Pero ello no implica, en absoluto, que sea "propiedad del Estado chino".

296. Pero aunque no sea de propiedad estatal, ¿hay indicios de que Huawei está "controlada por el Estado"? Esta es la cuestión a la que nos referimos ahora.

14.1.2. ¿Está Huawei controlada por el Estado?

297. Huawei reconoce que algunos de sus empleados y directivos pueden ser miembros del PCC, pero que eso no tiene ninguna relación con quién controla la compañía o cómo se dirige esta. Específicamente sostiene que:[78]

- Huawei cumple con el artículo 19 del Capítulo I de la Ley de sociedades de China que, como se ha señalado anteriormente, establece que "En una sociedad, se establecerá una organización del Partido Comunista de China para que lleve a cabo las actividades del partido de conformidad con la Carta del Partido Comunista de China. La sociedad proporcionará las condiciones necesarias para las actividades de la organización del partido". Esta disposición es seguida no sólo por Huawei, sino también por todas las demás empresas establecidas en China, incluyendo las subsidiarias de empresas estadounidenses como, por ejemplo, Walmart, Motorola, o General Motors. La organización del PCC de Huawei no participa en ninguna de las actividades comerciales de Huawei. Además, Huawei nunca ha establecido ninguna organización del PCC fuera de China.

- "El hecho de que el Sr. Ren Zhengfei, otros ejecutivos de Huawei u otros empleados sean miembros del PCC no afecta la toma de decisiones ni a las operaciones de Huawei". "La decisión de un empleado de unirse al PCC es un asunto privado".

- "Huawei cuenta con una estructura de gobierno sólida y efectiva que garantiza su operación y gestión independientes, lo que significa que ninguna organización externa controla a Huawei. Los empleados que cuentan con acciones eligen la Comisión de Representantes (Comisión) sobre la base de un voto por acción. La Comisión, junto con el Consejo de Administración y el Consejo de Supervisión, que son elegidos por la Comisión, deciden sobre y gestionan la empresa principal".

- "Huawei cuenta con 96.768 empleados que son parte de su accionariado activo, de los cuales 86.514 empleados con derecho de voto eligieron 115 representantes empleados (por periodo de 5 años). El comité de representantes de los empleados del accionariado elige al presidente y otros 16 directores, y el consejo de administración elige 4 (el vicepresidente y tres directores ejecutivos). El presidente rotatorio cuenta con tres vicepresidentes. El presidente rotatorio dirige el consejo de administración y su comité ejecutivo mientras está en el cargo. El consejo ejerce la autoridad de toma de decisiones para la estrategia corporativa, operaciones y gestión, y es el máximo responsable de la estrategia corporativa, las operaciones, la gestión y la satisfacción del cliente".

[78] *Cfr*. https://www.huawei.com/minisite/who-runs-huawei/en/.

298. Aun cuando, como se ha indicado anteriormente, Huawei no es de propiedad estatal, se ha argumentado que está controlada indirectamente por el Estado o por el PCC, por su influencia y estrechos vínculos con altos directivos y empleados. Se han aducido al respecto dos fuentes de sospechas:

- El antiguo vínculo del Sr. Ren con el Ejército de Liberación del Pueblo (PLA, en su acrónimo en inglés) de China.

- Los vínculos entre empleados de Huawei y la inteligencia china.

299. Se ha argumentado, por ejemplo, que el Sr. Ren fue un oficial de inteligencia de alto rango en el Ejército de Liberación del Pueblo, y que sus contactos tuvieron que ver con la obtención por Huawei de las ayudas gubernamentales para que China superara su dependencia de los equipos de telecomunicaciones extranjeros.

300. Huawei responde que el fundador de Huawei, el Sr. Ren, fue tan solo un militar de baja graduación en el Cuerpo de Ingeniería del Ejército de la RPC, que se retiró en 1983 cuando el ejército redujo significativamente sus efectivos y que no ha tenido relación con el ejército desde entonces. "En 70 años, más de 50 millones de personas han abandonado el ejército chino. Al igual que los veteranos en los Estados Unidos, muchas de estas personas buscan nuevos empleos en el gobierno o en el sector privado". El propio Sr. Ren ha declarado que "Estados Unidos está exagerando mi formación militar porque no tiene pruebas concretas contra Huawei".

301. En cuanto a los vínculos entre los empleados de Huawei con la inteligencia china, el economista estadounidense Christopher Balding "utilizando un conjunto único de datos de CV que se filtraron desde bases de datos y sitios web chinos poco seguros de selección de personal que aparecieron en Internet en 2018", descubrió que "personal técnico clave de nivel medio empleado por Huawei cuenta con antecedentes significativos en trabajos estrechamente vinculados a recopilación de inteligencia y actividades militares" [79].

302. Del análisis de estos CV, el Sr. Balding deduce que "los empleados de Huawei efectivamente confirman la rumoreada relación entre el Estado chino, el ejército, y los servicios de inteligencia de recopilación de información (y) los temores de que [Huawei] tenga vínculos y actúe en concierto con el Estado chino (…) Hay una institucionalización clara en cuya virtud el Estado chino y personal responsable de recopilación de inteligencia se infiltran en Huawei como parte de una organización sistémica concebida para facilitar flujos de información".

303. Huawei responde a esas insinuaciones que "mantiene políticas estrictas para la contratación de candidatos con antecedentes militares o gubernamentales. Durante el proceso de contratación se requiere que estos candidatos presenten documentación que demuestre que han terminado sus relaciones con el ejército o el gobierno".

[79] *Cfr*. Balding, C. (2019, 5 julio). *Huawei Technologies' Links to Chinese State Security Services by Christopher Balding*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726.

304. En mi opinión, existe una larga tradición en el pensamiento occidental, que se remonta al menos a la famosa obra de Adolf Berle y Gardiner Means "*The Modern Corporation & Private Property"* (1932) que reconoció la separación en las empresas industriales modernas entre "propiedad" y "control" y llegó a la conclusión de que tales grandes empresas, en la práctica, no están controladas por sus accionistas, sino por sus gerentes. En las famosas palabras de Berle y Means:[80]

> "*La separación de la propiedad y el control se convierte en casi completa cuando no existe ni siquiera un interés minoritario sustancial, como en la American Telephone and Telegraph Company, cuyo principal accionista se dice que cuenta con menos del 1 % de las acciones de la empresa. Cuando se da esa situación, el control puede ejercerse por los directivos o gerentes, que pueden aprovechar la maquinaria de las delegaciones de voto para convertirse en un órgano que se auto-perpetúa, aunque, como grupo no posean sino una pequeña fracción de las acciones(…) Las empresas donde esta separación se ha convertido en un factor importante pueden clasificarse como cuasi-públicas, en contraste con las sociedades privadas, o sociedades anónimas cerradas, en la que no se ha producido una separación importante de la propiedad y el control*."

305. Unos años después, el economista estadounidense John Kenneth Galbraith confirmó esa misma impresión:[81]

> "*En las últimas décadas se han ido acumulando pruebas del desplazamiento del poder desde los propietarios a los gerentes en las grandes corporaciones modernas. El poder de los accionistas se ha hecho cada vez más débil. Solo una pequeña proporción de las acciones está representada en las Juntas de accionistas, una ceremonia cuya banalidad se combina con su irrelevancia*".

306. En opinión de Galbraith, el poder se ha desplazado a lo que él describió como la "tecnoestructura":[82]

> "*La organización empresarial moderna, o la parte de la misma que tiene que ver con la orientación y la dirección, consiste en numerosas personas que se dedican, en un momento dado, a obtener, digerir, intercambiar y comprobar información. Gran parte del intercambio y comprobación de la información se realiza boca a boca –una conversación en la oficina, a la hora de la comida o por teléfono-. Pero el procedimiento más típico es a través de los comités y las reuniones de comités (…) De esa forma, las decisiones en la empresa moderna no son el producto de individuos, sino de grupos*".

307. Las corporaciones estadounidenses, y particularmente las compañías que cotizan en bolsa, han pasado por una serie de cambios desde que Galbraith escribió esas palabras, como resultado de la fiebre de las fusiones y adquisiciones y las compras apalancadas de los años 80, la revolución desregulatoria y la ola de privatizaciones que comenzaron en el Reino

[80] *Cfr*. Berle, A. A., & Means, G. C. (2006). Property in Transition. En *The Modern Corporation & Private Property* (p. 6). Transaction Publishers.
[81] *Cfr*. Gabraith, J. K. (1967). *The New Industrial State*, p. 65 (2.ª ed.). Penguin Books.
[82] *Ibid.* pgs. 78 y 79.

Unido y Estados Unidos en los años 80, la explosión de las ".com" de finales del siglo XX y el nacimiento, a principios del nuevo siglo, de las nuevas empresas que pronto serían etiquetadas como "*Big Techs*", o el creciente papel del "activismo accionarial", que trajo consigo el poder y la influencia del capital privado y otros inversores institucionales en las grandes empresas cotizadas. Probablemente como resultado de esos factores, el "capitalismo gerencial" (*managerial capitalism*) de las primeras décadas de posguerra fue abandonado gradualmente, como escribieron dos economistas británicos:[83]

> "*Ya en 2002 la idea básica de una gran empresa como institución jerárquica multidivisional que podía ofrecer a sus empleados una carrera de por vida a sus se había desintegrado*".

308. Mi argumento es que Huawei, al ser una empresa que se ha vuelto extremadamente grande, que no cotiza en bolsa y que vende equipos y servicios en todo el mundo, encaja principalmente en el viejo molde del capitalismo gerencial, en el que está al mando una "tecnoestructura" cualificada, y casi exclusivamente china, inspirada por las opiniones estratégicas de uno de sus fundadores, el Sr. Ren, y un complejo sistema de unidades, líneas jerárquicas y comités se ocupa de sus actividades y decisiones empresariales.

309. En tales organizaciones, no es fácil identificar dónde reside el "poder" y el "control", ya que son el resultado de la interacción entre una amplia gama de altos directivos y comités y otros órganos colegiados, sin que ningún individuo tenga un papel decisivo. Este enfoque colectivo lo ilustra bien el peculiar sistema de Huawei de los tres presidentes ejecutivos rotatorios.

310. La cultura corporativa dominante de Huawei parece reflejar lo que el famoso consultor empresarial irlandés Charles Handy describió como una "cultura apolínea" o "cultura de roles", en la que no hay un solo dios "Zeus" que tome las decisiones y domine la organización, sino que las decisiones son el resultado de un proceso de decisión complejo e interactivo -parecido a un templo de Apolo-en el que el poder de los respectivos responsables deriva de sus funciones en la organización, no de su relación personal con "Zeus"[84].

311. El propio fundador de Huawei, Ren Zhengfei, reconoció cómo Huawei replicó la estructura de las grandes empresas estadounidenses:[85]

> "*Una razón importante del éxito hoy de Huawei es que la mayoría de nuestras prácticas de gestión las hemos aprendido de las empresas estadounidenses. Desde que Huawei fue fundada, contratamos a docenas de firmas consultoras estadounidenses para que nos enseñaran cómo gestionar la compañía. Ahora todo nuestro sistema es muy similar al de esas empresas estadounidenses. Así que Estados Unidos debería estar orgulloso*".

---

[83] *Cfr*. Micklethwait, J., & Wooldridge, A. (2003). *The Company. A Short History of a Revolutionary Idea*. Modern Library.

[84] *Cf.* Handy, C. (1978). *Gods Management. The Changing Work of Organisations*. Arrow.

[85] *Cfr*. *Ren Zhenfei and Yuvol Noah Harari at Davos*, entrevista realizada por Zanny Minton Beddoes, jefe de redacción del *The Economist* (2020, 21 enero) en Davos (Suiza). Disponible en https://www.huawei.com/en/facts/voices-of-huawei/davos.

312. Aunque no sea un "Zeus", el Sr. Ren sigue siendo un líder influyente:[86]

> "*Dentro de Huawei, Ren es considerado más como un líder espiritual que como un directivo en la brega. Sus reflexiones a menudo se publican en la web interna de la compañía para que los empleados las lean. Le gustan las metáforas militares y ha comparado sus problemas con Washington con una guerra. 'La gente se levantaba y aplaudía cada vez que entraba en una sala', dijo un británico que trabajaba para la empresa en Shenzhen y hablaba bajo anonimato porque había firmado un acuerdo de confidencialidad. 'La gente paladearía cada una de sus palabras. Era reverenciado por todos. A pesar de no ser el primer ejecutivo o presidente, sus decisiones siempre fueron definitivas*."

313. El propio Sr. Ren ha reconocido que posee un "poder de veto" (algo equivalente a lo que en Europa sería una "*golden share*" o "acción dorada"):

> *"Nuestros Artículos de Gobernanza establecen que el poder de veto puede ser heredado, pero eso no va a suceder en mi familia", dijo Ren. "Todo lo contrario, el poder de veto va a ser ejercido colectivamente por un grupo de élite compuesto por siete miembros electos. Es posible que ninguno de ellos sea miembro de mi familia". Ren dijo que no tenía prisa en renunciar a su poder de veto, teniendo en cuenta las incertidumbres presentes en la economía global debido a los vientos en contra tales como el Brexit. Pero lo que revela de manera destacada es cómo Ren está cada vez más dispuesto a levantar gradualmente el velo sobre su compañía".*

314. Otro ejemplo ilustrativo de su notable influencia puede verse:

- En el envío de cartas a todos los empleados de Huawei, como hizo, por ejemplo, el 27 de diciembre de 2018, con el título "Mejora integral de las capacidades y prácticas de ingeniería de software para construir productos de calidad fiables", donde se esboza el programa de transformación y de cumplimiento de las expectativas del Consejo de Supervisión del Reino Unido.

- En sus recientes esfuerzos por colaborar con la comunidad internacional y representar el punto de vista de Huawei, como hizo, por ejemplo, en su entrevista con *The Economist*[87], cuando ofreció vender todas las patentes de Huawei 5G a cualquier comprador dispuesto a comprarlas por cierta suma y dio a entender que había tenido la idea esa misma mañana (presumiblemente sin consultar previamente con ninguno de los presidentes rotatorios).

315. Visto desde la distancia, se diría que Huawei está controlado no por el Estado chino o el PCC, sino por un grupo bien integrado de altos directivos bajo la inspiración y el liderazgo del "padre fundador" de Huawei, el Sr. Ren. Contrariamente a lo que opinan los críticos de

[86] Pearlstine *et al.* (2019, 10 abril). *The Man behind Huawei*. Los Angeles Times. https://www.latimes.com/projects/la-fi-tn-huawei-5g-trade-war/.
[87] *Vid*. The Economist. (2019, 12 septiembre). *Ren Zhengfei may sell Huawei's 5G technology to a Western buyer*. https://www.economist.com/business/2019/09/12/ren-zhengfei-may-sell-huaweis-5g-technology-to-a-western-buyer.

Huawei, el liderazgo espiritual de Huawei por parte del Sr. Ren, confirma con claridad que la compañía no está controlada por el Estado.

316. Además, como resultado de la naturaleza competitiva de los mercados en los que vende, y de acuerdo con la filosofía empresarial de su fundador, el Sr. Ren, Huawei ha desarrollado una cultura empresarial en la que el "servicio al cliente" es el objetivo primordial.

317. Huawei, que sigue siendo un gran grupo industrial chino con sede en China -aunque ya tenga importantes actividades en el extranjero-, no puede escapar a las características del peculiar sistema capitalista chino, como la presencia de representantes del PCC dentro de sus bases.

318. Estas peculiaridades, inauditas en las corporaciones occidentales modernas, no menoscaban el hecho de que bajo circunstancias normales y previsibles Huawei opera, y operará, como una empresa capitalista, en la que los objetivos comerciales y el éxito en el mercado son, y seguirán siendo, los objetivos primordiales.

319. Como subrayan los directivos de Huawei, la empresa es consciente de que la menor desviación respecto de un enfoque comercial estricto y el mero surgimiento de rumores o indicios de que Huawei se ha plegado a instrucciones políticas de las autoridades gubernamentales chinas-y, no digamos, que ha hecho cosas ilegales y traicionado la confianza de sus clientes (como colocar puertas traseras ilegales o boicotear sus equipos)- constituiría un golpe devastador para sus ambiciones internacionales de convertirse (y permanecer como tal) en líder mundial en este sector.

320. Por último, los argumentos mencionados anteriormente sobre las actividades pasadas del Sr. Ren, hace casi 40 años, o los “vínculos” con la inteligencia china resultantes del análisis de los currículos de los empleados de Huawei son tan alambicados, se apoyan en tan pocas pruebas y tienen tan poco peso legal para demostrar que Huawei está “controlada por el Estado” que no hay necesidad de discutirlas. Si aplicásemos un estándar tan ridículo a las compañías occidentales, especialmente las estadounidenses, probablemente llegaríamos también a la absurda conclusión de que no son privadas, sino que están "controladas por el Estado".

14.1.3. ¿Podrían las leyes de seguridad chinas desplegar efectos extraterritoriales ilegales?

321. La Toolbox de la UE se refiere a la “legislación de un país tercero” como un factor potencial a tener en cuenta al evaluar si un proveedor podría estar sujeto a “interferencia política” por parte del gobierno de su país de origen.

322. La pregunta práctica es, pues, si las leyes chinas relacionadas con el control de las actividades o datos de los ciudadanos o, más ampliamente, las que requieren que todos los operadores del mercado en China cooperen con las autoridades nacionales de inteligencia o de seguridad nacional en la recopilación de información podrían aplicarse a las actividades en el extranjero de Huawei y potencialmente requerir la colocación en sus equipos y programas de dispositivos de espionaje, puertas traseras ilegales, mecanismo de sabotaje o cosas parecidas.

323. A este respecto, he leído las versiones en inglés de las leyes y reglamentos vigentes en la RPC, así como el análisis jurídico de su contenido realizado por tres bufetes de abogados especializados, el despacho EY Chen&Co, Clifford Chance LLP y Simmons & Simmons.

324. Esas leyes son las siguientes:

- La Ley Antiterrorista, aprobada en la 18ª sesión del Comité Permanente del 12º Congreso Nacional del Pueblo, el 27 de diciembre de 2015 (la "Ley Antiterrorista");

- La Ley de Contraespionaje, aprobada en la 11ª sesión del Comité Permanente del 12º Congreso Nacional del Pueblo, el 1 de noviembre de 2014 (la "Ley de Contraespionaje");

- La Ley de Ciberseguridad, aprobada en la 24ª sesión del Comité Permanente del 12º Congreso Nacional del Pueblo, el 7 de noviembre de 2016 (la "Ley de Ciberseguridad");

- La Ley de Inteligencia Nacional, aprobada en la 28ª sesión del Comité Permanente del 12º Congreso Nacional del Pueblo, el 27 de junio de 2017 (la "Ley de Inteligencia Nacional"); y

- La Ley de Seguridad Nacional, aprobada en la 15ª sesión del Comité Permanente del 12º Congreso Nacional del Pueblo, el 1 de julio de 2015 (la "Ley de Seguridad Nacional").

325. Encuentro convincentes las conclusiones de dichos análisis jurídicos de que ninguna de las leyes antes mencionadas:

- Despliega efectos extraterritoriales fuera de China;

- Autoriza a las autoridades chinas a ordenar a los fabricantes de equipos de telecomunicaciones, como Huawei, que instalen puertas traseras (*backdoors*), dispositivos de escucha (*eavesdropping devices*) o programas espía (*spyware*) en los equipos de telecomunicaciones.

326. Dichos análisis jurídicos concluyen que la legislación china no otorga a las autoridades competentes chinas la facultad de obligar a las empresas filiales o asociadas en el extranjero de una empresa china a revelar o proporcionar acceso a los datos almacenados fuera de China. En términos generales, las autoridades chinas encargadas de hacer cumplir la ley no están facultadas para hacer cumplir la legislación china a entidades en extranjeras ni para obligar a éstas a prestarles asistencia, salvo, de forma indirecta, mediante la asistencia judicial prestada en virtud de los tratados bilaterales pertinentes por las autoridades extranjeras responsables de hacer cumplir las leyes.

327. Estas conclusiones son coherentes con la Declaración de los Sres. Jihong Chen y Jianwei Fang, socios de la firma jurídica china Zhong Lun, ante la Comisión Federal de Comunicaciones de los Estados Unidos de fecha 27 de mayo de 2018, en la que afirmaron que:

- *“A menos que se especifique claramente en la norma, el derecho chino por lo general no tiene jurisdicción extraterritorial”.*

- *"China tiene una jurisdicción extraterritorial limitada y solo cuando alguien lleva a cabo actividades terroristas contra ciudadanos o instituciones chinos o comete las actividades terroristas señaladas en los tratados internacionales concertados o en los que ha participado China. Las empresas que fabrican y venden equipos legalmente no están sujetas a jurisdicción extraterritorial del gobierno chino y, por lo tanto, no tienen obligación de asistencia legal.”*

328. Dicha declaración fue acompañada de un memorándum preparado por el bufete Clifford Chance para Huawei, de fecha 11 de diciembre de 2018, en el que se declara:

> “*Hemos pedido a Zhong Lun que desarrolle su afirmación de que “A menos que se especifique claramente en la norma, el derecho chino por lo general no tiene jurisdicción extraterritorial”. Zhonglun ha explicado lo siguiente:*
>
> *(i) Si el legislador de la RPC tuviera la intención de otorgar algún efecto extraterritorial a una disposición jurídica, normalmente utilizaría un lenguaje explícito para indicarlo, y*
>
> (ii) *El Ministerio de Asuntos Exteriores de la RPC ha expresado reiteradamente la objeción general del Gobierno de la RPC a la jurisdicción extraterritorial (“long arm jurisdiction”).*”

329. Huawei adicionalmente me ha explicado que:

- “El Sr. Yang Jiechi, miembro del Comité Central del Partido Comunista de China y Director de la Oficina de la Comisión de Asuntos Exteriores del Comité Central del Partido Comunista de China, declaró oficialmente en febrero de 2019 durante la 55ª Conferencia de Seguridad de Múnich, que el gobierno chino siempre exige a las empresas chinas que cumplan con las normas internacionales y las leyes y reglamentos de los países en los que operan, y que China no tiene ninguna ley que obligue a las empresas a instalar puertas traseras o a recopilar información de inteligencia extranjera”.

- “El Primer Ministro Li Keqiang reiteró este punto en una conferencia de prensa después de una reciente sesión del Congreso Nacional del Pueblo. El 12 de abril de 2019, en la "Cumbre 16+ " en Croacia, el Premier Li dijo repetidamente a todos nuestros empleados que no instalaran puertas traseras en las redes. Esto representa la posición de los líderes del Estado chino en cuanto a puertas traseras, por lo que es imposible para nosotros instalar puertas traseras en nuestros equipos”.

- “Incluso si se nos ordenara, Huawei no instalaría puertas traseras. Si se encontrara una sola puerta trasera en cualquiera de los 170 países en los que operamos, nuestras ventas se reducirían en todos ellos. En ese caso, un gran número de nuestros empleados querría marcharse de la compañía, pero no estarían en condiciones de hacerlo. Tendría deudas que pagar por volumen de decenas de miles de millones de

dólares. Y si no pudieran pagarlas, los acreedores les acosarían a diario. ¿Cómo podrían vivir así? Así que nunca seguiríamos las instrucciones de nadie para instalar puertas traseras. Eso no ocurrirá nunca".

- "Estamos comprometidos con el cumplimiento de todas las leyes y reglamentos aplicables vigentes en la UE. Asumiremos compromisos con los gobiernos locales sobre lo que haremos y no haremos en los países en los que operamos, y seremos auditados al efecto. Esto ayudará a aumentar su confianza en nosotros".

- "El Reino Unido tiene la supervisión más estricta sobre Huawei. Confiamos en el Reino Unido y en Alemania, por lo que estamos abiertos a sus inspecciones. También prestan mucha atención a nuestros problemas y nos critican constructivamente. Este proceso ha contribuido a crear confianza. Nos complace asumir estos compromisos y someternos nosotros mismos a auditorías de acuerdo con los requisitos de gestión de la UE".

- "La seguridad cibernética y la protección de la privacidad son las principales prioridades de Huawei. Estamos dispuestos a firmar con cualquier país acuerdos de rechazo de puertas traseras y de espionaje".

14.1.4. ¿Por qué (solo) Huawei?

330. Huawei ha señalado que la cadena de suministro de todos los fabricantes de equipos 5G (incluidos Ericsson y Nokia) es global, con actividades significativas en China en todos los casos, como consecuencia de lo cual, "gran parte de la infraestructura de Estados Unidos que utiliza [equipos] de Ericsson y Nokia está hecha en China". Además, "si Pekín realmente quiere tener acceso a, digamos, las redes alemanas de telecomunicaciones, las agencias de inteligencia chinas podrían intervenir a través las cadenas de suministro de Ericsson y de Nokia".

331. Más específicamente, según Huawei:

- Ericsson cuenta con 11.000 empleados en China (es decir, alrededor del 11,6% de su plantilla global), de los cuales 5.000 son empleados de I+D. También cuenta con 5 centros de Innovación, incluyendo un centro de innovación 5G. Además, Ericsson posee en Nanjing el mayor centro de fabricación y suministro de sistemas de telecomunicaciones, que incluye 5G.

- Nokia tiene en China más de 16.000 empleados (es decir, alrededor del 15,5% de su plantilla global), con más de 10.000 empleados de I+D. Cuenta con 4 bases de fabricación de sistemas de telecomunicaciones (Dongguan, Shenzhen, Pekín y Suzhou). Nokia China es en parte propiedad del Gobierno de China, su director General es nombrado por el Gobierno de China y su presidente desde julio de 2017, el Sr. Yuan Xi, es también secretario del PCC.

332. Por lo tanto, Huawei sostiene que, en un mundo de cadenas de suministro globales, "la seguridad de los equipos de comunicaciones no depende de su país de origen. La seguridad

de los productos del sistema de comunicaciones deberá garantizarse, por el contrario, mediante estándares de seguridad globales y unificados".

333. Aunque no estoy en condiciones de confirmar las cifras específicas que me ha proporcionado Huawei, si está claro que:

- El Informe Anual de Ericsson 2019 confirma que su cadena de suministro es global y tiene en China centros de fabricación, servicios e I+D[88].

- El Informe Anual de Nokia 2019 confirma que su cadena de suministro es también global y tiene al menos un centro de fabricación en China[89].

334. Así pues, en la medida en que todas las fábricas en China, sea cual sea la empresa, están sujetas a una legislación local similar, no hay ninguna razón obvia que haga que el riesgo de instalación maliciosa de dispositivos ilegales por orden de las autoridades chinas o del PCC no afecte a las instalaciones o subcontratistas locales de empresas no chinas.

335. En realidad, hay buenas razones para pensar que la nacionalidad del proveedor de equipos es un mal indicador de vulnerabilidad frente a potenciales ciberataques malintencionados. De hecho, nada menos que el director del NCSC de Reino Unido declaró recientemente:[90]

> "*En los últimos dos años, el gobierno del Reino Unido, basándose en las conclusiones del NCSC, ha atribuido a Rusia, China, Corea del Norte e Irán actividades cibernéticas maliciosas promovidas por el Estado. También existe una amenaza grave y sostenida de ciberdelincuencia organizada.*
>
> *Estos ataques se han dirigido contra una serie de objetivos de distintos sectores. Sus objetivos han sido diferentes. Los métodos han sido diferentes. La cadena de suministro, y de dónde son los proveedores, es un aspecto, pero no el único. El año pasado, el NCSC atribuyó públicamente algunos ataques a las redes británicas, incluyendo las redes de telecomunicaciones, a Rusia. Por lo que sabemos, esas redes no tenían dispositivos rusos en ellas. Las técnicas que los rusos usaron para atacar a esas redes buscaban debilidades en cómo se diseñaron y cómo se manejaron.*
>
> *No somos ingenuos. En absoluto. En los aproximadamente 1.200 incidentes de ciberseguridad que el NCSC ha gestionado desde que fue creado, el país de origen de los proveedores no ha estado entre los principales motivos de preocupación sobre cómo se llevaron a cabo esos ataques*."

336. En otras palabras, centrarse en la nacionalidad de los proveedores podría ser un claro caso de errar el tiro o, como ha declarado con más elegancia el Comité de Inteligencia y Seguridad

---

[88] *Cfr*. *Ericsson 2019 Annual Report*, p. 17. (2019). https://www.ericsson.com/495c1f/assets/local/investors/documents/2019/ericsson-annual-report-2019-en.pdf.

[89] *Cfr*. *Nokia 2019 Annual Report*, p. 120. (2019).

[90] *Cfr*. Discurso de Ciaran Martin en CyberSec (Bruselas) el 20 de febrero de 2019. Disponible en https://www.ncsc.gov.uk/speech/ciaran-martins-cybersec-speech-brussels.

del Parlamento del Reino Unido, "el "pabellón de origen" de los equipos de telecomunicaciones no es el elemento crítico a la hora de determinar su ciberseguridad"[91].

14.1.5. Conclusiones

337. Mis conclusiones del análisis de las cuestiones examinadas en esta sección pueden resumirse así:

- Aunque China abrazó hace años los principios clave de una economía de mercado, sigue siendo un país comunista, no una democracia occidental, y esto implica que las empresas con sede en China muestran algunas características (como la presencia de representantes del PCC en la empresa) desconocidas en las economías de mercado occidentales.

- Independientemente de ello, no hay la más mínima evidencia, y mucho menos prueba convincente, de que:

  - Huawei sea una empresa de propiedad estatal.

  - Huawei esté controlada por el Estado.

  - La legislación china pueda obligar a Huawei a instalar dispositivos ilegales en sus equipos u otras actividades ilegales que suscitaran en España los riesgos de ciberseguridad descritos en la Toolbox de la UE bajo el epígrafe R5.

- Ni el "pabellón de origen" de los equipos 5G, ni mucho menos la nacionalidad de la empresa proveedora, es un elemento particularmente pertinente a efectos de ciberseguridad.

338. En todos los escenarios normales y previsibles, la cultura corporativa, la ética empresarial, los sistemas de seguridad internos y los objetivos económicos de Huawei mantendrán a Huawei totalmente alineado con los intereses de sus clientes y harán de Huawei un aliado en la preservación de la integridad y la resiliencia contra ciberataques de la red española 5G.

339. ¿Y en el caso de un hipotético "escenario de tensión" de confrontación geopolítica intensa entre China y alguna potencia occidental con repercusiones en España? ¿Qué pasaría, por ejemplo, si, en esas circunstancias, se promulgaran nuevas leyes en China o incluso se nacionalizara Huawei?

340. Independientemente de la probabilidad que atribuyamos a tales escenarios hipotéticos, la idea clave a tener en cuenta sería el retraso inevitable entre cualquier decisión ilegal de motivación política por parte de las autoridades chinas y su efecto potencial en la red 5G española: salvo que los equipos de Huawei ya instalados fuesen vulnerables a tales maniobras ilícitas, la red no se vería afectada por ellas, siempre que cualquier operación de

[91] *Cfr*. Comité de Inteligencia y Seguridad del Parlamento del Reino Unido (2019, 19 julio). *Statement on 5G suppliers*. Disponible en http://isc.independent.gov.uk/.

mantenimiento o mejora necesarias se llevase a cabo de forma segura por personal de confianza.

341. En otras palabras, incluso si los objetivos comerciales y cultura de Huawei quedaran algún día en entredicho por circunstancias hipotéticas y graves, cualquier intento teórico de espionaje o sabotaje por Huawei de las redes 5G españolas sería ineficaz, siempre que se hubieran tomado las precauciones adecuadas al instalar, mantener y actualizar la red 5G.

342. Así pues, la mejor estrategia para mitigar el riesgo potencial de interferencia de un Estado extranjero en la cadena de suministro - que la Toolbox describe como R5- no sería declarar a Huawei "proveedor de alto riesgo" (HRV), sino aplicar efectivamente un sistema de certificaciones, inspecciones y control de todos los proveedores, como prevé la medida técnica 9 (TM09) de la Toolbox. Como ventaja adicional, eso protegería a la red 5G española contra posibles interferencias políticas de cualquier país, incluidas las agencias de seguridad e inteligencia de Estados Unidos.

14.2. Trayectoria de Huawei

343. Al evaluar el perfil de riesgo de un proveedor es necesario tener en cuenta no sólo su nacionalidad, estructura corporativa y cadena de suministro, sino también, según la Toolbox, sus prácticas en materia de ciberseguridad y el grado de prioridad que les ha otorgado. Este será el objeto de los siguientes párrafos.

14.2.1. Ausencia de incidentes de ciberseguridad

344. Como bien afirma Huawei, si bien ha dado servicio a 3.000 millones de personas en más de 170 países y regiones en los últimos 30 años, no hay registros públicos de interrupciones importantes de la red o incidentes de ciberseguridad que puedan manchar su trayectoria en materia de ciberseguridad.

345. Por ejemplo, en 2008 el periódico francés "*Le Monde*" informó de que los servidores de la sede de la Unión Africana en Addis-Abeba habían sido pirateados a través de una puerta trasera, y recordó que el edificio había sido construido en 2012 por chinos, pero en el informe ni siquiera se hace referencia a Huawei, que informó haber instalado el sistema de Internet de la organización, pero negó cualquier implicación en el caso[92].

346. En otro llamativo episodio, en febrero de 2020, la prensa alemana informó de que una delegación estadounidense había presentado pruebas a las autoridades alemanas de que en 2009 Huawei había tenido acceso a información de comunicaciones móviles como resultado de que sus equipos se habían utilizado para fines policiales. Sin embargo, la prueba era tan débil que la revista alemana *Der Spiegel* informó sobre los esfuerzos de la delegación estadounidense para convencer a las autoridades alemanas con el título "Una puerta trasera que sólo EE.UU. puede ver"[93].

[92] *Cf*. https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.
[93] *Cf*. "Einer Hintertür, die nur die USA sehen", disponible en https://www.spiegel.de/netzwelt/netzpolitik/huawei-und-die-spionage-vorwuerfe-eine-hintertuer-die-nur-die-usa-sehen-a-c9c40afd-51a3-43d3-a853-75d1fcdd1946.

347. Es cierto que en su Informe de 2019, el Consejo de Supervisión del HSCEC manifestó lo siguiente:[94]

> "*La deficiente ingeniería de software y los procesos de ciberseguridad conducen a problemas de diseño e implementación lo que incluye vulnerabilidades. El número y la severidad de las vulnerabilidades descubiertas, junto con problemas de arquitectura y construcción por parte del pequeño equipo del HSCEC es preocupante. Si un atacante tuviese conocimiento de estas vulnerabilidades y acceso suficiente para explotarlas, podría ser capaz de afectar el funcionamiento de la red, en algunos casos haciendo que dejase de funcionar correctamente. Otros impactos podrían incluir el ser capaz de acceder al tráfico de los usuarios o de reconfigurar los elementos de la red*".

348. No obstante, el Informe deja claro que las vulnerabilidades descubiertas en la ingeniería y el software de Huawei no eran cruciales ni intencionados:

> *"Sin embargo, los controles [de calidad] sobre el diseño de la red utilizados actualmente por la mayoría de los operadores del Reino Unido limitan la capacidad de los atacantes de poder acceder a partes de la red que no están públicamente expuestas, lo que, junto con otras medidas utilizadas, dificulta la explotación de las vulnerabilidades. Estos controles de diseño, unido la gestión operativa y de seguridad de las redes por parte de los operadores del Reino Unido, seguirán siendo de importancia crítica en los próximos años para gestionar los riesgos residuales causados por los defectos de ingeniería que se detecten".*
>
> *"Estos hallazgos tratan sobre competencias básicas de ingeniería e higiene de la ciberseguridad que dan lugar a vulnerabilidades que pueden ser explotadas por una serie de agentes. El NCSC no cree que los defectos identificados sean resultado de interferencia estatal china".*

14.2.2. Máxima prioridad a ciberseguridad y cooperación con las autoridades

349. A lo largo de los años, Huawei ha realizado continuos esfuerzos para colaborar con sus clientes y con las autoridades públicas para garantizar que sus equipos y productos sean seguros y no vulnerables frente a riesgos de ciberseguridad. En palabras del Sr. Ren:[95]

> "*En Huawei, la ciberseguridad y la protección de la privacidad son siempre las principales prioridades de la compañía. Huawei incorpora de manera decidida los requerimientos del Reglamento General de Protección de Datos (RGPD) de la Unión Europea en todos los procesos de su negocio. Ahora estamos invirtiendo de manera considerable en la mejora de las redes existentes y en la construcción de nuevas redes.*

[94] *Cfr*. Consejo de Supervisión del Centro de Reino Unido de evaluación de ciberseguridad de Huawei. (2019, marzo). *Annual Report 2019*, párrafo 3.18.
[95] *Cfr*. *The Economist.* (2019, 12 septiembre), *op. cit*.

En segundo lugar, durante más de 30 años, Huawei ha dado servicios de red en más de 170 países y regiones, dando servicio a aproximadamente tres mil millones de usuarios. Contamos con una demostrable trayectoria de seguridad. De hecho, nunca hemos tenido incidentes de seguridad importantes, creo que ese dato habla por sí mismo.

Además, estamos más que dispuestos a someternos a una estricta supervisión en los países donde operamos. En la actualidad, el Reino Unido ha llevado a cabo la supervisión más estricta de Huawei. ¿Por qué el Reino Unido está decidido a seguir utilizando nuestros equipos? Han detectado algunos problemas y defectos en nuestro equipo, y sin embargo pueden confiar en nosotros más que en otros proveedores porque hemos sido revisados con mayor rigor".

350. En particular, como ya se indicó secciones anteriores del presente Dictamen, Huawei ha establecido voluntariamente:

- Un laboratorio interno independiente de ciberseguridad (ICSL), que es una unidad de verificación de seguridad certificada por la ISO independiente de los equipos comerciales y de los departamentos de I+D.

- Tres Centros de Transparencia en Europa, que permiten a los clientes verificar e inspeccionar los equipos de Huawei, incluyendo su código fuente, sin comprometer la propiedad intelectual de Huawei. Como ya se indicó, el centro más antiguo y activo es el HCSEC del Reino Unido, que, presidido por la autoridad de ciberseguridad más importante del Reino Unido, se encarga de revisar los equipos y procesos de Huawei, y está tutelada por un Comité de Supervisión (*Oversight Board*). Este último ha confirmado la estrecha participación de Huawei en el proceso de verificación de sus equipos y en el trabajo de corrección necesario para solucionar los problemas técnicos detectados. También ha confirmado que las vulnerabilidades detectadas en el *software* no eran resultado de la interferencia de ningún Estado.

  Según la información pública existente, ningún otro proveedor de equipos de telecomunicaciones ha aceptado un control externo tan riguroso.

- Una Oficina Mundial de Ciberseguridad (GSPO) robusta, de alto nivel y autónoma, con su máximo responsable con línea directa jerárquica y de comunicación con el presidente rotatorio, a través del Comité Global de Ciberseguridad y Protección de la Privacidad de los Usuarios (el GCSPC).

  A pesar de que aún no existe una práctica internacional ni una norma sobre los *Chief Information Officers* ("CIO", o delegados de Información), el lugar que ocupa el *Global Cyber Security and Privacy Officer* (GSPO) de Huawei en la estructura corporativa de la compañía evidencia la importancia clave que se atribuye a su papel, lo que está en línea con las prácticas de otras empresas de telecomunicaciones líderes a nivel mundial (como Telefónica o Apple).

- El nombramiento de un responsable de la protección de datos de la UE independiente, de conformidad con lo dispuesto en el artículo 37 del RGPD -que, según ha confirmado,

no recibe instrucciones sobre el ejercicio de sus funciones, no puede ser destituido ni penalizado por el desempeño de sus tareas y mantiene una línea jerárquica directa con el más alto nivel directivo -el presidente rotatorio- a través del GCSPC, resulta plenamente conforme con las exigencias del artículo 38 del RGDP.

351. Esta actitud cooperativa y proactiva de Huawei al tratar los riesgos de ciberseguridad, y la prioridad que Huawei ha venido atribuyendo a limitarlos, no concuerda con las acusaciones de que podría estar intentando colocar puertas traseras ilegales o dispositivos de sabotaje para hacer que las redes de 5G sean vulnerables a intentos de espionaje o sabotaje promovidos por China.

14.3. Los costes de declarar a Huawei Proveedor de Alto Riesgo (HRV)

352. Como se ha indicado anteriormente, al evaluar la conveniencia de adoptar cualquier medida restrictiva para luchar contra un riesgo hipotético, el principio de proporcionalidad exige tener en cuenta los costes probables de la restricción que se está considerando.

353. En el caso de una prohibición completa del uso de equipos de Huawei en las redes 5G de la Unión Europea, debido al número limitado de proveedores distintos de Huawei (esencialmente Ericsson y Nokia), la exclusión de Huawei tendría un efecto significativo sobre la competencia, en detrimento de los ORM, con efectos en dos o incluso tres frentes:

- El coste de los equipos, que probablemente serían mayores en ausencia de Huawei, un productor de bajo coste cuya presión comercial ha forzado a la baja los precios.

- Una menor innovación tecnológica, ya que los ORM no podrían beneficiarse de las soluciones tecnológicas punteras de Huawei, ni de la presión para innovar resultante de una mayor competencia.

- Una menor competencia en los estándares de seguridad, ya que, como ha declarado el Comité de Inteligencia y Seguridad del Parlamento de Reino Unido, "exigir a los operadores de redes móviles que utilicen equipos de más de un proveedor aumenta la competencia entre dichos proveedores, lo que les obliga a mejorar sus estándares de seguridad"[96].

354. Aunque es difícil calcular con exactitud las consecuencias económicas adversas de una prohibición total sobre Huawei, los cálculos preliminares llevados a cabo el año pasado, a petición de Huawei, por la consultora del Reino Unido *Oxford Economics* sugieren que los costes podrían ser elevados[97]. Los cálculos se basaron en lo siguiente:

- En primer lugar, el aumento estimado de los costes de inversión de los ORM como resultado de los precios más altos cobrados, en ausencia de Huawei, por los dos

[96] El Comité de Inteligencia y Seguridad del Parlamento del Reino Unido (2019, 19 julio), *op. cit.*, p. 2.
[97] *The Economic Impact of Restricting Competition in 5G Network Equipment*, Fig. 1 p. 5. (2019, diciembre). Oxford Economics. https://www.oxfordeconomics.com/recent-releases/Economic-Impact-of-Restricting-Competition-in-5G-Network-Equipment.

competidores restantes (es decir, Nokia y Ericsson), que, según los cálculos de *Oxford Economics*, serían, dependiendo del país, entre un 9% y un 29% más altos (ver tabla).

- En segundo lugar, suponiendo que los ORM mantuvieran su inversión anual nominal en el despliegue del 5G, el aumento de los costes se traduciría en un retraso en el despliegue del 5G, de modo que menos personas tendrían acceso al 5G.

- En tercer lugar, un menor acceso al 5G se traduciría a su vez en un menor crecimiento de la productividad de entre un 0,15% y un 0,30% anual entre 2020 y 2035, lo que llevaría a un PIB significativamente menor en 2035 que en caso de no imponerse restricciones a los proveedores de 5G.

Fig. 1: Economic impacts of restricting a player of Huawei's size from competing in the 5G infrastructure market

Market	Price impact (% increase in investment costs)	Reduction in number of people with access to 5G by 2023 (millions)	Reduction in GDP in 2035 (US$ billions, 2019 prices)
Australia	8% to 27%	0 to 3.1	0.8 to 8.2
Canada	8% to 24%	2.2 to 5.7	1.0 to 6.7
France	9% to 29%	2.1 to 5.7	2.6 to 15.6
Germany	9% to 29%	3.8 to 10.0	2.4 to 13.8
Japan	9% to 27%	7.2 to 19.1	5.3 to 34.3
India	8% to 27%	15.9 to 45.3	4.7 to 27.8
United Kingdom	9% to 29%	3.9 to 10.4	1.8 to 11.8
United States	8% to 24%	0 to 27.1	8.6 to 63.0

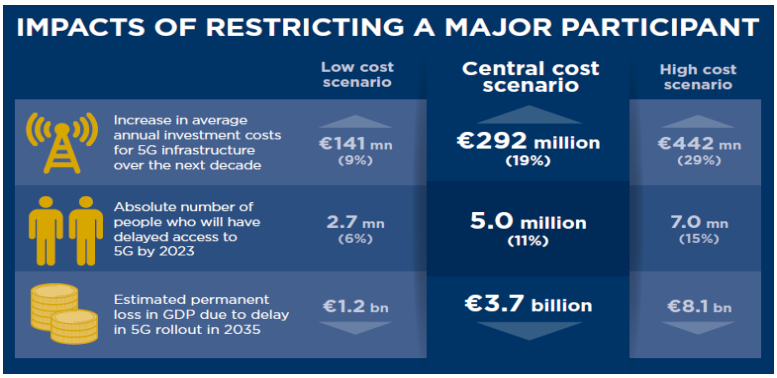
Note: In Australia and the US, 5G rollout is expected to cover a vast majority of the population over the next 2-3 years with almost no increase in coverage in the following years. In our low cost scenario, the increase in investment costs leads to delays in rollout of a few months, despite which a vast majority of the population receives access by 2023.

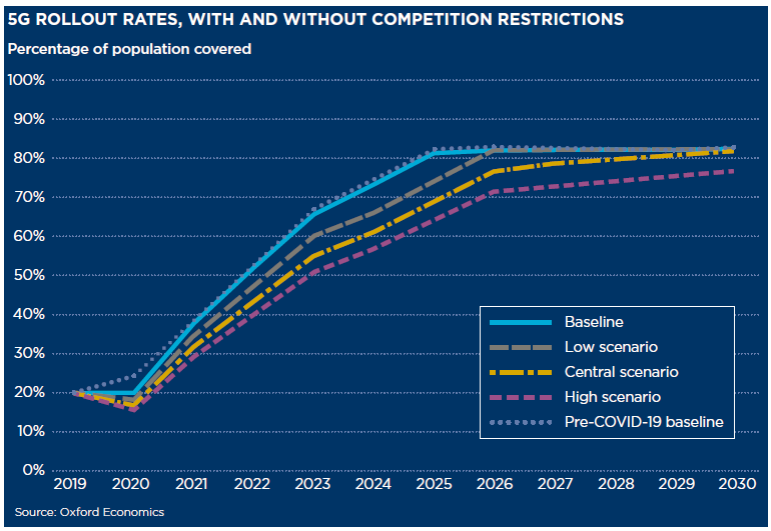
Source: Oxford Economics

355. *Oxford Economics* ha actualizado y ampliado recientemente su análisis preliminar de 2019 sobre el coste para los países europeos que impidan a Huawei competir con Ericsson y Nokia como proveedor potencial de 5G[98]. En el caso de España, consideraron tres escenarios básicos, dependiendo del aumento de los costes de inversión provocado por la ausencia de Huawei: 9% (escenario de bajo coste), 19% (escenario de coste medio) y 29% (escenario de coste alto).

356. Como muestra el cuadro adjunto, en la hipótesis de coste medio o central, los costes anuales de inversión de los ORM aumentarían en unos 292 millones de euros, lo que se traduciría en 5 millones menos de potenciales clientes con acceso a las redes de la ORM en 2023 y una pérdida anual del PIB de 3700 millones de euros en 2035[99].

[98] *The Economic Impact of Restricting Competition in 5G Network Equipment*. (2020, junio). Oxford Economics. https://www.oxfordeconomics.com/recent-releases/The-Economic-Impact-of-Restricting-Competition-in-5G-Network-Equipment.
[99] *Ibid.* p. 75.





357. Además, incluso si, contrariamente a los deseos de los halcones estadounidenses, no fuese legalmente obligatoria una estrategia de "arrancar" los equipos Huawei ya instalados, la prohibición de Huawei sería difícil de conciliar con la arquitectura NSA (*non stand alone*) de la red 5G planeada en España, ya que las estaciones de Huawei ya instaladas no podrían actualizarse para dar servicio a la nueva red de 5G y deberían o bien duplicarse -con un equipo para la red 4G y otro diferente para la nueva 5G- o ser totalmente desmontadas y sustituidas por otras nuevas. Cualquiera de las dos posibilidades implicaría, con toda probabilidad, enormes costes adicionales para los ORM y grandes retrasos en el despliegue real de las redes 5G, ya que las limitaciones de endeudamiento y los límites de inversión podrían obligar a los ORM a extender sus proyectos a horizontes más largos.

358. A modo de ilustración, como informó recientemente el *Financial Times*, "Vodafone ha advertido que las esperanzas del Reino Unido de liderar el mundo en tecnología 5G sufrirían un revés demoledor si el gobierno elimina a Huawei de la infraestructura de telecomunicaciones del país. Como declaró al periódico Scott Petty -director de Tecnología de Vodafone en Reino Unido-, 'el liderazgo del Reino Unido en el 5G se perderá si los operadores móviles se ven obligados a gastar tiempo y dinero en reemplazar equipos existentes'. (…) El Sr. Petty afirmó que, en lugar de eliminar los equipos de Huawei, 'los esfuerzos deberían centrarse en ampliar la cobertura de 5G, desarrollando capacidades en 5G para la industria del Reino Unido'"[100].

[100] *Cfr*. Fildes, N. (2020, 9 junio). *Vodafone warns ripping out Huawei would cost UK lead in 5G*. Financial Times. https://www.ft.com/content/c2fd1c70-3eaa-4e80-8ad3-e88e7bec7d12.

359. Además, en este escenario, los operadores de redes móviles podrían requerir una indemnización por parte de los gobiernos, puesto que, con toda probabilidad, las restricciones legales sobre el uso de los equipos de Huawei tendrían naturaleza expropiatoria, como ocurrió hace ya décadas en España cuando, como consecuencia de las presiones de ETA sobre las centrales nucleares del País Vasco, estas fueron clausuradas como parte de la llamada "moratoria nuclear".

14.4. La existencia de alternativas más eficaces y menos restrictivas

360. La propia Toolbox y la experiencia del Reino Unido con el HCSEC sugieren que habría alternativas menos invasivas, menos discriminatorias y más eficaces para hacer frente a los riesgos hipotéticos que supuestamente justificarían la declaración de Huawei como HRV.

361. Tales medidas podrían consistir, por ejemplo, en el establecimiento, para todo el equipamiento relevante utilizado en las redes 5G, con independencia de quién fuese su proveedor o del lugar en que se fabricasen, de:

- Un sistema obligatorio, pero ágil, de certificación de la ciberseguridad a escala de la UE, tal como se prevé en la medida técnica 9 (TM09) –Utilizar certificaciones de la UE para los componentes de la red 5G, equipos para clientes y/o los procesos de los proveedores- y en la acción de apoyo 5 (SA05) –garantizar la aplicación de medidas de seguridad técnicas y organizativas estándar a través de un esquema de certificación específico a nivel de toda la UE-.

- Facilidades para su inspección o revisión (incluyendo controles de software y código fuente), similares a las que existen actualmente en el Reino Unido para el HCSEC.

362. Queda fuera del alcance de este Dictamen especificar cómo podrían organizarse tales sistemas de certificación e inspección (ya sea para equipos o proveedores, máquinas o procesos, etc.). Pero la mera lectura de la Toolbox sugiere que, en lo relativo a los riesgos de ciberseguridad, algunas de las “medidas técnicas” que sugiere harían innecesarias algunas de las “medidas estratégicas” que defiende, como la 3 (SME 03).

363. En cuanto a los riesgos de ciberseguridad, como tales, esta opinión es compartida por algunos analistas, como Tim Rühlig, del Instituto Sueco de Asuntos Internacionales:[101]

> "*Existen medios más eficaces [que excluir completamente a Huawei del despliegue de la infraestructura de 5G] para mitigar los riesgos de seguridad de la red. Los más efectivos son un mejor cifrado de extremo a extremo, lo que dificulta el espionaje; y redundancias de red que aumentan la disponibilidad de cobertura junto con diversidad de proveedores. La diversidad de proveedores se basa en el supuesto de que todos los equipos de 5G contendrán vulnerabilidades, pero los equipos de los distintos proveedores tendrán vulnerabilidades de distinto tipo que harán más difícil*

[101] *Cfr*. Rühlig, T. (2020, 27 febrero). *Who controls Huawei? Implications for Europe*, pgs. 4 y 5. UI paper 5/2020, Instituto Sueco de Asuntos Internacionales. Disponible en https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf.

para los atacantes su identificación y explotación de manera eficaz. Estos medios podrían combinarse con una mejor evaluación y certificación de productos y procesos, incluyendo revisiones de código fuente o monitorización del flujo de red".

364. En realidad, al reducir la diversidad de proveedores, la exclusión de Huawei podría ser contraproducente:[102]

> "*Una respuesta europea adecuada abordaría los problemas de seguridad de la red por medios técnicos en lugar de excluyendo a Huawei. Una mejor encriptación de extremo a extremo, redundancia y diversidad de proveedores serán las medidas más importantes, aunque costosas de implementar (…)*
>
> *Una prohibición absoluta de Huawei sería contradictoria con el objetivo de diversidad de proveedores, particularmente en lo que respecta a la Red de Acceso Radio que actualmente sólo es provista por tres empresas: Huawei, Nokia y Ericsson*".

365. Por último, como ya se ha indicado, un sistema general de certificación y control de los equipos 5G, independientemente de su proveedor, podría ayudar a evitar la interferencia en las redes de comunicaciones de la UE por parte de todos los Estados extranjeros, incluidos los Estados Unidos y sus agencias de inteligencia, que en virtud del capítulo 26 de la Ley de Vigilancia de la Inteligencia Extranjera (FISA, *Foreign Intelligence Surveillance Act*) permite al Gobierno de los Estados Unidos llevar a cabo vigilancia electrónica fuera de los Estados Unidos, como se establece explícitamente en la Ley de Enmienda a la FISA de 2008.

14.5. Conclusiones

366. El examen de la jurisprudencia relativa a la "excepción de seguridad nacional" del artículo XXI del GATT, al llamado "principio de precaución" y al ejercicio de facultades administrativas discrecionales lleva a la conclusión ineludible de que, al evaluar los riesgos no técnicos de un suministrador de equipos para redes 5G, como Huawei, y al considerar posibles medidas restrictivas para mitigar tales riesgos, en España -y probablemente en muchos otros países de la UE-:

- Las restricciones no pueden basarse en "meras suposiciones" o ser el resultado de un "perfilado" (*profiling*) de proveedores basado en su nacionalidad.

- En las evaluaciones de riesgos se debe tener en cuenta la trayectoria del proveedor y la prioridad que ha venido otorgando a las medidas de mitigación de los riesgos de ciberseguridad.

- Los costes de las medidas restrictivas deben ser ponderados objetivamente en relación con sus beneficios probables.

- Deberán preferirse siempre aquellas medidas menos invasivas y menos discriminatorias que logran los mismos resultados o incluso son más eficaces para

[102] *Ibid.* p. 19.

alcanzar el objetivo público perseguido. En particular, hay medidas técnicas -como los esquemas de certificación, defendidos por la Toolbox- que serían más idóneos y proporcionales para lograr el objetivo de ciberseguridad que imponer cualquier restricción específica a proveedores de 5G como Huawei.

15. Conclusiones generales

367. A la luz del análisis anterior y con las limitaciones descritas en la Introducción, las principales conclusiones del presente Dictamen pueden resumirse así:

XI. La Toolbox de la UE es un instrumento de "*soft law*" preparado por expertos en ciberseguridad, en el marco del Grupo de Cooperación NIS. Por tanto, por su propia naturaleza y origen, la Toolbox guarda silencio respecto a los criterios jurídicos que deben aplicar los Estados miembros al realizar la evaluación de riesgos recomendada en la medida estratégica 3 (SM 03).

XII. De acuerdo con los principios jurídicos y jurisprudencia europeos y españoles, la adopción de medidas restrictivas de protección contra riesgos hipotéticos no puede basarse en meras especulaciones. Además, deben preferirse las alternativas más eficaces y menos restrictivas y costosas que logran un objetivo público -como la ciberseguridad de las redes 5G- antes que otras menos efectivas y más invasivas y costosas.

XIII. España cuenta con un sólido marco jurídico y reglamentario que otorga a las autoridades españolas las competencias sugeridas por la Toolbox. Sus amplias facultades para hacer cumplir las leyes, al permitirles imponer elevadas multas y medidas correctoras, pueden constituir una medida de mitigación de riesgos muy eficaz.

XIV. La evaluación de riesgos de proveedores individuales, como Huawei, no puede llevarse a cabo mediante métodos de "perfilado" (*profiling*) basados en la mera nacionalidad, sino que requiere considerar la trayectoria específica de Huawei y la prioridad otorgada a las medidas de mitigación y prevención de riesgos de ciberseguridad.

XV. A lo largo de los años, Huawei se ha esforzado de manera continua en cooperar con sus clientes y con las autoridades públicas a fin de garantizar que sus equipos y productos son seguros y no vulnerables frente a riesgos de ciberseguridad. Como parte de este esfuerzo, ha establecido voluntariamente:

- Un laboratorio interno independiente de ciberseguridad (ICSL), que es una unidad de verificación de seguridad certificada por la ISO independiente de los equipos comerciales y de los departamentos de I+D.

- Tres Centros de Transparencia en Europa, que permiten a los clientes verificar e inspeccionar los equipos de Huawei, incluyendo su código fuente, sin comprometer la propiedad intelectual de Huawei. Como ya se indicó, el centro más antiguo y activo es el HCSEC del Reino Unido, que, presidido por la autoridad de ciberseguridad más importante del Reino Unido, se encarga de revisar los equipos y

procesos de Huawei, y está tutelada por un Comité de Supervisión (*Oversight Board*). Este último ha confirmado la estrecha participación de Huawei en el proceso de verificación de sus equipos y en el trabajo de corrección necesario para solucionar los problemas técnicos detectados. También ha confirmado que las vulnerabilidades detectadas en el *software* no eran resultado de la interferencia de ningún Estado.

Según la información pública existente, ningún otro proveedor de equipos de telecomunicaciones ha aceptado un control externo tan riguroso.

- Una Oficina Mundial de Ciberseguridad (GSPO) robusta, de alto nivel y autónoma, con su máximo responsable con línea directa jerárquica y de comunicación con el presidente rotatorio, a través del Comité Global de Ciberseguridad y Protección de la Privacidad de los Usuarios (el GCSPC).

  A pesar de que aún no existe una práctica internacional ni una norma sobre los *Chief Information Officers* ("CIO", o delegados de Información), el lugar que ocupa el *Global Cyber Security and Privacy Officer* (GSPO) de Huawei en la estructura corporativa de la compañía evidencia la importancia clave que se atribuye a su papel, lo que está en línea con las prácticas de otras empresas de telecomunicaciones líderes a nivel mundial (como Telefónica o Apple).

- El nombramiento de un delegado europeo de protección de datos independiente, de conformidad con lo dispuesto en el artículo 37 del RGPD -que, según ha confirmado, no recibe instrucciones sobre el ejercicio de sus funciones, no puede ser destituido ni penalizado por el desempeño de sus tareas y mantiene una línea jerárquica directa con el más alto nivel directivo -el presidente rotatorio- a través del GCSPC, resulta plenamente conforme con las exigencias del artículo 38 del RGDP.

Esta actitud cooperativa y proactiva de Huawei al tratar los riesgos de ciberseguridad, y la prioridad que Huawei ha venido atribuyendo a limitarlos, no concuerda con las acusaciones de que podría estar intentando colocar puertas traseras ilegales o dispositivos de sabotaje para hacer que las redes de 5G sean vulnerables a intentos de espionaje o sabotaje promovidos por China.

XVI. Las especulaciones de que los equipos de Huawei están especialmente expuestos a un riesgo de interferencia por parte de las autoridades chinas -presumiblemente mediante la colocación de puertas traseras, con propósitos de espionaje, o de mecanismos de sabotaje (como *kill switches*) parecen infundadas y pasan por alto, además, que una parte significativa de la cadena de suministro de todos los proveedores de 5G, incluidos Ericsson y Nokia, incluyen actividades de fabricación llevadas a cabo en China.

XVII. Más concretamente, en mi opinión:

- Huawei es una empresa privada, no muy diferente de una gran cooperativa europea, y no es de propiedad estatal.

- No hay ni el más mínimo indicio de que Huawei esté "controlada por el Estado".

- El riesgo de que Huawei o algunos de sus empleados se vean obligados a incorporar dispositivos ilegales en sus equipos o programas de 5G es extremadamente remoto y no superior al de otros fabricantes.

- La trayectoria de Huawei en materia de ciberseguridad es excelente.

- A lo largo de los años, Huawei ha demostrado un gran espíritu de cooperación en materia de ciberseguridad con todas las autoridades europeas y con los ORM europeos, y se ha sometido voluntariamente a los controles más estrictos.

- Imponer medidas restrictivas a Huawei, y no digamos una prohibición total, como proveedor de equipos 5G para los ORM españoles implicaría un alto coste.

XVIII. Los riesgos de ciberseguridad resultantes de la interferencia de Estados de fuera de la Unión (R5, en la terminología de la Toolbox) podrían abordarse de manera más eficaz mediante un sistema general de verificación y/o inspección obligatoria de todos los equipos relevantes de 5G, junto con estrictos controles en las posteriores actividades de mantenimiento o actualización de equipos. Cualquiera de estas inspecciones o de estos controles deberían ser de aplicación para todos los proveedores, independientemente de su nacionalidad o del lugar de fabricación, adquisición o desarrollo de esos equipos.

XIX. Sobre la base de lo anterior y de la información que he revisado, considero que no existe base legal para imponer a Huawei restricciones específicas en desarrollo de la medida estratégica 3 (SM 03) de la Toolbox.

La adopción de tales restricciones sobre Huawei no sería una medida ni adecuada o idónea, ni proporcional.

La medida no sería "adecuada" para alcanzar el objetivo público perseguido -es decir, la ciberseguridad de las redes 5G de España-, ya que los potenciales riesgos de ciberseguridad de las redes de 5G:

- No están relacionadas con la nacionalidad del proveedor de los equipos, sino con las medidas de ciberseguridad utilizadas en su diseño, fabricación, control, verificación e inspección, cualquiera que sea su proveedor o la nacionalidad de este. Aunque se trate de una cuestión técnica que rebasa la experiencia del autor de este Dictamen, la aseveración de Huawei de que todos sus equipos cumplen con los estándares de ciberseguridad más exigentes, incluida la inspección de su código fuente, y por lo tanto, son equiparables a las mejores en términos de ciberseguridad, parece cierta.

- El objetivo de ciberseguridad podría verse en realidad puesto en peligro si se impusiera restricciones a un proveedor concreto, Huawei, y se obligara a los ORM a depender exclusivamente de los otros dos proveedores.

La medida tampoco sería proporcional, ya que existen otras medidas menos restrictivas, más eficaces y menos costosas para lograr el objetivo perseguido, a saber, el establecimiento de un sistema riguroso de verificación, certificación, inspección, pruebas, auditoría o, más en general, de control de todos los equipos relevantes utilizados en las redes 5G, aplicado de forma general, independientemente del proveedor y del lugar en que lo haya diseñado o fabricado.

16. Consideraciones finales

I. Los estándares jurídicos y principios constitucionales aplicables al que Alan Dershowitz ha denominado "Estado preventivo" pueden no ser necesariamente iguales en los Estados Unidos que en la Unión Europea o en España.

II. En la historia de los Estados Unidos existe un caso de una evaluación no técnica del riesgo llevada a cabo por el Gobierno de los Estados Unidos sobre la base de "perfiles raciales", que, aunque en su momento fue parcialmente refrendada por el Tribunal Supremo[103], no cumple con los principios jurídicos descritos en este Dictamen y fue posteriormente desautorizado en los EE.UU. Se trata de la detención masiva de unos 110.000 estadounidenses de ascendencia japonesa tras el ataque a Pearl Harbour en diciembre de 1941, tal y como lo describe Dershowitz:[104]

> "*Circulaban rumores de que hawaianos de ascendencia japonesa estaban guiando a los pilotos y submarinos enemigos, que los japoneses-americanos se habían infiltrado intencionalmente en las compañías de energía y agua, y que habían formado miles de redes de sabotaje y espionaje. No se pudo demostrar que fuese cierta ninguna de estas historias. Los registros del FBI, del Ejército y de la inteligencia naval indican que no hubo ni un solo caso de espionaje o sabotaje por ningún residente de ascendencia japonesa antes, durante, o después de la Segunda Guerra Mundial. La ausencia de tales actividades no satisfizo, sin embargo, a una población histérica, con prejuicios raciales profundamente arraigados. De hecho, el Fiscal General de California, Earl Warren, expresó una idea del tipo "Alicia en el País de las Maravillas" cuando afirmó que la ausencia misma de sabotajes era "la señal más ominosa de toda esta situación [ya que] fue diseñada para proporcionarnos una falsa sensación de seguridad (…) Creemos que cuando tratamos con la raza caucásica tenemos métodos que pondrán a prueba su lealtad, pero cuando hablamos de la japonesa... no podemos formarnos una opinión sólida*".

El General estadounidense John De Witt, jefe del *Western Defense Command*, expresó las opiniones de Warren en términos más sucintos y lapidarios:

> "*Un japonés es un japonés. No hay forma de determinar su lealtad*".

[103] En el caso *Korematsu v. United States* (1944), el Tribunal Supremo estadounidense, aunque no versaba sobre el internamiento en los campos de reubicación, apoyó la decisión de Roosevelt de excluir a los japoneses-americanos de la zona militar de la costa oeste.
[104] *Cfr*. Dershowitz, A. M. (2006), *op. cit*. pgs. 111 y 112.

III. Pues bien, a pesar de la presión política de un poderoso aliado político, el Gobierno español debiera abstenerse de aplicar a Huawei lo que sería, en esencia, un "perfilado (*profiling*) al estilo De Witt" y, basándose en que es una empresa china, declarar a Huawei proveedor de alto riesgo (HRV).

IV. En suma, la ciberseguridad de las futuras redes 5G constituye un objetivo público esencial, que las autoridades europeas y españolas deberán mitigar con las medidas técnicas idóneas descritas por la propia *Toolbox*, entre las que destaca la 9 (TM09): Uso de certificaciones UE para los componentes de la red de 5G, equipos de cliente y/o procesos de proveedores. Por el contrario, aplicar a Huawei, por ser empresa china, restricciones como proveedor de 5G en aplicación de la "medida estratégica" 3 (SM03) constituiría una arbitrariedad política sin base jurídica.

V. Es célebre el dicho de Deng Xiaoping de que "da igual que el gato sea blanco o negro, lo importante es que cace ratones". Pues bien, un enfoque mucho más coherente con las normas y jurisprudencia españolas que el "perfilado (*profiling*) al estilo De Witt" sería que el Gobierno español aplique a todos los proveedores de 5G una versión actualizada del dicho de Deng:

> "*Da igual que el gato sea chino u occidental, lo importante es que todos cumplan al 100% con las normas de ciberseguridad*".

Madrid, 4 de julio de 2020

Manuel Conthe Gutiérrez