



**TIPO DE TRABALHO:** INFORMAÇÃO

**SOLICITANTE:** Deputada PERPÉTUA ALMEIDA

**ASSUNTO:** Elaborar informação Técnica com a situação da tecnologia 5G no Brasil e no mundo.

**AUTOR:** Fabio Luis Mendes  
Consultor Legislativo da Área XIV  
Ciência e tecnologia, Comunicação Social,  
Informática, Telecomunicações e Sistema Postal

## Sumário Executivo

Esta Informação Técnica tem por finalidade expor os principais aspectos da tecnologia 5G de telefonia móvel, e um resumo dos aspectos geopolíticos e técnicos que estão direcionando sua implantação em âmbito global, assim como seu reflexo no Brasil.

O 5G é a mais recente tecnologia de transmissão de internet móvel, podendo oferecer, em certas circunstâncias, até 20 vezes mais velocidade que a tecnologia atual, 4G, sendo considerada fundamental para o desenvolvimento de funcionalidades como carros autônomos, telecirurgias, IoT (Internet das coisas), entre outros.

Há basicamente 5 fornecedores da tecnologia em âmbito global: Huawei (China), Ericsson (Suécia), Samsung (Coreia do Sul), Nokia (Finlândia) e Fujitsu (Japão). Hoje a maior fornecedora é a Huawei (28,5% de *market share* global de infraestrutura), seguida da Ericson (25,5%)<sup>1</sup>. Os EUA baniram os equipamentos desta marca em suas redes sob a alegação de que a tecnologia contém "*backdoors*" que permite a espionagem sobretudo em função da Lei de Inteligência chinesa, de 2017, e estão fomentando parceiros a adotar medidas similares. Inglaterra, Austrália, Japão e Nova Zelândia já baniram a empresa de suas redes.

No caso do Brasil, os leilões de frequência da tecnologia 5G tem previsão de ocorrer em 2021, e serão executados pela Anatel. As empresas fornecedoras de infra-estrutura, posteriormente, terão seus equipamentos homologados pela Anatel (conforme previsão da Lei Geral de Telecomunicações), e deverão adotar os requisitos em termos de segurança cibernética previstos na IN nº4, de 4 de março de 2020, do GSI (Gabinete de Segurança Institucional).

Ao final da Informação estabelecemos as possibilidades de atuação do Congresso Nacional na formulação da política da tecnologia 5G.

---

<sup>1</sup><https://www.trendforce.com/presscenter/news/20200803-10422.html>

## **Informação Técnica - Tecnologia 5G**

A tecnologia de comunicação móvel 5G é uma evolução da utilizada atualmente, 4G, trazendo mais velocidade na transferência de dados. Enquanto a tecnologia 4G permite transferências em média a 5 MBPS (Megabytes por segundo), a tecnologia 5G permite conexões móveis de até 100 MBPS (Megabytes por segundo).

A tecnologia 5G, para implantação no Brasil, depende de leilões de frequência da Anatel, os quais devem ocorrer em 2021. Já há, porém, uma operação da empresa Claro - 5G DSS (Compartilhamento Dinâmico de Espectro), implementado por tecnologia da empresa sueca Ericsson, sobre as frequências 4G.

## **Fornecedores de infraestrutura 5G**

Atualmente existem 5 principais fornecedores globais de equipamentos para implantação da tecnologia 5G: Ericsson (Suécia); Fujitsu (Japão); Huawei (China); Samsung (Coreia do Sul) e Nokia (Finlândia).

## **EUA x Huawei**

Os EUA vêm adotando uma postura em sua política externa de fomentar que seus parceiros em âmbito mundial proibam a adoção da tecnologia da empresa chinesa Huawei em suas redes de telecomunicações.

A principal argumentação dos EUA é que a Huawei está submetida à “Lei de Inteligência Nacional”<sup>2</sup>, em vigor desde 2017 na China, a qual estabelece que qualquer organização ou cidadão deve apoiar, ajudar e cooperar com o trabalho da inteligência do estado chinês.

O fato de a Huawei ter sido fundada, em 1987, por Ren Zhengfei, um engenheiro chinês que é ex-militar do exército chinês e próximo do Partido Comunista chinês, reforça as suspeitas. A Huawei nega que ajude o governo chinês a espionar. Mas os EUA e alguns aliados temem que a empresa possa tanto empenhar-se ativamente em espionar quanto ser

---

2

<https://www.bbc.com/portuguese/brasil-50468237#:~:text=A%20Lei%20de%20Intelig%C3%AAncia%20Nacional,meio%20ao%20avan%C3%A7o%20do%205G>.

incapaz, pela lei chinesa, de rejeitar pedidos de Pequim para entregar dados que estejam em seus servidores sobre cidadãos que não são chineses.

Em audiência pública<sup>3</sup> no Senado dos Estados Unidos da América, em 4 de março de 2020, James Andrew Lewis, que é vice-presidente sênior e diretor do Programa de Tecnologia e Políticas Públicas do CSIS<sup>4</sup> (Centro de Estudos Estratégicos e Internacionais), afirmou que EUA, Japão e Austrália baniram a Huawei de duas redes de telefonia 5G. À época, o Reino Unido tinha proibido a tecnologia da empresa chinesa em dois terços de sua rede 5G e de ser usada em áreas sensíveis do governo<sup>5</sup> em instalações militares. Segundo Lewis, a única maneira de os EUA, Japão, Austrália eliminarem totalmente o risco de insegurança de suas redes foi de proibir a tecnologia da Huawei em suas redes.

A estratégia inicial do Reino Unido tinha sido banir a Huawei do "núcleo" das redes de telecomunicações e confiá-la à "borda", como a rede de acesso de rádio (a torre de celular que conecta seu telefone à rede). Entretanto, desde julho de 2020 a proibição é total<sup>6</sup> também no Reino Unido<sup>7</sup>.

Segundo o executivo, “espionagem, subsídios ilícitos e preços predatórios ajudaram a Huawei a afastar os fabricantes de telecomunicações ocidentais do mercado e outros setores da economia europeia, como aeroespacial e automóveis, estão agora em risco”. Ele afirmou ainda que a “Huawei não é o único fornecedor de tecnologia 5G, nem dispõe do melhor equipamento disponível. De fato uma análise de uma agência de inteligência

---

3

<https://www.commerce.senate.gov/services/files/563D903B-FEF0-4A1C-9202-A7DC1CCEFC6>

4 <https://www.csis.org/people/james-andrew-lewis>

5

<https://www.london.gov.uk/press-releases/assembly/huawei-5g-ban-emergency-services-system-compromis>

6

<https://www.moneytimes.com.br/governo-britanico-decide-proibir-huawei-em-rede-5g-do-reino-unido/>

7 <https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027>

européia concluiu que a Huawei era a mais vulnerável à exploração de inteligência devido a problemas de engenharia e software”.

Ainda segundo o pesquisador do CSIS, “Nokia e Ericsson oferecem tecnologia 5G que é melhor e mais segura, e a Samsung também está estabelecendo uma presença no mercado 5G”.

Reportagem do “The Wall Street Journal”<sup>8</sup>, de 12/02/2020, aponta que o sistema da Huawei, há mais de uma década, usa “*backdoors*” para aplicação da lei de inteligência chinesa. Segundo o jornal, os EUA notaram acesso em equipamentos 4G desde 2009.



Os “*backdoors*” são recursos presentes em sistemas informáticos, em geral camuflados, que são uma porta de acesso não declarada ao sistema. Essas portas podem ser criadas por programa instalado

---

8

<https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256>

posteriormente não autorizado pelo fabricante ou proprietário, ou até mesmo por quem desenvolveu o sistema.

Segundo a reportagem do WSJ, os “backdoors” foram inseridos para uso da “polícia” em estações rádio-base, antenas e equipamentos de comutação. Autoridades dos EUA alegam que os “backdoors” foram projetados para serem acessíveis pela Huawei.

A BBC britânica também apontou em reportagem, de 8 de março de 2019<sup>9</sup>, que o governo do Reino Unido tinha preocupações com backdoors na tecnologia da Huawei. A empresa sofria acusações de que sua tecnologia 5G pode representar risco à segurança nacional, já que a China poderia estar usando a Huawei como forma de espionar nações rivais e obter informações.



**BBC** Sign in Home News Sport Reel

## NEWS

Home | US Election | Coronavirus | Video | World | US & Canada | UK | Business | Tech | Science | Stories

### Government's worries over backdoors in Huawei's 5G tech castle

Huawei is facing allegations that its next generation 5G equipment could pose a national security risk.

There are concerns that China is using Huawei as a proxy and could spy on rival nations and scoop up useful information.

The BBC's cyber security reporter Joe Tidy explains why one potential problem with 5G technology may have more to do with castles than you'd expect.

#### IN nº 4, de 26 de março de 2020 - GSI - Brasil

Disposições sobre “backdoors” em tecnologia 5G já estão presentes na legislação brasileira. O GSI (Gabinete de Segurança

<sup>9</sup> <https://www.bbc.com/news/av/technology-47489411>

Institucional)<sup>10</sup> editou a Instrução Normativa nº 4, de 26 de março de 2020<sup>11</sup>, que dispõe sobre os requisitos mínimos de Segurança Cibernética que devem ser adotados no estabelecimento das redes 5G.

Nesta instrução normativa, o art. 3º define que “os requisitos estabelecidos neste ato buscam elevar a proteção da sociedade e das instituições nacionais, em face da possibilidade de existência de vulnerabilidades e backdoor sem sistemas de tecnologia 5G”, e, no parágrafo único, que as “vulnerabilidades e backdoors existentes nos equipamentos 5G, implementadas de forma intencional ou involuntária pelos fornecedores da tecnologia, poderão ocasionar o comprometimento da segurança do sistema”.

#### *Homologação de equipamentos*

Os equipamentos de infraestrutura de 5G deverão ser homologados pela Anatel (art. 19, XIII da LGT), conforme a Resolução Anatel nº 715, de 23 de outubro de 2019<sup>12</sup>. Os equipamentos devem estar em conformidade com as normas da Anatel, sendo que isso atestado por Organismos de Certificação Designados (OCDs)<sup>13</sup>, entre os quais do CPqD<sup>14</sup>.

#### **Open RAN**

As infraestruturas de transmissão de dados e voz das operadoras de telecomunicações têm como elemento central o que se chama de RAN (*Radio Access Network*). Esse conjunto de equipamentos que, de um lado, recebe e transmite os sinais para os terminais dos usuários, os processa, e, posteriormente, envia e recebe esses sinais para todo o sistema de transmissão que implementa a rede de telefonia móvel.

---

<sup>10</sup> <https://www.gov.br/gsi/pt-br>

<sup>11</sup> <https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-250059468>

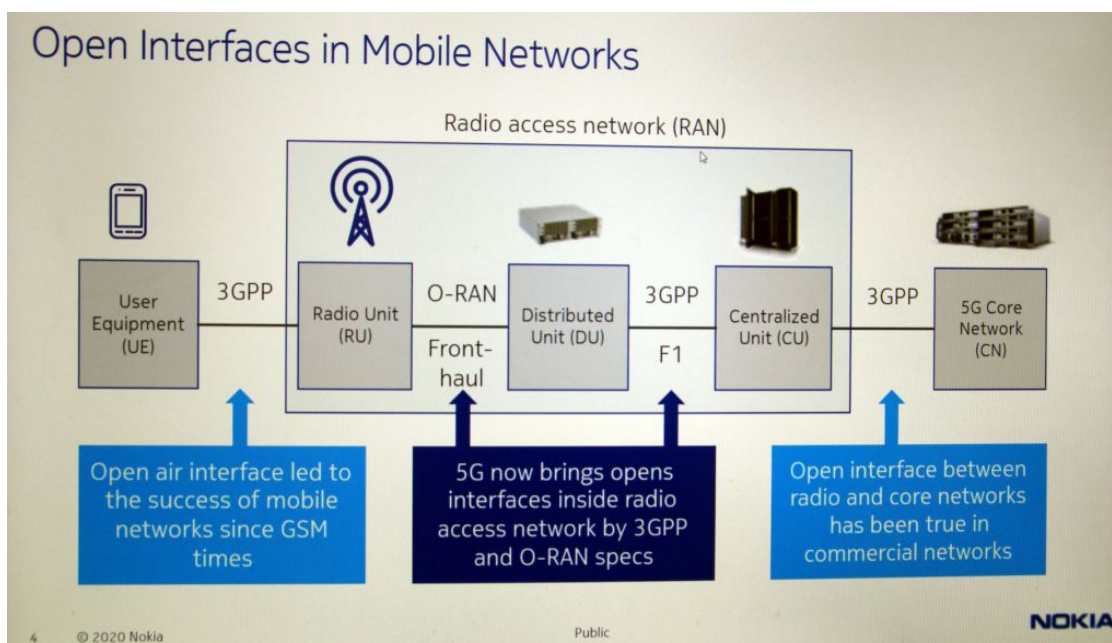
<sup>12</sup> <https://www.anatel.gov.br/legislacao/resolucoes/2019/1350-resolucao-715#art3>

<sup>13</sup> [https://www.anatel.gov.br/Portal/exibirPortalPaginaEspecial.do?acao=&codItemCanal=606#~:text=Organismo%20de%20Certifica%C3%A7%C3%A3o%20Designado%20\(OCD,os%20certificados%20de%20conformidade%20correspondentes.](https://www.anatel.gov.br/Portal/exibirPortalPaginaEspecial.do?acao=&codItemCanal=606#~:text=Organismo%20de%20Certifica%C3%A7%C3%A3o%20Designado%20(OCD,os%20certificados%20de%20conformidade%20correspondentes.)

<sup>14</sup> <https://www.cpqd.com.br/>



Uma das questões que é objeto de discussão no setor é que, em decorrência de especificações e padrões técnicos estabelecidos por cada fornecedor de infraestrutura, se uma operadora adquire um componente dessa RAN de um fornecedor, ela será obrigada a comprar todos os demais componentes desse mesmo fornecedor, já que componentes de fornecedores diversos não “conversam” entre si. O esquema abaixo, da Nokia, mostra esquematicamente o RAN.



Essa característica limita a competição de mercado entre os fornecedores dos equipamentos que formam o RAN. Dessa forma, para tentar endereçar esse problema criou-se, em âmbito internacional, a iniciativa Open RAN - Open Radio Access Network Alliance<sup>15</sup>.

Open RAN é basicamente um consórcio de empresas (do qual a Huawei não faz parte, mas a ZTE chinesa e a operadora China Telecom estão presentes) que propõe um padrão de RAN que permitiria que componentes de várias empresas se comunicassem dentro dela. Isso evitaria a necessidade atual de uma operadora ser obrigada a comprar a RAN inteira de um fabricante, pois os elementos internos de um fabricante não conversam

<sup>15</sup> <https://www.o-ran.org/>



com componentes de outro fabricante. Ou seja, é uma tentativa de criar um padrão para permitir interoperabilidade, e, assim, ampliar a competição.

Esse é o aspecto mais visível de uma mudança em termos de ampliação de mercado, sendo um projeto de um grupo formado por um consórcio de empresas<sup>16</sup> para desenvolvimento de arquiteturas e software que permitirão redes virtualizadas (por exemplo, aquelas com base em software em vez de hardware) e interface padronizada.

É necessário considerar que o RAN (*Radio Access Network*) é uma das partes mais caras da infraestrutura de telecomunicações. A limitação de interoperabilidade de equipamentos de outros fornecedores decorre de um protocolo técnico denominado CPRI, o qual gerencia as conexões entre o equipamento de processamento de sinal (chamado de banda base) e os rádios, no que as operadoras chamam de parte "*fronthaul*" da rede. Há tantas variáveis em qualquer implementação de CPRI que os operadores são forçados a trabalhar no sistema de um único fornecedor, se tornando, portanto, uma ferramenta proprietária.

Um aspecto importante a se considerar é que grande parte da rede 5G será criada com equipamentos da rede 4G em uso. Antenas e grande parte do RAN será compartilhado. Dessa forma, há uma tendência de as operadoras de telefonia optarem por comprar o equipamento adicional necessário para implementar a rede 5G do fornecedor de sua rede atual (4G), tornando o custo de migração menor.

Caso uma empresa use um equipamento RAN de um fornecedor, e, por alguma razão (como a proibição legal de um determinado fornecedor), tenha que optar por outro fornecedor, se deparará com um custo de implantação maior, porque essa empresa terá que substituir milhares de antenas de um fornecedor e trocá-las por um kit completo de outro - o que eleva significativamente os custos.

---

<sup>16</sup> <https://www.o-ran.org/membership>

Segundo um documento da Deutsche Telekom<sup>17</sup>, a principal operadora de telefonia alemã, caso a Huawei seja banida da Alemanha, o custo para ajustar sua rede para eliminar equipamentos será da ordem de € 3 bilhões de euros.

#### Iniciativa Clean Network - Departamento de Estado (EUA)



O programa “Clean Network” foi estabelecido pelo Departamento de Estado dos EUA<sup>18</sup>, e anunciado como “abordagem abrangente da Administração Trump para proteger os ativos da nação, incluindo a privacidade dos cidadãos e as informações mais confidenciais das empresas contra intrusões agressivas de atores malignos, como o Partido Comunista Chinês”.

A iniciativa parte de um documento denominado “Propostas de Praga”, oriundo de um Grupo de Trabalho sobre segurança em redes 5G, criado a pedido do Departamento de Estado dos EUA, e que reuniu especialistas asiáticos, empresas e centros de pesquisa europeus e americanos, para desenvolver critérios para avaliar a confiabilidade de fornecedores de equipamentos de telecomunicações. O grupo emitiu um

---

<sup>17</sup>

<https://www.lightreading.com/5g/deutsche-telekom-is-in-a-5g-mess-if-huawei-is-banned/d/d-id/762569>

<sup>18</sup> <https://www.state.gov/the-clean-network/>

documento com 31 pontos para determinar a confiabilidade e a segurança das redes 5G<sup>19</sup>.

Essas recomendações se dividem em “**Critérios Políticos e de Governança**”, “Critérios de avaliação de práticas comerciais”, “Critérios de mitigação de risco de segurança cibernética” e “**Ações governamentais para aumentar a confiança na escolha de um fornecedor**”.

No grupo de “**Critérios Políticos e de Governança**” estabelece-se que fornecedores são considerados confiáveis se estiverem sediados em países democráticos, com judiciário independente, que sigam princípios de estado de direito, de proteção de dados pessoais e de transparência, entre outros .

Já no contexto das recomendações de “ações governamentais para aumentar a confiança na escolha de um fornecedor”, o documento estabelece que os governos devem ter a política e ferramentas legais para avaliar o perfil de risco de um fornecedor e determinar que os fornecedores são capazes de demonstrar confiabilidade com base em avaliações independentes de critérios técnicos e não técnicos (políticos) relacionados, mediante avaliações sistemáticas e periódicas, e que devem evitar a “monocultura de fornecedores”.

Os Estados Unidos alegam que cerca de 30 países e regiões aderiram ao plano da Rede Limpa, incluindo Reino Unido, República Tcheca, Polônia, Suécia, Estônia, Romênia, Dinamarca e Letônia. Entretanto, segundo a publicação chinesa Global Times<sup>20</sup>, “*muitos dos países negaram ter aderido ao programa, mas mesmo assim foram incluídos pelos EUA na lista*” .

*Posicionamento da “European Competitive Telecommunications Association (ECTA)” sobre Clean Network*

---

<sup>19</sup>

[https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200511\\_Lewis\\_5G\\_v3.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200511_Lewis_5G_v3.pdf)

<sup>20</sup> <https://www.globaltimes.cn/content/1200334.shtml>

A ECTA<sup>21</sup> é uma associação europeia de telecomunicações competitiva, formada por operadores de telecomunicações e fornecedores de soluções digitais em toda a Europa.

Em 16 de outubro de 2020<sup>22</sup> essa associação emitiu uma declaração denunciando quaisquer proibições de fornecedores 5G chineses por razões geopolíticas e enfatizando que tais decisões só podem ser justificadas com base em fatos bem estabelecidos, frisando que a exclusão de fornecedores específicos terá impactos negativos sobre os consumidores, empresas e mercados.

#### *Posicionamento do Itamaraty sobre Clean Network*

Nos dias 9, 10 e 11 de novembro de 2020 o Brasil recebeu a visita do subsecretário para Crescimento Econômico, Energia e Meio Ambiente do Departamento de Estado (DoS) dos EUA, Keith Krach.

Na Nota à Imprensa nº 135<sup>23</sup>, de 10/11/2020, atualizada em 11/11/2020, divulgada pelo Itamaraty, afirma-se que “*Brasil e EUA discutiram novos temas, como economia digital e 5G. O Brasil apoia os princípios contidos na proposta do Clean Network feita pelo EUA, inclusive na Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), destinados a promover, no contexto do 5G e outras novas tecnologias, um ambiente seguro, transparente e compatível com os valores democráticos e liberdades fundamentais*”.

---

<sup>21</sup> <https://www.ectaportal.com/about-ecta/who-are-we>

<sup>22</sup> <https://www.ectaportal.com/news/ecta-press-releases/1306-ecta-warns-against-adverse-consequences-of-a-ban-of-chinese-suppliers-for-eu-welfare-and-5g-deployment>

<sup>23</sup> [https://www.gov.br/mre/pt-br/canais\\_atendimento/imprensa/notas-a-imprensa/visita-do-subsecretario-para-crescimento-economico-energia-e-meio-ambiente-do-departamento-de-estado-dos-eua-keith-krach-ao-brasil-de-9-a-11-de-novembro-de-2020](https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/visita-do-subsecretario-para-crescimento-economico-energia-e-meio-ambiente-do-departamento-de-estado-dos-eua-keith-krach-ao-brasil-de-9-a-11-de-novembro-de-2020)

### **Panorama atual - fornecedores das operadoras brasileiras**

Nesse contexto, torna-se importante avaliar os fornecedores de equipamentos das atuais operadoras brasileiras. Essas empresas de telefonia móvel contam com redes 4G com equipamentos de vários fabricantes<sup>24</sup>, conforme a seguir:

- **Vivo** - Ericsson responde por boa parte da implementação de sua rede (a Huawei ficou com uma fatia menor);
- **Oi** - Alcatel-Lucent, Ericsson e Nokia Siemens;
- **Claro** - Ericsson e Huawei;
- **TIM**<sup>25</sup> - Huawei, Ericsson<sup>26</sup> e Nokia<sup>27</sup>.

Como se pode observar, a Huawei já está presente na rede de infraestrutura de 4G de operadoras brasileiras, sobretudo Vivo e Claro. E isso é o que levou o vice-presidente da República, Hamilton Mourão, a declarar que excluir a empresa chinesa do mercado brasileiro é “difícil”.

*“A Huawei já está aqui. A Huawei já está há mais de 10 anos aqui no Brasil. Parte da nossa rede de 4G usa os equipamentos da Huawei. As nossas operadoras não podem da noite para o dia simplesmente retirar isso”* afirmou o vice-presidente<sup>28</sup>.

### **Como restringir a tecnologia de um determinado fornecedor?**

Vislumbramos 5 (cinco) possibilidades para que o Poder Executivo possa evitar a participação de um determinado fornecedor na implantação das redes de telefonia 5G.

<sup>24</sup> <https://www.telesintese.com.br/4g-mobiliza-fabricantes-tradicionais-e-novos-players/>

<sup>25</sup> <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&UserActiveTemplate=mobile%252Csite&inoid=44216&sid=17#.X1QCQ3IKgdV>

<sup>26</sup> <https://economia.estadao.com.br/noticias/negocios,tim-define-fornecedores-de-infraestrutura-para-4g,132849e>

<sup>27</sup> <https://www.telesintese.com.br/tim-anuncia-fornecedores-para-expansao-da-rede-movel/>

<sup>28</sup> <https://www.minhaoperadora.com.br/2020/07/banir-huawei-no-brasil-e-dificil-diz-mourao.html>

1. **Editais dos leilões de frequência** - os leilões de frequência que serão feitos pela Anatel em 2021 terão a participação das operadoras de telecomunicações (Oi, Vivo, TIM e Claro), sendo que as empresas fornecedoras de tecnologia, como a Huawei, Ericsson ou Nokia, não participam diretamente. Entretanto, tendo em vista que muitos equipamentos de cada fabricante contam com tecnologias patenteadas<sup>29</sup>, o que pode complicar a vida de um ou mais fornecedores específicos de infraestrutura são as especificações das tecnologias previstas nos editais de licitação de frequências que serão feitos em 2021. Caso o Edital estabeleça definições precisas de tecnologias e requisitos tecnológicos, por exemplo, apontando para tecnologias patenteadas, e não licenciadas, por um fornecedor ou um consórcio de fornecedores, essa definição dificultaria a entrada no mercado de uma determinada empresa (como a Huawei, por exemplo).
2. **Conselho de Defesa Nacional.** Uma outra possibilidade de restrição de uma determinada empresa seria por intermédio do **Conselho de Defesa Nacional** o qual tem competência, segundo artigo 1º, alínea “d)” da Lei nº 8.183, de 11 de abril de 1991<sup>30</sup>, combinado com art. 6º da mesma lei, para “*propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do estado democrático*”, solicitando, para isso, que “*os órgãos e as entidades de Administração Federal*” realizem estudos, emitam pareceres prestem toda a colaboração de que o Conselho de Defesa Nacional necessitar.

---

<sup>29</sup>

<https://on5g.es/wp-content/uploads/2020/06/AAFF-Informe-de-estandarizacio%CC%81n-y-despliegue-de-5G.pdf>

<sup>30</sup> [http://www.planalto.gov.br/ccivil\\_03/LAIS/L8183.htm](http://www.planalto.gov.br/ccivil_03/LAIS/L8183.htm)

3. **Proibição de importação.** Vislumbramos, ainda, uma terceira hipótese, que seria por intermédio de uma proibição direta de importação. Isso poderia ser implementado mediante uma recomendação apropriada (por exemplo, do Conselho de Defesa Nacional, baseada na segurança territorial brasileira, da qual a rede de telecom é um elemento). O Poder Executivo poderia inserir um dispositivo no Regulamento Aduaneiro, Decreto 6759/2009<sup>31</sup>, vedando a entrada de equipamentos de telecomunicações de certas classificações oriundos da China ou lá produzidos, ou de determinados fornecedores. Esta última seria uma alternativa mais simples, pois dispensa mexer nos editais de licitação, e não exige Lei ou MP específica, e pode ser estendida a outras marcas chinesas com simplicidade.
4. **A Instrução Normativa GSI nº 4, de 26 de março de 2020**<sup>32</sup>, acima mencionada já aponta os primeiros elementos para impedir que equipamentos de empresas que tenham “backdoors” sejam adotados nas redes de comunicação 5G no Brasil.
5. O Decreto nº 10.569, de 9 de dezembro de 2020<sup>33</sup>, que aprova a “**Estratégia Nacional de Segurança de Infraestruturas Críticas**”. Esta legislação tem caráter principiológico e genérico, mas pode vir a sustentar intervenção do Estado em operadores de infraestruturas consideradas críticas - energia, transportes, águas, finanças e comunicações (o termo “comunicações”

---

<sup>31</sup>

[http://www.planalto.gov.br/ccivil\\_03/\\_ato2007-2010/2009/decreto/d6759.htm#:~:text=DECRETO%20N%C2%BA%206.759%2C%20DE%205.que%20lhe%20confere%20o%20art.](http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/decreto/d6759.htm#:~:text=DECRETO%20N%C2%BA%206.759%2C%20DE%205.que%20lhe%20confere%20o%20art.)

<sup>32</sup>

<https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-4-de-26-de-marco-de-2020-25005946&>

<sup>33</sup>

[http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/decreto/D10569.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm)



congrega telecomunicações, radiodifusão e Internet). Há referência a um futuro “Plano Nacional de Segurança de Infraestruturas Críticas”, que ainda será elaborado. O texto suscita preocupações no setor privado com aumento de interferência do Estado em aspectos operacionais de empresas, conforme artigo do Teletime de 11/12/2020 - “Estratégia para infraestruturas críticas: intervencionismo no 5G?”<sup>34</sup>

### <sup>35</sup>Legislação estrangeira

Neste tópico abordamos os instrumentos legais adotados na Inglaterra e Austrália para banir a Huawei das redes 5G de seus países.

#### **Inglaterra**

Na Inglaterra a medida de proibição da Huawei será implementada por meio da aprovação de um Projeto de Lei sobre segurança de telecomunicações - Telecoms Security Bill - no âmbito do Parlamento britânico, conforme comunicado (*oral statement*) oficial do Secretário para Assuntos Digitais, Cultura, Media e Esportes do Reino Unido, Sr. Oliver Dowden, em 14 de Julho de 2020<sup>36</sup>.

Quando esse Projeto de Lei for aprovado, todas as operadoras de telecomunicações do Reino Unido não poderão mais comprar equipamentos da Huawei, com efeitos a partir de 31 de dezembro de 2020. No cronograma do governo britânico, até 2027 todos os equipamentos Huawei serão eliminados da rede 5G da Inglaterra.

O comunicado oficial do Secretário foi feito após decisão do Conselho de Segurança Nacional (NSC) do governo britânico, em reunião

---

<sup>34</sup>

<https://teletime.com.br/11/12/2020/estrategia-para-infraestruturas-criticas-intervencionismo-no-5g/>

<sup>35</sup> [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/decreto/D10569.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm)

<sup>36</sup>

<https://www.gov.uk/government/speeches/digital-culture-media-and-sport-secretarys-statement-on-telecoms>

presidida pelo primeiro ministro - Boris Johnson - em resposta às sanções americanas impostas em maio de 2020, e também baseada em um relatório técnico da NCSC (*National Cyber Security Centre*)<sup>37</sup>, apontando o risco para o Reino Unido dos equipamentos da Huawei.

### ***Austrália***

Em agosto de 2018 o governo australiano proibiu a Huawei de fornecer tecnologia 5G para redes sem fio do país. Além disso, a fabricante chinesa ZTE também foi proibida - ambas por motivos de segurança nacional.

O governo australiano alterou as recomendações de segurança nacional, estendendo para os fornecedores de equipamentos os mesmos requisitos que já eram estabelecidos para as operadoras (empresas de telecomunicações). Dessa forma, a nova diretriz do governo australiano estabeleceu que as empresas que "provavelmente estarão sujeitas a ordens extrajudiciais de um governo estrangeiro" podem representar um risco de segurança.

A implementação legal da diretriz foi feita, conforme comunicado do poder executivo<sup>38</sup>, por intermédio de uma emenda na subseção 315 da Lei de Telecomunicações de 1997, a qual já tinha sido alterada por uma Reforma de Segurança do Setor de Telecomunicações de 2017, conhecida como TSSR. Essa nova diretriz adentrou ao ordenamento australiano por meio de uma emenda adicional ao TSSR<sup>39</sup>.

---

<sup>37</sup> <https://www.ncsc.gov.uk/information/huawei-advice-what-you-need-to-know>

<sup>38</sup> <https://www.homeaffairs.gov.au/nat-security/files/tssr-annual-report-2018-19.pdf>

<sup>39</sup> <https://www.legislation.gov.au/Details/C2017A00111>

### 315A Direction if use or supply of carriage services prejudicial to security

(1) If:

- (a) a person who is a carrier or carriage service provider proposes to use, or uses, for the person's own requirements or benefit, or proposes to supply, or supplies, to another person, one or more carriage services; and
- (b) the Attorney-General, after consulting the Prime Minister and the Minister administering this Act, considers that the proposed use or supply would be, or the use or supply is, as the case may be, prejudicial to security;

the Attorney-General may give the carrier or carriage service provider a written direction not to use or supply, or to cease using or supplying, the carriage service or the carriage services.

### **Possibilidades de atuação do Congresso Nacional para impedir a proibição de uma determinada empresa**

Para evitar um direcionamento da tecnologia 5G exclusivamente por parte do Poder Executivo, poderiam ser estudadas medidas legislativas para impedir uma atuação discricionária, como as seguintes:

- Alterar a Lei nº 9.472, de 1997 - Lei Geral de Telecomunicações (LGT)<sup>40</sup> - para determinar que os leilões de frequência não criem óbices para que os atuais fornecedores de infra-estrutura sejam excluídos do mercado;
- Alterar a LGT para determinar que os leilões de frequência não impeçam que infra estruturas atuais de rede 4G que podem ser aproveitadas nas novas redes de 5G tenham que ser substituídas;
- Alterar a LGT para obrigar que os editais de licitação sejam submetidos à aprovação prévia do Congresso Nacional; entretanto, esta é uma alternativa de difícil implementação e de elevado risco de questionamento judicial;

<sup>40</sup> [http://www.planalto.gov.br/ccivil\\_03/leis/l9472.htm](http://www.planalto.gov.br/ccivil_03/leis/l9472.htm)

- Os editais de leilões de frequência e/ou os regulamentos de homologação de equipamentos poderiam adotar requisitos de Open-RAN (arquitetura aberta e intercambiável de redes de acesso)<sup>41</sup>, caso essa arquitetura venha a se consolidar no mercado;
- Estabelecer critérios mais rígidos para eventuais intervenções sob a argumentação de “segurança nacional”.

Consultoria Legislativa, em 15 de janeiro de 2021.

Fabio Luis Mendes  
Consultor Legislativo

2020-12204

---

<sup>41</sup> <https://www.o-ran.org/>