BIGS

BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

O CUSTO OCULTO DE FORNECEDORES NÃO-CONFIÁVEIS EM 5G

ESTADO DA DISCUSSÃO E ESTIMATIVAS PARA PORTUGAL

Carlos Oliveira

Dezembro 2020

Contacto do autor:

Carlos E.F. Oliveira

E-mail: carlos@nomadriver.co

Este estudo foi comissionado pelo Departamento de Estado dos Estados Unidos da América. As opiniões, descobertas e conclusões aqui explanadas são dos seus autores e não refletem necessariamente as do Departamento de Estado dos EUA.

Tabela de Conteúdos

Sumário Executivo

Num mercado não regulamentado, os fornecedores não confiáveis podem ter uma vantagem quando os operadores de redes móveis (MNOs) se concentram primariamente numa estratégia de preços orientada para ganhos a curto e médio prazo.

Apesar de se esperar que o quadro regulamentar português para 5G evolua de forma bastante drástica durante 2021, à data de hoje não existem restrições significativas impostas aos Prestadores de Serviços de Comunicação (CSPs), no que respeita à adopção de fornecedores potencialmente não confiáveis para as suas redes (infraestrutura central ou respectivo acesso rádio). A democratização das regras em Portugal, com a entrada em cena de novos operadores e a instalação dos seus próprios equipamentos, pode também vir a impactar a situação quanto à segurança dos dados e das pessoas, assim não se considere necessário que seja efectuada qualquer intervenção regulamentar.

Apesar da dimensão relativamente pequena da economia portuguesa, em relação às congéneres europeias analisadas no estudo-pai deste estudo de país, uma grande parte do PIB está em jogo devido a estas intervenções, e a escala dos custos óbvios e ocultos de fornecedores não-confiáveis poderia representar desafios significativos para o tecido económico português.

Propomos que os custos de remoção de fornecedores não confiáveis das redes portuguesas, como proposto por estudos anteriores, não são tão significativos como os custos acima mencionados, de acordo com a nossa própria investigação, e outras recentes, e são relativamente pequenos quando comparados com os nossos cenários realista e catastrófico para infraestruturas comprometidas.

Os intervenientes portugueses incorrem em risco moderado a elevado, num ambiente volátil, de incorrer em custos ocultos com fornecedores não confiáveis em 5G.

Introdução e Estado do Debate (a 31 de Outubro de 2020)

A introdução do 5G em Portugal, tal como no resto do mundo, tem sido alvo de grandes expectativas pelo seu impacto transformador na inovação e nas paisagens económicas do país. Contudo, o desenvolvimento não tem passado incólume e tem tido a sua quota-parte de controvérsia e debate público.

A ambição era elevada no início do processo. O regulador nacional abriu uma quantidade recorde de espectro disponível para leilão, e expandiu o mercado nacional a novos operadores. Liberalizaram-se muitos dos aspectos competitivos do sector das telecomunicações português, criando-se assim as condições para que 5G florescesse, com o aparecimento de novas redes e operadores públicos e privados. No entanto, gerou-se um campo de batalha legislativo e legal entre o regulador nacional e os CSPs incumbentes, que acreditam estar a ser tratados injustamente e exigem igualdade de condições no novo panorama competitivo.

Estes desafios vêm lado a lado com a introdução, em toda a UE, da Toolbox da UE de Medidas de Mitigação de Riscos, que Portugal considerou como um factor chave para os seus planos (ainda a disponibilizar publicamente) de implantação de 5G e respectivas contramedidas de cibersegurança. Isto à luz dos bem conhecidos e reconhecidos vetores de ameaça associados à massificação de dispositivos de acesso e utilizadores finais, ecossistemas complexos de fornecedores com implicações geopolíticas, e à natureza interconectada e imprevisível das redes baseadas em software e novas configurações de acesso via rádio, nas quais se fundem iniciativas públicas e privadas.

O governo português declarou que irá legislar em total alinhamento com as medidas a nível da UE[1] e que irá pôr em vigor regulamentação para certificar e autenticar os fornecedores no panorama nacional 5G. Estes compromissos ainda não se concretizaram, apesar do leilão estar à data, em curso. Este relatório analisa o estado atual do debate, os custos óbvios e ocultos da introdução de fornecedores potencialmente não confiáveis, e o impacto da sua participação na rede.

Em 2011, o leilão da 4G em Portugal viu os Operadores de telecomunicações investir 372M EUR em tecnologia 4G LTE.[2] Estes operadores eram TMN (agora Altice MEO), Optimus (agora NOS) e Vodafone. Isto ficou abaixo da expectativa do Estado português de vender todo o espectro leiloado com um orçamento total de 429 milhões de euros. A tabela abaixo mostra a última atribuição a cada operador.

Operador	***Downlink***		***Uplink***		**Largura de banda (MHz)**	**Tecnologia**
MEO	791,000	801,000	832,000	842,000	800	Neutro Técnico
MEO	950,900	958,900	905,900	913,900	900	LTE
MEO	1845,000	1865,000	1750,000	1770,000	1800	LTE
MEO	2149,900	2169,700	1959,900	1979,700	2100	UMTS
MEO	2670,000	2690,000	2550,000	2570,000	2600	Neutro Técnico

[1] https://www.anacom.pt/render.jsp?contentId=1507487

[2] https://www.dinheirovivo.pt/especial/vodafone-business-conference/anacom-massificacao-e-custos-de-equipamentos-serao-determinantes-no-5g-12778288.html

https://expresso.pt/economia/2020-03-06-Huawei-nao-vai-integrar-o-nucleo-da-rede-5G-em-Portugal

NOS	811,000	821,000	852,000	862,000	800	Neutro Técnico
NOS	943,100	950,900	898,100	905,900	900	LTE
NOS	1825,000	1845,000	1730,000	1750,000	1800	LTE
NOS	2130,100	2144,900	1940,100	1954,900	2100	UMTS
NOS	2650,000	2670,000	2530,000	2550,000	2600	Neutro Técnico
Vodafone	801,000	811,000	842,000	852,000	800	Neutro Técnico
Vodafone	930,000	935,000	885,000	890,000	900	LTE
Vodafone	935,100	943,100	890,100	898,100	900	LTE
Vodafone	1805,000	1825,000	1710,000	1730,000	1800	LTE
Vodafone	2110,300	2130,100	1920,300	1940,100	2100	UMTS
Vodafone	2570,000	2595,000			2600	Neutro Técnico
Vodafone	2630,000	2650,000	2510,000	2530,000	2600	Neutro Técnico

Em 2020, para o leilão 5G, o governo espera poder leiloar 237,9 milhões de euros, com 58 bandas de frequência disponíveis, mas com muitas frequências ainda a serem libertadas de outros serviços, ou ainda ao abrigo de acordos de licenciamento anteriores.

Há também uma diferença fundamental no leilão de 2020. A consulta pública original teve 505 comentadores, o que, juntamente com o impacto da COVID-19, levou a atrasos no processo de leilão que, no entanto, deverá estar concluído até ao final do 1º trimestre de 2021. Muitos destes comentários dizem respeito à abertura do processo a novos participantes, que podem reservar espectro e aceder ao roaming nacional, com o objectivo de aumentar a competitividade no mercado de telecomunicações. Qualquer novo operador será sujeito a cobrir 25% a 50% da população nacional, 3-6 anos após a compra do espectro, e a garantir que as suas ofertas de banda larga suportam pelo menos 30Mbps de débito de descarregamento. A acompanhar isto, as novas regras também formularam a necessidade de assegurar serviços compatíveis com 5G a hospitais, universidades, parques industriais, portos, aeroportos e instituições militares, seja com infraestruturas próprias, infraestruturas partilhadas ou recorrendo à oferta OEM.

Inicialmente, a linha temporal portuguesa para a implantação de 5G deveria ter pelo menos 2 cidades cobertas pela infraestrutura até ao final de 2020. Isto estender-se-ia a todos os principais municípios, hospitais, universidades, institutos de investigação e outros locais-chave até ao final de 2023, e a 90% da população até ao final de 2025. Atualmente, o plano é que o leilão tenha lugar em Dezembro de 2020 e que todos os procedimentos de aquisição sejam finalizados no 1º trimestre de 2021, adiando todas as outras datas, e também adiando as decisões críticas que têm de ser tomadas em torno da aquisição de fornecedores.

Além disso, o atual procedimento de leilão ainda está sob litígio por parte dos três operadores-chave, que argumentam que os novos operadores irão beneficiar indevidamente de condições especiais e prejudicar a competitividade do mercado. O regulador português ANACOM, por outro lado, afirma estar a fazer isto para aumentar a competitividade e combater a base de clientes amplamente estabelecida dos operadores históricos.

Apesar destes atrasos nos quadros regulamentares e no guião de implementação 5G, os três grandes operadores Telco já declararam que não utilizarão Huawei na infraestrutura central da rede. Isto apesar do facto de não ter havido uma decisão clara do governo português sobre se haverá uma proibição do fornecedor chinês de equipamento de rede, apesar da pressão da Comissão Europeia para salvaguardar a infraestrutura nacional 5G.

A Vodafone declarou que irá utilizar equipamento Ericsson, um parceiro de longa data, enquanto a NOS (que se diz ser parceira da Nokia) e a Altice (que se diz estar a adquirir uma implementação de rede de base baseada na CISCO) declararam publicamente que irão evitar a Huawei no núcleo. No entanto, os MNOs não declararam que tipo de protocolos para as suas redes de acesso rádio serão aplicados para a aquisição de fornecedores (e que fornecedores).

Recentemente, o Subsecretário de Estado dos EUA e a Embaixada dos EUA em Portugal declararam que preferiam que Portugal não incorporasse qualquer equipamento Huawei na sua rede 5G, particularmente por serem ambos membros da NATO e trocarem regularmente informações classificadas. O governo português, na sua resposta, não se comprometeu, contudo, a fazê-lo para lá da execução de eventuais acordos à escala da UE (como a Toolbox, acima referida) e declarou que quando se tratasse de sistemas que ameaçassem os sistemas de segurança ou defesa nacionais, os seus critérios de avaliação deveriam salvaguardar estes requisitos contra actores mal intencionados.

A [7] de Fevereiro de 2020, o governo português mandatou a criação de uma taskforce dentro do seu CSSC (*Conselho Superior de Segurança do Ciberespaço*), que será responsável pela avaliação e assistência a:

1) Implementação e operacionalização da Toolbox da UE, para medidas de mitigação de riscos.
2) Rever periodicamente os riscos de cibersegurança que afectam as redes 5G e ajudar na avaliação dos referidos riscos a nível da UE.
3) Elaborar um relatório que descreva as acções e o guião necessários para a cibersegurança e medidas auxiliares.
    a. Embora conste que este relatório já foi disponibilizado ao governo, não foi tornado público, e foi na realidade categorizado como classificado,[3] apesar da pressão parlamentar para a sua divulgação. A única recomendação pública é a que está por detrás do comentário acima referido. A imprensa portuguesa relata que a posição actual do governo é que a segurança das redes deve ser promovida pela certificação e aprovação do equipamento, e não pela exclusão de fornecedores. Esta exclusão pode, contudo, acontecer como parte da referida atividade de certificação e aprovação, bem como da atividade contínua de avaliação de risco. [4]
    b. Isto alinharia a abordagem portuguesa com parte das recomendações oferecidas no âmbito da Caixa de Ferramentas da UE, mas distanciá-la-ia das medidas empreendidas por alguns dos seus outros homólogos europeus, que impuseram proibições rigorosas aos fabricantes chineses.

[3] https://eco.sapo.pt/2020/09/29/governo-nao-divulga-e-classifica-relatorio-de-risco-do-5g-como-secreto/

[4] https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2020-06-05-governo-portugues-nao-vai-impedir-huawei-ou-qualquer-outra-marca-de-fornecer-tecnologias-5g/

Custos estimados da proibição de fornecedores não confiáveis

No seu "Restricting competition in 5G network equipment throughout Europe", a Oxford Economics afirma que mais de 63 milhões de euros extraordinários teriam de ser gastos anualmente (até 2023) em Portugal como resultado de impedir a Huawei e a ZTE de competir no mercado. Incorrer-se-ia em mais de 1 milhão de euros de custos pelo atraso na implementação de 5G até 2023, e mais de 500 milhões de euros seriam permanentemente perdidos do PIB nacional em resultado destes atrasos. Com 11.900.000 contratos de telemóveis em Portugal, isto traduzir-se-ia num custo adicional de cerca de 5 euros por contrato. Essa perda do PIB, em perspectiva da dimensão global da população, ascenderia a cerca de 49 euros per capita.

Os pressupostos subjacentes às suas curvas (usadas para a base e considerando o cenário pós-COVID) podem e devem ser examinados. Por um lado, estas olham à percentagem da população coberta, e extrapolam os resultados dessa cobertura para os impactos no PIB. A realidade do país é substancialmente diferente, com duas grandes áreas metropolitanas (Lisboa e Porto) que representam cerca de 50% do PIB e as 8 divisões administrativas seguintes que representam cerca de mais 27%. Uma vez que todas estas regiões estão ancoradas em torno das principais áreas metropolitanas, existe um incentivo económico directo para os operadores Telco adquirirem tecnologia e serviços que ajudem a assegurar a implantação da tecnologia 5G a estas populações muito cedo, particularmente com a introdução de concorrentes externos no mercado português, ajudando a regulação a cobrir as restantes atempadamente.

Para além da cobertura da população, os prazos e o *lead time* para cobrir 90% da população não se alinham com os do governo português, sobre os quais se basearão os procedimentos de aprovisionamento para o espectro 5G. Também não são responsáveis pela potencial introdução de novos intervenientes no sector português das telecomunicações, o que aumentaria as pressões competitivas e resultaria numa absorção de mercado acelerada e num aumento do poder negocial por parte dos consumidores.

Outros estudos questionaram desde então estes números, e extrapolaram que muitas das infraestruturas existentes teriam de ser gradualmente eliminadas e substituídas de qualquer forma, pelo que a incrementalidade dos custos não é tão relevante como os estudos da Oxford Economics sugerem. Além disso, o estudo ignora os custos directos, óbvios e ocultos de fornecedores não confiáveis, incluindo os delineados na Toolbox da UE.

Para Portugal, com populações tão fortemente concentradas em poucos distritos, a implantação atingirá rapidamente enormes faixas da população, o que significa que as projecções de perda de PIB não devem ser consideradas tão linearmente. Os atrasos impostos ao leilão e à regulamentação do espectro 5G são certamente a questão sistémica, ao invés da transferência de quota de mercado para fornecedores que, inclusivé, já operam em mercado nacional.

Custos óbvios de fornecedores maliciosos

- **Estimativa de sabotagem / interrupção intencional**

Em Portugal, estima-se que 6,5% do PIB seja perdido a cada 30 dias que a economia permanece parada, de acordo com as estimativas do Ministério das Finanças. Se houver sabotagem intencional ou uma interrupção intencional causada por um fornecedor malicioso, é esta a gama de custos a que a economia estaria sujeita. O Ministério das Finanças também estima que estes custos se deterioram à medida que o tempo avança, de uma forma não linear, com o impacto mensal a crescer mais por cada dia adicional em que a economia é impedida de funcionar normalmente. Com instituições financeiras, governamentais e empresariais tão dependentes das infraestruturas de telecomunicações, existe um risco não negligenciável de depender de redes que estão sujeitas a sabotagem e interrupções. Isto, naturalmente, é incremental às externalidades humanas, ambientais e outras.[5]

- **Estimativas de Choques de Causas Naturais**

O SIRESP, o sistema nacional de comunicação de emergência, mencionado mais tarde na secção sobre Infraestruturas Redundantes, esteve sob grande escrutínio público depois de ter deixado de funcionar durante o Verão enquanto o país estava a ser subsumido pelos incêndios florestais, com perda de terras e vidas. Embora não como resultado de sabotagem, em 2017, enquanto estes incêndios devastaram o país, o SIRESP, responsável por manter a rede em funcionamento e as equipas de emergência em comunicação constante, falhou repetidamente e de forma intermitente. Isto gerou uma situação em que os vários serviços de resposta a emergências foram incapazes de se coordenar de forma segura e atempada, e tiveram de recorrer a redes externas e protocolos *ad-hoc*, com os custos resultantes estimados em mais de 613 milhões de euros. Isto reflecte o volume de danos externos potenciais que podem resultar da incapacidade de coordenação em situações de emergência, devido a falhas de rede. [6]

- **Estimativas de Choques de Greve**

Em 2019, uma greve do sindicato dos condutores de camiões de materiais perigosos (incluindo petróleo e gases) paralisou o país durante dias. As estimativas apenas para a indústria alimentar situam os prejuízos causados pela greve em 21 milhões de euros por dia, para este sector primário, uma indicação da medida em que uma falha de um sector infraestrutural afecta a economia como um todo. [7]

Custos ocultos de fornecedores não confiáveis

Centros de teste - Centros de avaliação e certificação de hardware, software e funcionamento de rede 5G

Mesmo as redes 5G de confiança são vulneráveis a ataques e subversão. Os governos mais prudentes desejarão sempre certificar as infraestruturas de telecomunicações e as cadeias de

[5] https://www.jornaldenegocios.pt/economia/detalhe/centeno-queda-do-pib-e-de-65-por-cada-30-dias-uteis-com-economia-parada

[6] https://www.sabado.pt/portugal/detalhe/os-custos-associados-ao-incendio-de-pedrogao-grande

[7] https://www.publico.pt/2019/08/05/economia/noticia/portugal-fresh-estima-prejuizo-diario-21-milhoes-impacto-greve-1882443

fornecimento de forma independente para mitigar as vulnerabilidades. Como as redes e a tecnologia são hoje em dia tão complexas, a tarefa de certificação está cada vez mais para além da capacidade dos MNOs. Os fornecedores não confiáveis aumentam substancialmente o custo destas actividades, uma vez que os testes terão de ser feitos sem a cooperação do fornecedor, exigindo um escrutínio mais amplo e minucioso, e o desenvolvimento de um banco de ensaios e de redes digitais "gémeas" para se compreenderem em detalhe os cenários em que a rede física poderá ser exposta. Em Portugal, a criação de um centro de testes deste tipo poderia custar até 20 milhões de euros. Esta estimativa colocaria o Centro de Testes Português na proximidade do custo anual de outros centros de I&D de referência no país, como o INESCTEC.

Custos regulatórios

Em Portugal, foi criada a UTAIL (Unidade Técnica de Impacto Legislativo) para examinar os custos de regras e legislação, uma vez provinda de mandatos parlamentares e inscrita na lei. Desde a sua criação inicial em 2017, a unidade detectou que algumas introduções regulamentares teriam um impacto na ordem dos 20 a 30 milhões de euros no caso de serem aprovadas. Existe, evidentemente, um custo associado a este controlo, à realização e à operacionalização dos procedimentos legislativos, que deve ser tidos em conta ao considerar a introdução de fornecedores não confiáveis. Haverá também um custo para os quadros legislativos, que ainda será trazido à peça, como resultado do cumprimento da Toolbox da UE, especialmente se for concedida autorização para que fornecedores potencialmente não confiáveis possam operar. [8]

Um regulamento recente que foi submetido ao escrutínio da UTAIL é o RGPD.[9] Olhando para o impacto que o regulamento teria nas empresas de todas as dimensões, o custo total do regulamento para Portugal foi estimado em 126 milhões de euros. Isto abarca novas medidas de protecção de dados, contratação de recursos humanos e implementação de processos adequados para o cumprimento da legislação. No caso das empresas terem de adoptar e reforçar as suas medidas de protecção de dados para se protegerem contra o perigo de um intermediário não confiável, não é surpreendente que possam daí advir custos de ordem de grandeza análoga.

Cibercriminalidade e Incidentes com Dados

O CERT, parte do Centro Nacional de Cibersegurança, afirma que, em 2019, foram detectados 62 ataques por mês (um aumento de 29% em relação ao ano anterior).[10] Em 2020, esta tendência aumentou drasticamente à medida que a COVID atingiu o país e uma percentagem muito maior da população se deslocou para teletrabalho.

A tendência é a seguinte:

- 248 em 2015
- 413 em 2016 (aumento de 66% em relação ao ano anterior)
- 501 em 2017 (21%)
- 599 em 2018 (19%)
- 752 em 2019 (26%)
- 2075 em 2020 (176% Q1, reforçado pela COVID)

Mesmo excluindo 2020, a taxa média de crescimento em Portugal tem sido de 33% por ano. Se acrescentarmos 2020, esse número quase duplica para 61%. Se partirmos do princípio que, após a

[8] https://www.dn.pt/portugal/custa-quanto-governo-vai-medir-impacto-das-novas-leis-na-vida-dos-cidadaos-9422655.html

[9] www.jurisapp.gov.pt/media/1109/ail-rgpd.pdf

[10] https://www.cncs.gov.pt/observatorio/relatorios/

COVID, assistiremos a uma estabilização e regressão em relação aos números anteriores (desacelerados), é provável que Portugal continue a crescer acima da média mundial.

Tabela 1 - Número de Incidentes reportados pelo CERT.PT

Ano	2015	2016	2017	2018	2019
Número de incidentes	248	413	501	599	752

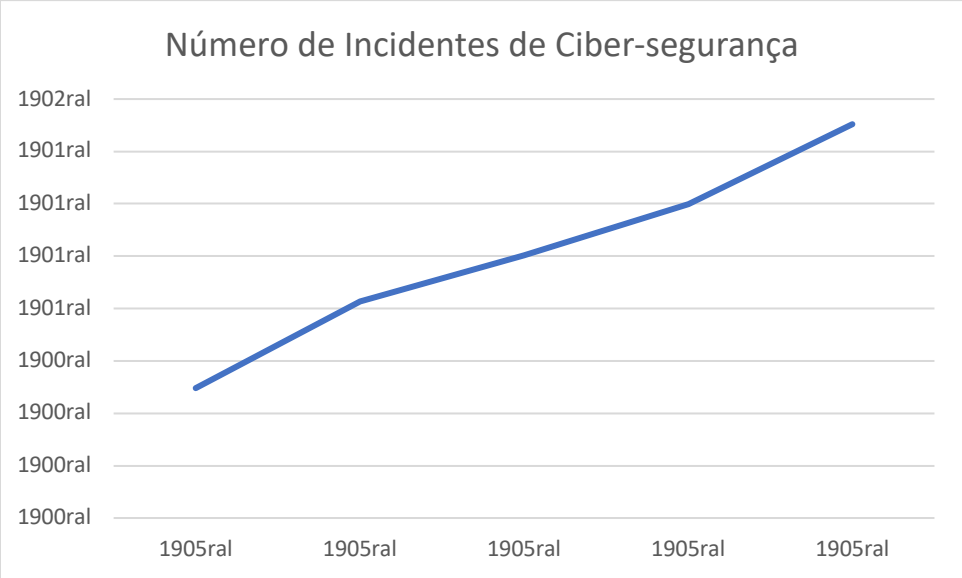


Figura 1: Tendência dos ataques - Portugal

De acordo com o Relatório Anual sobre o Cibercrime,[11] espera-se que o cibercrime tenha uma taxa de crescimento mundial aproximada de 15% por ano até 2025, mesmo após a introdução do 5G (ver Quadro abaixo). As três fases do ciclo de vida dos dados são: ingestão (aquisição dos sensores locais), dados em trânsito e dados em repouso. No entanto, mesmo que uma quebra de dados possa ocorrer em qualquer destas fases, apenas os "dados em trânsito" envolvem 5G. Onde quer que os dados se desloquem, medidas eficazes de protecção de dados para o trânsito de dados são críticas, uma vez que os dados são muitas vezes considerados menos seguros enquanto em movimento.

Portanto, da taxa de crescimento mundial aproximada de 15% por ano até 2025, podemos estimar um aumento percentual aproximado de 5% para a fase "dados em trânsito" (dividindo as percentagens linearmente entre as várias fases do ciclo de vida - ver Quadro 1). Para Portugal, podemos assumir que estas percentagens são ligeiramente mais elevadas, uma vez que o volume de ataques está a crescer praticamente ao dobro da média mundial.

Tabela 1: Estimativa do aumento do Cibercrime em Portugal.

	2021	2022	2023	2024
Aumento anual estimado da cibercriminalidad	33%	33%	33%	33%

[11] https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

e em Portugal (aumento linear)				
Aumento anual do cibercrime para a fracção "dados em trânsito"	11%	11%	11%	11%

Custo de uma violação de dados

Um relatório da IBM indica que o tempo médio que uma empresa italiana levou em 2019 para identificar e conter uma infracção foi de 283 dias. Embora não sejam oferecidos dados sobre Portugal, as indústrias TIC de ambos os países representam uma percentagem semelhante do valor acrescentado em relação ao PIB (cerca de 3%).[12] Pode supor-se que existe uma maturidade semelhante em resposta e capacidade entre o tecido económico das empresas de TIC. O mesmo relatório estima o custo por ataque em 3,19 milhões de dólares. Assumindo que o rácio do PIB entre ambos os países se aplica, com a economia portuguesa aproximadamente 12% da sua homóloga italiana, um valor semelhante para Portugal representaria 383K. Em 2020, a aplicação da mesma proporção colocaria o custo médio por violação de dados de Portugal em 424K dólares. O número de violações comunicadas para 2019 foi de 752, enquanto que para 2020 o valor estimado é de 2075.

Tabela 2: Resultados de Portugal.

Média dos resultados de Portugal	2019	2020
Custo total de uma violação [13]	$424k	$383k
Número de violações de dados [14]	752	2075
Tempo para identificar e conter	283 dias	268 dias

O quadro seguinte mostra o custo de uma violação (calculado com a fórmula acima definida) de 2021 a 2024 e o número de violações de dados de 2021 a 2024 (calculado com o mesmo método).

Quadro 3: Aumento do cibercrime global na fracção "dados em trânsito".

Ano	**2021**	**2022**	**2023**	**2024**
Crescimento YoY	*33%*	*33%*	*33%*	*33%*
Custo da violação	**$0.47M**	**$0.52M**	**$0.58M**	**$0.64M**
Quebras por ano	**2303**	**2557**	**2838**	**3150**

[12] https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_sector_-_value_added,_employment_and_R%26D#The_size_of_the_ICT_sector_as_measured_by_value_added

Fracção de uma quebra de dados superior a 5G

O último passo é calcular a fracção de violações de dados que podem ser atribuídas a problemas de segurança com dados em trânsito superiores a 5G. Para esta fracção, utilizamos a estimativa de penetração de 5G em relação ao tráfego global. Em 2023, a penetração de 5G (a percentagem do total de ligações móveis) atingirá uma média de 26%[13] na Europa Ocidental e uma média de 29% em 2024. [14]

*Quadro **4**: Penetração estimada de 5G no tráfego da Europa Ocidental.*

	2022	2023	2024
Penetração estimada de 5G vs tráfego global	26%	26%	29%

O custo de uma infracção relatada no Quadro 3 refere-se exclusivamente à parte do tráfego "dados em trânsito", enquanto a soma total dos dados inclui também os dados em repouso e os dados em processamento. Para estimar melhor o impacto das violações, tal como serão aplicados ao 5G, os valores do Quadro 3 devem ser ponderados com a fracção de uma violação de dados que pode ser atribuída à rede 5G. Para tal, veja-se o Quadro 5 (ou seja, violações especificamente atribuídas a problemas de segurança com dados em trânsito em 5G).

Finalmente, temos de estimar a parte de uma violação de dados que acontece, em média, durante o "dados em trânsito", numa rede 5G controlada por um dispositivo "não confiável". Para este último passo, é necessário calcular a percentagem de dependência dos operadores de telecomunicações em fornecedores não confiáveis. Como as entrevistas mostram, em Itália, a dependência dos operadores de telecomunicações de fornecedores não confiáveis é apenas parcial.

Uma estimativa recente relata que a percentagem de dependência dos operadores de telecomunicações de fornecedores não confiáveis deverá ser, em média, de 8% em 2022. Assumimos uma taxa de obsolescência de 10%, com os fornecedores europeus a assumirem a responsabilidade pelas substituições.

Quadro 5: percentagem de dependência do tráfego não confiável

% de dependência do tráfego não confiável apenas para 5G		
2022 [7]	**2023**	**2024**

[13] E. Qi, "As ligações móveis 5G atravessarão o marco de 1,7 biliões em 2023," 23 07 2020. [Online]. Disponível: https://www.counterpointresearch.com/5g-mobile-connections/.

[14] [5] C. Donkin, "ligações 5G para atingir 1.5B até final de 2024 - Ericsson," 27 11 2018. [Online]. Disponível: https://www.mobileworldlive.com/featured-content/home-banner/5g-connections-to-hit-1-5b-by-end-2024-ericsson.

8.9 %	*8.0%*	*8.0%*
Obsolescência % por ano	10%	

Cenários de custos

O cenário relatado abaixo descreve uma situação em que todos os dispositivos não confiáveis numa rede 5G recebem comandos para cometer uma violação de dados e exfiltração de dados. Nesta situação, a parte de uma violação de dados que é atribuída à parte não confiada de uma rede 5G pode ser calculada da seguinte forma:

$$pca_t^{br\ 5G\ ctry} = \left(c_{t-1}^{br\ ctry} * \frac{1}{3} * r_t^{cc\ ctry} + c_{t-1}^{br\ ctry}\right) * \sum_{mno=1}^{n} \left(dsh_t^{mno\ ud\ ctry} * msh_t^{mno\ m\ ctry}\right) * \left(pen_{t-1}^{5G\ ctry} * \left(1 - obs_t^{5G\ ctry}\right)\right) * n_t^{br\ ctry}$$

sendo

$pca_t^{br\ 5G\ ctry}$ = porção estimada dos custos agregados das violações de dados, devido a problemas de segurança de 5G, no respectivo país no período de tempo ano t

$c_{t-1}^{br\ ctry}$ = custo total de uma infracção, no respectivo país no período de tempo ano t-1 (ano passado)

$r_t^{cc\ ctry}$ = aumento da cibercriminalidade, no respectivo país no período de tempo ano t

$dsh_t^{mno\ ud\ ctry}$ = % de dispositivos não fiáveis 5G activos nas operadoras, no respectivo país no período de tempo ano t

$msh_t^{mno\ m\ ctry}$ = quota de mercado do operador no respectivo país, no respectivo país no período de tempo ano t

$caneta_{t-1}^{5G\ ctry}$ = estimativa de penetração de 5G vs tráfego global, no respectivo país no período de tempo ano t-1 (ano passado)

$obs_t^{5G\ ctry}$ = obsolescência % dos terminais 5G existentes (taxa de substituição, no respectivo país no período de tempo ano t

$n_t^{br\ ctry}$ = número total de infracções, no respectivo país no período de tempo ano t

t = período de tempo, ano de consideração

resultando em:

Quadro 6: parte estimada do custo para os clientes de uma (única) violação de dados, devido a problemas de segurança de 5G (cenário realista)

2022	2023	2024
$0.046M	$0.046M	$0.052M

Quadro 7: parte estimada do custo para os clientes de uma (única) violação de dados, devido a problemas de segurança de 5G (cenário realista) - conversão para €

2022	2023	2024
€96.72M	107,25MM	€132.65M

Quantificação da ordem de grandeza das perdas potenciais

Uma **segunda abordagem** a ser considerada é pensar nos **custos em termos da ordem de grandeza dos diferentes eventos** (casos) contra uma escala logarítmica. Esta escala ajuda a diferenciar melhor quatro cenários - abaixo - de acordo com a sua gravidade, e a mostrar melhor as diferenças muito importantes entre eles.

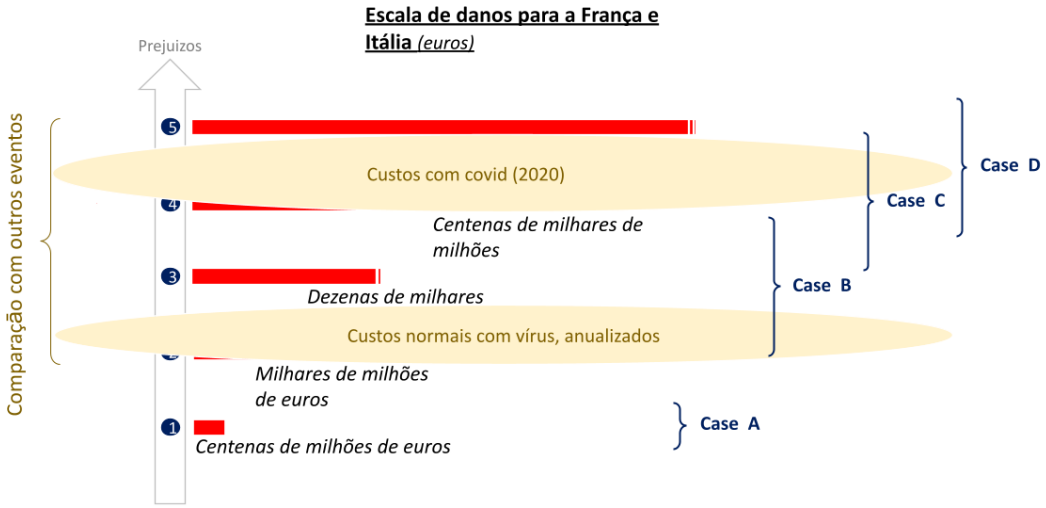
Caso A - Um bloqueio completo e definitivo de 100% das infraestruturas de telecomunicações de um MNO, causando um blackout de chamadas telefónicas pessoais e comerciais, SMS, MMS, & serviços de Internet móvel.

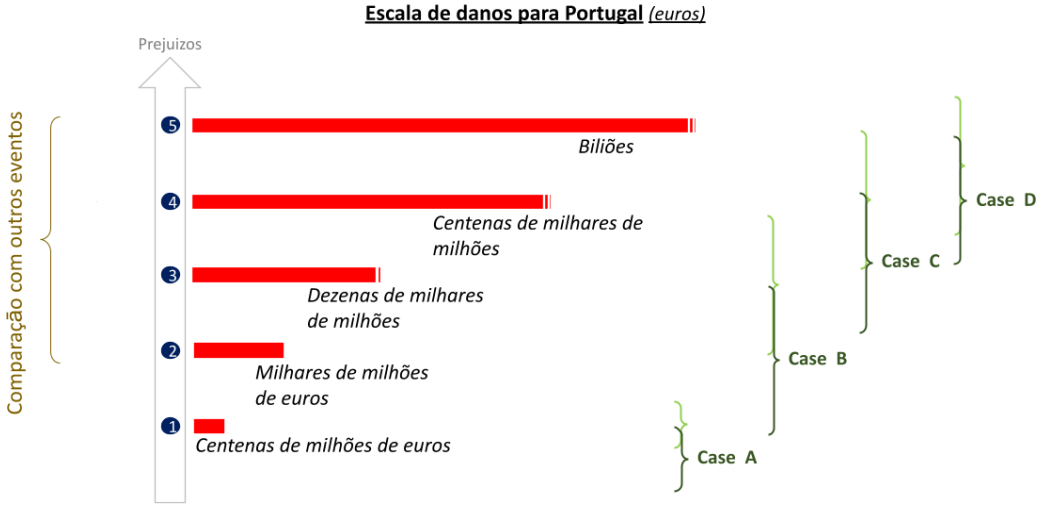
Caso B - O bloqueio também afecta IoT, usos industriais (Fábrica 4.0....), ou veículos de comunicação.

Caso C - Para além de A e B, há um ataque a dados, programas e software (propriedade de pessoas, empresas, associações, administrações) através da infraestrutura 5G fornecida por um fornecedor, resultando na sua destruição definitiva, encriptação ou inacessibilidade.

Caso D - Para além do caso C há também falsificação destes dados, programas e software, causando acidentes automóveis, ferroviários ou marítimos, acidentes domésticos, e desastres médicos e industriais.

Como economias de dimensão semelhante, a **França** e a **Itália** são susceptíveis de sofrer perdas semelhantes contra cada um dos casos. Sendo a economia mais pequena do estudo Clean5G, é provável que **Portugal** sofra o menos em termos absolutos, mas não de forma insignificante em relação à sua dimensão (verde escuro vs França em verde claro). Para mais pormenores sobre as premissas por detrás deste cálculo, consulte o estudo de país para a França como base para o cálculo original.





Transferência da procura

Infraestrutura Crítica

A definição oficial de infraestruturas críticas em Portugal é particularmente redutora, circunscrevendo-a à energia e aos transportes - uma definição que o próprio governo disse estar a ser revista para a alinhar ainda mais com outras definições à escala da UE.[15] Os sectores de

[15] https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBAAAAB%2bLCAAAAAAABACzNLYwAgCF3gJVBAAAAA%3d%3d

infraestruturas definidos como constituindo infraestruturas críticas em Portugal (ver ilustração abaixo) contribuíram, em 2017, com cerca de 12% do PIB. [16]

Sector	**Subsector**
Energia	Electricidade
	Petróleo
	Gás
Transportes	Estrada
	Caminho de ferro
	Ar
	Vias navegáveis do interior do país
	Marítimo

Sectores definidos como infraestruturas críticas, tal como adoptados pelo governo português em 2011.

Estes sectores não se reflectem na contabilidade nacional um para um. Ainda assim, é possível derivar valores aproximados para pelo menos alguns deles.

Assumindo que esta proporção se reflecte na estrutura dos clientes do sector das telecomunicações, derivamos que aproximadamente 12% do volume de negócios do sector das comunicações (o sector público e clientes empresariais, e não clientes finais privados) podem mudar, no caso de fornecedores não confiáveis serem mantidos na rede portuguesa 5G. Os clientes de infraestruturas críticas ou mudariam para fornecedores que trabalham exclusivamente com fornecedores de equipamento de rede de confiança, construiriam as suas próprias redes de campus, ou decidiriam mesmo não utilizar a tecnologia 5G de todo (e, em vez disso, operariam a tecnologia 4G/ WLAN), pelo menos em aplicações particularmente sensíveis em termos de segurança.

Embora o primeiro aspecto - dos clientes que mudam de operador - seja antes uma consideração da gestão para os operadores que tomam decisões sobre a sua escolha de fornecedores, enquadra-se na categoria de custos ocultos. A necessidade de construir e operar redes em campus, por outro lado, tem um custo económico - nomeadamente, um efeito de *crowding-out* no investimento e o custo de oportunidade. O terceiro aspecto advém dos ganhos de produtividade perdidos.

O volume de negócios da indústria de serviços de telecomunicações - sem sequer considerar as infraestruturas de telecomunicações e os dispositivos finais - para 2019 em Portugal está estimado em 3,55 mil milhões de euros. Destes, os serviços de telecomunicações móveis representam cerca de 81% de todas as receitas,[17] uma vez que a maioria está agrupada em pacotes de 2/3/4/5-play, de longe o método de subscrição mais comum no país. Os clientes empresariais representam aproximadamente 28% de todas as receitas. Portanto, os 12% acima mencionados correspondem a um valor absoluto de 97,23 milhões de euros que poderia ser transferido dos actuais MNOs para outros MNOs, redireccionado para redes universitárias, ou investido na manutenção de tecnologia obsoleta mas de confiança e menos eficiente. Os ganhos de produtividade perdidos neste último caso são difíceis de estimar.

[16] https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_cnacionais2010b2016&perfil=392022253&INST=391941652&contexto=am

[17] https://anacom.pt/streaming/SectorComunicacoes2019.pdf?contentId=1530341&field=ATTACHED_FILE

Indústrias intensivas em direitos de propriedade intelectual

Utilizando a mesma metodologia acima referida, se se aplicar a lógica da deslocação da procura das indústrias intensivas em DPI (em vez de infraestruturas críticas), que representam cerca de 42,5% do PIB português, os custos poderiam aumentar até 344,4 milhões de euros.

Total

Um total agregado estimado representaria aproximadamente 48% do PIB. Adoptando os mesmos pressupostos sobre a percentagem de receitas que passariam de operadores de telecomunicações com infraestruturas de fornecedores desconhecidos, isto poderia levar a uma deslocação da procura de até 388,9 milhões de euros.

Infraestrutura Redundante

O SIRESP, uma empresa nacional de serviços de telecomunicações de emergência - que era parcialmente detida pelo governo português (numa parceria com a Altice e a Motorola) - foi recentemente comprada de volta pelo Estado português por 7 milhões de euros. Estima-se que o sistema tenha custado mais de 450 milhões de euros para instalar e gerir até à data. Isto aconteceu depois de terem sido detectados numerosos problemas operacionais que dificultaram a continuação da gestão privada da empresa. Mesmo assim, o governo português ainda paga à Altice e à Motorola 30 milhões de euros por ano para operar e alugar a rede. Um estudo recente aponta os custos da implementação de melhorias de robustez e segurança na rede para um valor superior a 25 milhões de euros, que atualmente consiste de 550 antenas em todo o território nacional. Estes números apontam aos custos significativos de instalação, manutenção e funcionamento de uma infraestrutura deste género, que são ainda significativamente inferiores aos custos de funcionamento de um grande sistema operado por MNOs, para tecido empresarial e consumidores finais. Em particular, os custos associados a uma substituição completa do sistema se for detectado um fornecedor malicioso dentro dos seus limites, podem ser extrapolados para se aproximarem ou serem superiores aos custos associados à instalação e manutenção do mesmo sistema durante os últimos 15 anos de funcionamento.

Resumo e Conclusões

Dependendo da categoria de custos analisados, estimamos custos anuais ocultos de não excluir fornecedores não confiáveis que vão desde 19 milhões de euros para o funcionamento de um centro de testes até mais de 388 milhões de euros para a deslocação da procura das indústrias de DPI e Infraestruturas Críticas, para não mencionar o custo drástico para a economia de um encerramento total como provocado por um cenário de "kill-switch Armageddon". Embora algumas destas possam ser utilizadas apenas uma vez (causando uma reação de *rip-and-replace* por MNOs e reguladores), elas não são mutuamente exclusivas.

O que este estudo ilustra, particularmente no contexto das maiores implicações do *Policy Paper* conjunto, é que mesmo que existam custos associados ao atrasar-se ligeiramente a implementação da infraestrutura 5G, ou à escolha de um fornecedor marginalmente mais caro, os riscos sistémicos e os custos de uma alternativa potencialmente não-confiável são, de facto, bastante maiores.

Portugal ainda não concluiu o leilão 5G e ainda não completou o quadro regulamentar global em torno dos seus requisitos de rede 5G. A Toolbox da UE e as suas recomendações servirão sem dúvida de modelo para a elaboração de políticas em Portugal, mas a determinação com que for aplicada determinará a sua eficácia global. Se olharmos para os exemplos de outros países europeus que

reconheceram estes riscos e tomaram medidas, veremos a importância de tomar decisões rápidas e intransigentes que não só salvaguardem o mercado livre, protegendo os seus actores, mas também adotem uma visão a longo prazo sobre as consequências de não o fazer para a segurança nacional e para a economia europeia.

Nos últimos anos, Portugal viu as suas redes de comunicação seguras falharem em condições críticas, absorveu implicações políticas e societais consideráveis como resultado de violações de dados altamente publicitados, sofreu greves de alto impacto e viu as estatísticas de cibercrime crescerem muito acima da média global - e assim compreende muito bem o impacto da regulação e de processos de contratação pública bem concebidos, para o seu potencial de crescimento. Existem também os custos não monetários, tais como a potencial indisponibilidade dos serviços de inteligência aliados para partilhar informações relacionadas com a segurança, se essas informações corressem o risco de serem tornadas públicas por razões técnicas. Há ainda muito tempo para Portugal dar o exemplo nesta matéria e assegurar o sucesso a longo prazo do seu programa de implementação 5G.

Em conclusão, conseguimos mostrar que os custos totais para a sociedade portuguesa, incluindo externalidades, são mais elevados ao longo do tempo do que as poupanças potenciais que surgem para os operadores de redes móveis quando estes utilizam tecnologia de rede não fiável para implantar 5G. Esta forma de falha do mercado deve ser ultrapassada através de regulação adequada, a fim de realizar plenamente o potencial de crescimento de 5G. Na imagem seguinte, resumimos os custos por categoria, conforme descrito neste estudo de país.