LECA

Law & Economics Consulting Associates

O impacto econômico das leis que enfraquecem a criptografia

Por

George Barker, William Lehr, Mark Loney, and Douglas Sicker

5 de abril de 2021

Email: George.Barker@cleconsult.com

Contato pessoal: Dr George Barker (LECA)

Comissionado pela Internet Society

Revisão por Paulo Rená da Silva Santarém
Tradução por Paulo Rená da Silva Santarém
Supervisão da tradução por Diego Rafael Canabarro

Sumário

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

1. Resumo executivo[1]

Em dezembro de 2018, o Parlamento da Austrália aprovou a *Lei de Alteração das Telecomunicações e de Outras Legislações (de Assistência e Acesso) de 2018* (mais conhecida como LATO,[2] que ampliou a autorização legal das Autoridades e as ferramentas disponíveis ao Estado existentes na legislação para contornar as proteções de dados digitais. A LATO criou uma estrutura pela qual as agências de aplicação da lei e de inteligência, ou Autoridades,[3] podem solicitar ou exigir dos provedores de tecnologia da informação – ou, na terminologia da LATO, Provedores de Comunicação Designados (*Designated Communications Providers*) – que ajudem no acesso ao conteúdo de dados criptografados, o que pode envolver o compartilhamento de informações confidenciais da empresa, ou o desenvolvimento de novas ferramentas.

O foco deste relatório é avaliar as evidências disponíveis sobre o impacto da LATO nas economias australiana e global. Nossa análise nos leva a concluir que a *LATO tem potencial para resultar em danos econômicos significativos para a economia australiana e produzir repercussões negativas que amplificarão esses danos globalmente*. Por significativo, queremos dizer danos econômicos na escala de múltiplos *bilhões de dólares*, generalizados e que provavelmente serão (principalmente) sentidos nos próximos anos.

---

[1] Agradecimento: Somos gratos à Internet Society pelo apoio financeiro para esta pesquisa. As opiniões expressas neste documento, no entanto, e quaisquer erros, são exclusivamente nossos.

[2] Também conhecida como Lei de Criptografia ou Lei de Assistência e Acesso. Ver AUSTRALIA (2018), Registro Federal de Legislação (*Federal Register of Legislation*). Lei de Alteração das Telecomunicações e de Outras Legislações (de Assistência e Acesso) de 2018 ["*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*"], Lei Nº 148 de 8 de dezembro de 2018, "*Uma lei para alterar a legislação relativa às telecomunicações, mandados de acesso a computadores e mandados de busca e apreensão, e outras disposições*" ("*An Act to amend the law relating to telecommunications, computer access warrants and search warrants, and for other purposes*"), disponível em https://www.legislation.gov.au/Details/C2018A00148/Download; [Nota da Tradução 1: optou-se pelo acrônimo LATO em português onde o texto original usa a sigla TOLA, das iniciais de "*Telecommunications and Other Legislation Amendment*")]; [NdT. 2: para facilitar o maior entendimento possível na leitura em português, optou-se por traduzir inclusive apelidos de leis, nomes organizações, bem como títulos de artigos, livros e notícias, etc., mas sempre apresentando as palavras no idioma original em itálico e entre parênteses ou colchete, onde já houvesse parênteses].

[3] O termo Autoridade se refere às agências de aplicação da lei e de inteligência, incluindo as agências governamentais legalmente autorizadas a solicitarem acesso lícito aos dados. [NdT. 3: optou-se pela palavra em português "Autoridade" onde o texto original usa o acrônimo LEIAs, iniciais de *Law Enforcement and Intelligence Agencies*; pela palavra "Provedores" em vez de DCP, sigla adotada no original para resumir a denominação legal *Designated Communications Providers*, a qual no contexto brasileiro indicaria um conjunto maior do que a soma das duas categorias de provedores de conexão e provedores de aplicação, previstas no Marco Civil da Internet, pois abarca também fabricantes de equipamentos eletrônicos e programas de computador utilizados em comunicações digitais; e por "ferramenta" como tradução da palavra *capability*, privilegiando o significado funcional à literalidade de "capabilidade", e a fim de reduzir ruídos com a polissemia dos termos "capacidade" e "recursos"].

Existem vários mecanismos pelos quais a LATO pode gerar danos econômicos. Por exemplo, ela aumenta a incerteza dos negócios. Estudos concluídos pelo Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos em 2001 e 2018 concluíram que as intervenções do governo para reduzir a incerteza sobre a segurança digital resultaram em benefícios agregados de muitos bilhões de dólares.[4] Em sentido contrário, ao aumentar a incerteza entre os participantes do mercado digital quanto às melhores maneiras de proteger dados e informações digitais, a LATO pode significar abrir mão de produzir benefícios análogos.

Em segundo lugar, a LATO pode prejudicar a imagem da marca dos Provedores com operações na Austrália que estejam vulneráveis à ameaça que ela representa para a segurança digital de seus produtos e serviços. Os clientes, incluindo usuários corporativos e de mercado de massa da Internet, preocupados com a possibilidade de seus dados ficarem menos seguros devido à LATO, podem optar por levar seus negócios para outro lugar. Tais respostas podem reduzir as receitas e aumentar os custos operacionais dos Provedores, à medida que eles adotarem estratégias de solução alternativa para contrabalançar as ameaças relacionadas à LATO. Esses efeitos diretos não precisam ser limitados aos Provedores que receberem os avisos da LATO: podem ser também sentidos pelos Provedores em antecipação ao recebimento de uma notificação, ou por outras entidades preocupadas com o impacto da Lei. Essas entidades não precisam se restringir aos Provedores, e podem incluir seus clientes. Em conjunto, esses efeitos diretos e indiretos provavelmente serão generalizados e se acumularão ao longo do tempo, à medida que os efeitos se propagam pela economia.

Terceiro, talvez a maior fonte de efeitos econômicos adversos seja a ameaça indireta que a LATO representa para a confiança nos serviços digitais, incluindo a Internet. Estamos no meio de uma transição global para uma economia digital na qual o comércio eletrônico e as informações digitais em rede desempenham um papel cada vez maior, impactando todos os países, todos os setores e todos os negócios. Se os serviços e redes que oferecem suporte a essa atividade forem confiáveis (por exemplo, os Provedores), as perspectivas de crescimento econômico são prósperas. Espera-se que reduzir a confiança na segurança de dados diminua a demanda agregada em toda a economia digital e induza empresas a assumirem custos mais altos na tentativa de contrabalançar os danos resultantes da redução da confiança.[5] Além disso, como a tecnologia digital é usada em toda a economia, esses efeitos são abrangentes e afetam todos os aspectos de como as empresas modernas operam. Consequentemente, até mesmo pequenas ameaças à segurança cibernética ou, de forma equivalente, à confiança digital, têm o potencial de gerar grandes custos adversos. Um estudo mostra como as ameaças à confiança digital podem se traduzir em danos globais da ordem de um trilhão de dólares ou mais.[6] Medir,

[4] Veja NIST (2015, 2018), discutidos a seguir e referenciados nas Notas 110, 112 *infra*.

[5] Em 2019, 18% dos que não confiam na Internet responderam que fazem menos compras online [ver INTERNET SOCIETY (2019). A Situação da Privacidade do Usuários e da Confiança Online "*The State of User Privacy and Trust Online*"), Centro para Inovação em Governança Internacional ("*Centre for International Governance Innovation*"), Ipsos, junho de 2019, disponível em https://www.internetsociety.org/wp-content/uploads/2019/06/CIGI-Ipsos-Trust-User-Privacy_Report_2019_EN.pdf].

[6] Por exemplo, consulte o estudo do Zurich (2015), Nota 109 *infra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

atribuir e quantificar tal impacto adverso na confiança digital para a LATO não é viável com os dados disponíveis. Além disso, já que esses efeitos ocorrerão majoritariamente nos próximos anos, estimar o impacto depende da formulação de previsões adequadas para o que aconteceria com e sem a Lei. Qualquer uma dessas previsões dependerá de uma ampla gama de suposições de modelagem que provavelmente serão controversas.

Embora possamos identificar múltiplos vetores através dos quais os danos da LATO podem se propagar, as evidências não nos permitem fornecer uma quantificação mais precisa dos prováveis danos econômicos que essa Lei apresenta. As várias razões para isso são discutidas mais detalhadamente no relatório, mas incluem:

- Estimar o impacto econômico da LATO é inerentemente complexo e desafiador. Ela pode gerar impactos econômicos adversos direta e indiretamente de várias maneiras. Alguns são mais fáceis de rastrear e estimar do que outros, mas para capturar todos os efeitos, é importante não se concentrar apenas no que é prontamente observável;

- Até o momento, o uso de LATO foi limitado. Desde sua aprovação, várias análises e várias partes interessadas levantaram preocupações sobre o potencial de ela gerar danos econômicos significativos e pediram emendas para reduzir esse risco. O curto tempo desde a sua aprovação e as preocupações sobre a melhor forma de responder à oposição da LATO podem ser a causa da existência de limitadas evidências empíricas sobre a assunção de custos atribuíveis a ela; e

- O acesso aos dados relevantes sobre a LATO, para uso na estimativa de impactos econômicos, é severamente restrito pela falta de transparência e pelas suas regras de não divulgação. Essas lacunas de dados representam uma ameaça à supervisão eficaz, incluindo a capacidade dos analistas de tentarem desenvolver estimativas teórica e empiricamente corretas sobre os seus impactos.

Além disso, embora o foco aqui esteja nos custos potenciais gerados pela LATO, a consideração dos benefícios potenciais sugere que eles seriam ainda mais difíceis de estimar. Não está claro se a Lei melhorou ou melhorará o acesso das Autoridades aos dados digitais e aumentará sua eficácia operacional. Além disso, é geralmente aceito que uma das maneiras mais importantes de promover a segurança cibernética é promover uma adoção mais ampla da criptografia ponta a ponta.[7] A LATO representa um desafio para uma adoção mais ampla de criptografia ponta a ponta eficaz, uma vez que, por projeto, a Lei versa sobre como habilitar ferramentas para acessar o conteúdo de dados criptografados.

[7] "*A criptografia ponta a ponta - em que as chaves necessárias para decifrar uma comunicação criptografada residem apenas nos dispositivos que se comunicam - fornece o nível mais forte de segurança e confiança, porque, por projeto, apenas o destinatário pretendido possui a chave para descriptografar a mensagem*" (ver INTERNET SOCIETY (2020), Informativo: Varredura no Lado do Cliente ("Fact Sheet: Client-Side Scanning"), 24 de março de 2020, disponível em https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Ficamos surpresos ao descobrir que não houve esforços substanciais anteriores para estimar empiricamente os custos ou benefícios econômicos da LATO, ou de leis análogas (com implicações econômicas para a segurança digital) na Austrália ou em outro lugar.

Na falta de pesquisa de terceiros para fundamentar uma estimativa do impacto econômico da LATO, conduzimos uma pesquisa original na forma de entrevistas em profundidade por videoconferência com os principais Provedores multinacionais, e na forma de uma enquete anônima junto aos demais Provedores, todos com operações na Austrália. Conforme explicamos mais detalhadamente no relatório, os dados empíricos resultantes são totalmente consistentes e dão suporte à análise apresentada no restante de nosso relatório. A pesquisa de experiências e expectativas de Provedores com a LATO confere justificativa empírica para concluir que:

1. A expectativa é de que a LATO terá impactos adversos generalizados sobre as empresas e seus clientes (*ou seja*, não restritos apenas a empresas nos setores de TIC);

2. A maioria dos danos esperados serão indiretos e associados ao risco que a LATO representa para as percepções de clientes e parceiros da indústria sobre a confiança digital;

3. Persiste uma incerteza significativa sobre a LATO e seus efeitos;

4. A evidência empírica direta de custos (ou benefícios) econômicos é bastante limitada, mas atribuímos isso (a) à opacidade com a qual as atividades da LATO estão envoltas devido às regras de não divulgação; (b) ao tempo limitado desde a aprovação da Lei e contínua controvérsia sobre a Lei, impedindo seu uso pelas Autoridades; e (c) à expectativa de que os impactos sejam provavelmente indiretos e futuros;

5. A evidência direta limitada que observamos dá suporte à conclusão de que, para as empresas, os benefícios específicos são provavelmente pequenos, enquanto os custos específicos podem ser muito grandes; e,

6. Os dados empíricos disponíveis não fornecem uma base confiável para quantificar em dólares o impacto econômico agregado da LATO.

Os dados levantados pela pesquisa também foram consistentes com nossa expectativa de que a evidência empírica dos efeitos diretos da LATO seria esparsa e difícil de observar. Essa falta de evidência empírica, entretanto, *não é* a evidência da falta de um efeito. Mesmo assim, as limitadas evidências coletadas são reveladoras. Um entrevistado que havia sentido um impacto econômico adverso direto estimou o efeito como sendo da ordem de um bilhão de dólares (australianos),[8] enquanto o único entrevistado que considerou majoritariamente favorável o

[8] O resultado adverso foi diretamente atribuído aos danos da LATO à imagem da marca de um Provedor, resultando em perdas nas vendas atuais e futuras. Consulte o Capítulo 6 para uma discussão mais completa dos resultados da entrevista e da pesquisa.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

impacto da LATO viu seu principal efeito como a racionalização da legislação existente.[9] Ambas as observações são consistentes com a conclusão de que, para as empresas, os benefícios específicos são provavelmente pequenos, enquanto os custos específicos podem ser muito grandes. Embora a pesquisa empírica apoie a conclusão geral do relatório, o tamanho da amostra impede seu uso como base para uma quantificação mais precisa desses danos.

Resumindo

De um modo geral, esta análise nos leva a concluir que a *LATO representa um risco significativo de futuros danos econômicos líquidos para a economia da Austrália, com prováveis repercussões adversas no exterior*. A evidência preliminar demonstra que algumas empresas já experimentaram prejuízos econômicos significativos; embora pareça provável que a maior parte do impacto agregado dos danos ocorra no futuro e se espalhe, se a ameaça da LATO à criptografia continuar. Além disso, a confusão e a incerteza para Provedores causadas pela Lei persistem e ainda precisam ser tratadas de forma adequada.

Embora os desafios de estimar o impacto econômico sejam difíceis, não houve *nenhuma* pesquisa pública significativa que tentasse quantificar o impacto econômico da LATO ou de legislação semelhante na Austrália ou em outro lugar. No entanto, a falta de tais evidências empíricas não significa que não haja impacto significativo. Em vez disso, sugere que o ônus da prova deve ser deslocado para avaliar o motivo pelo qual se espera que a LATO produza benefícios significativos, já que é claro o risco de danos significativos representados pela Lei .

2. Introdução e Visão Geral

O foco deste relatório é fornecer uma avaliação das evidências disponíveis sobre o impacto econômico da *Lei de Alteração das Telecomunicações e Outras Legislações (de Assistência e Acesso) de 2018* (mais conhecida como LATO, pelas iniciais do nome em inglês, "*Telecommunications and Other Legislation Amendment*"), aprovada pela Austrália.[10]

A LATO é uma legislação importante e complexa. Como explicaremos com mais detalhes abaixo, ela altera sete importantes leis australianas relacionadas à segurança da informação, bem como dá sequência e contribui para os esforços legislativos semelhantes em vários outros países, como Reino Unido e Estados Unidos. Assim, espera-se que ela tenha implicações nacionais (para a Austrália) e internacionais sobre os esforços de proteção de dados digitais.

O foco deste estudo é a criação de novas ferramentas governamentais para contornar a criptografia, mediante a ampliação da autorização legal para o governo solicitar (ou exigir) o auxílio dos Provedores de Comunicações Digital na obtenção de acesso a dados digitais,

[9] Antes da LATO, um subconjunto dos Provedores estava sujeito à legislação existente que fornecia acesso governamental a dados digitais. Um entrevistado considerou a LATO uma redução de custos ao racionalizar a exposição da empresa à legislação existente. O entrevistado não forneceu uma estimativa da economia de custos, mas elas não foram consideradas muito grandes.

[10] Para o texto original da LATO, ver AUSTRALIA (2018), Nota 2 *supra*. Ela também é às vezes denominada "Lei de Criptografia", "Lei de Assistência e Acesso Australiana" ou "AAA".

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

incluindo dados criptografados. A definição aberta de Provedores prevista na LATO inclui uma gama imensa de empresas e atividades associadas ao fornecimento de produtos e serviços de tecnologia da informação e comunicação (TICs).

O Capítulo 3 fornece uma breve visão geral da história e do impacto jurídico da LATO. Ela foi aprovada em dezembro de 2018, em um processo sumário e rápido. Depois, sofreu várias revisões, cada uma recomendando modificações no texto e em sua aplicação.

O Capítulo 4 explica a função crítica que a criptografia desempenha na proteção de dados digitais e destaca algumas das implicações técnicas da ampliação das ferramentas para contornar a criptografia.

O Capítulo 5 analisa os potenciais impactos econômicos da LATO. Conclui-se existir o risco de a lei gerar futuros custos econômicos significativos que provavelmente não serão contrabalanceados pelos futuros benefícios econômicos compensatórios. Embora os dados e pesquisas disponíveis até o momento não permitam uma quantificação precisa do impacto econômico líquido, tal conclusão é sustentada, em parte, pela opacidade que a LATO cria.

O Capítulo 6 apresenta os resultados da pesquisa original realizada como parte deste projeto. Ela incluiu entrevistas detalhadas com os principais Provedores multinacionais e uma enquete anônima com Provedores que operam na Austrália, para avaliar suas experiências e expectativas em relação à LATO desde sua aprovação em 2018. A pesquisa foi semelhante a dois esforços anteriores – o primeiro realizado na véspera da passagem do LATO, e o segundo, um ano depois. Embora sejam insuficientes como base empírica confiável para quantificar o impacto esperado da LATO, esses resultados foram consistentes e apóiam a conclusão alcançada no Capítulo 5.

No somatório, essa análise nos leva a concluir que a *LATO representa um risco significativo de futuros danos econômicos líquidos para a economia da Austrália, com prováveis repercussões adversas no exterior*. A evidência preliminar demonstra que algumas empresas já experimentaram prejuízos econômicos significativos; embora pareça provável que a maior parte do impacto agregado dos danos ocorrerá no futuro e será generalizada se a ameaça da LATO à criptografia continuar. Além disso, a confusão e a incerteza para os Provedores, causadas pela Lei, persistem e ainda precisam ser tratadas de forma adequada.

Embora os desafios de estimar o impacto econômico sejam difíceis, não houve *nenhuma* pesquisa pública significativa que tentasse quantificar o impacto econômico do LATO ou legislação semelhante na Austrália ou em outro lugar. No entanto, a falta de tais evidências empíricas não significa que não haja um impacto significativo. Ao contrário, isso sugere que o ônus da prova deve ser deslocado para avaliar o motivo pelo qual se espera que a LATO produza benefícios significativos, já que é claro o risco de danos econômicos amplos e significativos por ela representados.

3. Estrutura e histórico da LATO

Nas duas subseções a seguir, fornecemos uma descrição geral sobre a estrutura jurídica da LATO e sua história até o momento. Primeiro, descrevemos como ela amplia a autorização legal do governo para obter auxílio da indústria no acesso a informações digitais criptografadas.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Em segundo lugar, revisamos a história da LATO, desde suas origens recentes até as muitas propostas de revisão ainda em análise.

3.1. Revisão estrutural da LATO

A LATO envolve mudanças extensas e significativas em sete importantes leis do Parlamento Australiano, e foi proposta a fim de "*introduzir medidas para melhor lidar com os desafios colocados às Autoridades pela criptografia onipresente*".[11] A legislação afetada inclui:[12]

1. *Lei de Telecomunicações de 1997* (TA1997),[13]
2. *Lei de (interceptação e acesso a) Telecomunicações de 1979* (Lei TIA),[14]
3. *Lei de Vigilância de Dispositivos de 2004* (Lei SD),[15]
4. *Lei de Crimes de 1914* (Lei de Crimes),[16]
5. *Lei de Assistência Mútua em Questões Criminais de 1987* (MACMA),[17]
6. *Lei da Organização Australiana de Inteligência de Segurança de 1979* (Lei ASIO),[18] e
7. *Lei Aduaneira de 1901* (Lei Aduaneira).[19]

3.1.1. Ampliação da autorização legal para o governo acessar dados criptografados

Com 228 páginas, a LATO é uma lei extensa composta de cinco títulos que disciplinam diferentes aspectos das ferramentas [N.d.T.] disponíveis ao governo para obter acesso legal a

[11] A citação é do parágrafo de abertura da Exposição de Motivos que acompanhou a proposição da LATO ao Parlamento Australiano em setembro de 2018. Veja [o documento original em inglês] da Exposição de Motivos ("*Explanatory Memorandum*"), de 20 de setembro de 2018, distribuído à Câmara dos Representantes pelo Ministro do Interior, o Honorável Peter Dutton MP sobre a proposição da LATO, disponível em https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r6195%22 (daqui em diante, referida como "Exposição de Motivos de 2018").

[12] Ver o parágrafo 1 da Exposição de Motivos de 2018, Nota 11 *supra*.

[13] TA1997 (*Telecommunications Act 1997*) disponível em https://www.legislation.gov.au/Series/C2004A05145.

[14] Lei TIA [*Telecommunications (Interception and Access) Act*] disponível em https://www.legislation.gov.au/Series/C2004A02124.

[15] Lei SD (*Surveillance Devices Act*) disponível em https://www.legislation.gov.au/Series/C2004A01387.

[16] Lei de Crimes (*Crimes Act*) disponível em https://www.legislation.gov.au/Series/C1914A00012.

[17] MACMA (*Mutual Assistance in Criminal Matters Act*) disponível em https://www.legislation.gov.au/Series/C2004A03494.

[18] Lei ASIO (*The Australian Security Intelligence Organisation Act 1979*) disponível em https://www.legislation.gov.au/Series/C2004A02123.

[19] Lei Aduaneira (*Customs Act*) disponível em https://www.legislation.gov.au/Series/C1901A00006.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

informações digitais. O foco de nossa análise está no Título 1, que previu novas ferramenta para requisitar ou exigir auxílio da indústria no acesso a informações digitais criptografadas de uma "gama mais ampla de provedores".[20] Assim, é sustentado o foco no impacto econômico da LATO e na demanda e uso de criptografia.

Em suma, a LATO permite que um número seleto, porém grande, de Autoridades diferentes requeiram ou exijam que um Provedor de Comunicações Designado forneça assistência tecnológica para remover ou contornar a criptografia usando três instrumentos legais, um conjunto ao qual nos referimos neste documento como "avisos da LATO":[21]

1. Requisição de Assistência Técnica (**TAR**, do inglês "*Technical Assistance Request*") – uma solicitação para que um Provedor:
    a. voluntariamente ofereça ajuda ou assistência a uma agência governamental – e / ou
    b. voluntariamente desenvolva uma ferramenta de ajuda a uma Autoridade.
2. Notificação de Assistência Técnica (**TAN**, de "*Technical Assistance Notice*") – semelhante a um TAR, porém obrigatório, impõe exigências a um Provedor, e se limita ao oferecimento de ajuda, sem abarcar o desenvolvimento de uma ferramenta de ajuda.
3. Notificação de Ferramenta Técnica (**TCN**, de "*Technical Capability Notice*") – também obrigatória, requer ou determina a um Provedor que desenvolva uma nova ferramenta para permitir contornar criptografia,[22] ou que ofereça ajuda ou assistência.

Cada tipo de aviso da LATO está sujeito a diferentes requisitos legais em relação a quem pode emiti-lo, circunstâncias e regras do devido processo que regem o uso das ferramentas, o que pode ser solicitado ou determinado, e a supervisão e opções que os destinatários têm para contestarem.

Os avisos da LATO criam novos procedimentos governamentais para requerer e exigir que a indústria (a) forneça assistência; e/ou (b) desenvolva uma ferramenta para contornar criptografia. Ambos os tipos de poderes levantam preocupações, mas a ameaça de poder ser

[20] Ver parágrafos 8 e 10 da Exposição de Motivos de 2018, Nota 11 *supra.*

[21] A LATO trata disso em seu Título 1, ocupando mais da metade de sua extensão, propondo adicionar à TA1997 uma nova "Parte 15 - Assistência à Indústria" (ver páginas 4-109 da LATO, Nota 10, *supra*).

[22] Considerando que a "remoção de uma ou mais formas de proteção eletrônica" (ou seja, remoção da criptografia) está incluída como uma das obrigações de fazer ou coisas que uma TAR pode solicitar ou que um TAN pode exigir (ver seção 317E (1)(a) da LATO, Nota 10 *supra*), a LATO exclui do TCN o requerimento de que um Provedor disponibilize uma ferramenta para remover criptografia (ver seção 317T (4)(c)(i) da LATO, Nota 10 *supra*). Como os TCNs podem exigir que os Provedores forneçam uma ferramenta para habilitar outras obrigações de fazer listadas na 317E, os TCNs podem obrigar os Provedores a fornecer ferramentas que possam ajudar as LEIA a contornarem a criptografia.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

chamado a criar uma ferramenta para contornar criptografia quando se é destinatário de um aviso da LATO levantou as mais significativas preocupações. Uma vez criada, essa ferramenta pode fornecer meios para contornar a criptografia aplicável a qualquer informação digital, não apenas a criptografia do alvo designado, que justificou a solicitação original.[23]

Sem saber a natureza precisa da ferramenta que pode ser criada, é impossível saber a magnitude da ameaça à segurança digital que ela pode representar. A LATO procurou abordar essa preocupação óbvia, limitando as solicitações àquelas que não resultariam na criação de uma "vulnerabilidade sistêmica". Ou seja, que qualquer pedido de assistência da indústria ou de uma ferramenta seja suficientemente focado para abordar o(s) alvo(s) específico(s) do interesse legítimo objeto de autorização legal para o governo, sem criar vulnerabilidades de segurança que impactariam terceiros.[24] Conforme discutiremos adiante, a eficácia dessa limitação continua a suscitar preocupações.

Os tipos de assistência ou ferramentas que as agências governamentais podem solicitar sob a LATO são extensos e complexos. Isso inclui "remover uma ou mais formas de proteção eletrônica", que inclui criptografia, mas também inclui "fornecer informações técnicas", "facilitar (…) o acesso a (…) um recurso, equipamento de consumo, um dispositivo de processamento de dados, um serviço de transporte listado, (…) software" etc.[25] Embora a lei australiana forneça disposições que autorizam agências governamentais a solicitar assistência da indústria na execução de mandados legais e no acesso a dados digitais, a LATO amplia significativamente essa autorização legal.[26] Além disso, conforme apontado, a prerrogativa de requerer e exigir assistência para contornar criptografia é, aparentemente, nova para a

[23] Por exemplo, uma ferramenta criada nesses termos pode fornecer meios para contornar a segurança digital por terceiros que não eram o alvo original do aviso da LATO. As violações por parte desses terceiros podem ser intencionais (por exemplo, alguém mal-intencionado que busca intencionalmente obter acesso a informações confidenciais) ou não intencionais (por exemplo, alguém que comprometa a segurança digital por ignorância ou descuido). A questão é que, uma vez criada a ferramenta, restringir seu abuso subsequente representa um desafio adicional.

[24] A LATO define uma "vulnerabilidade sistêmica" ou "fragilidade sistêmica" como aquela que afeta "toda uma classe de tecnologia" (ver páginas 12, 84-81 na LATO, Nota 10 *supra*).

[25] A seção 317E da LATO fornece uma lista dos vários tipos de assistência que podem ser solicitados (páginas 18-20 da LATO, Nota 10 *supra*).

[26] Por exemplo, a Parte 14 da Lei TA1997 impõe às provedoras de conexão e prestadores de serviços de transmissão, comutação e roteamento as obrigações de fornecer assistência à LEIA "conforme for razoavelmente necessário" para "fazer cumprir a lei penal", de "ajudar na investigação e persecução" de crimes e "salvaguardar a segurança nacional" (ver páginas 322-328 da Lei TA1997, Nota 13 *supra*). Além disso, o Capítulo 5 da Lei TIA estabelece para as provedoras de conexão e prestadores de serviços de transmissão, comutação e roteamento obrigações de cooperarem com LEIA e de fornecerem assistência na implementação de atividades legais de interceptação (por exemplo, escutas telefônicas) (ver páginas 360-410 da Lei TIA, Nota 14 *supra*).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Austrália.[27] É claro que a LATO estende o poder das Autoridades para contornar a criptografia, mas os limites precisos desse poder, se houver, não são claros.

Além de adicionar tipos de assistência que podem ser requeridos ou exigidos da indústria por agências governamentais, a LATO também ampliou a gama de empresas de TIC às quais essas obrigações se aplicam. Isso representa uma mudança significativa. Antes da LATO, os provedores de serviços de comunicação (CSPs, de "*Communication Service Providers*") já estavam acostumados a cooperar com Autoridades no fornecimento de acesso legal a dados digitais em uma variedade de contextos (por exemplo, fornecendo assistência na execução de escutas telefônicas legais). A LATO expande o grupo de empresas sujeitas a requerimentos legislativos para entidades classificadas como Provedores. Ela os define como qualquer "pessoa" que se enquadre em uma das quinze categorias de empresas identificadas na seção 317C[28] e listadas de modo exaustivo no Apêndice.

Embora algumas entidades comerciais identificadas como Provedores já estivessem sujeitas a obrigações legais de cooperar com as Autoridades na obtenção de acesso legal às informações digitais, a LATO aumentou significativamente o escopo das empresas de TIC que poderiam estar sujeitas a solicitações ou ordens para fornecerem assistência, bem como a lista de atividades afetadas. Uma vez que muitas empresas de TIC estão envolvidas em várias atividades que abrangem várias categorias, e que a categorização apropriada das atividades pode ser ambígua, fica claro que o alcance da LATO é amplo. O que não fica claro é quais tipos de empresas de TIC, se houver, ou atividades estão isentas de serem destinatárias de avisos da LATO. Esse alcance da Lei que é amplo, porém incerto, significa que o seu impacto potencial também é bastante amplo, já que inclui essencialmente todo o setor de TIC. Além disso, a maioria das empresas em setores não relacionados às TIC utilizam essas tecnologias intensamente e têm funções de negócios que podem ser qualificadas como destinatárias dos avisos da LATO. Pode-se argumentar ser um Provedor qualquer empresa que interage com seus fornecedores ou clientes por meio de um site ou aplicativo.

A gama de Autoridades que podem emitir notificações da LATO também é extensa. Inclui agências responsáveis pela aplicação da legislação nacional, segurança nacional, aplicação da

[27] Limitamos nossa alegação de que a autorização prevista na LATO para contornar a criptografia é "nova" porque (a) autorização legal para o governo exigir assistência da indústria para obter acesso às informações criptografadas existia no Reino Unido desde antes da LATO, que se inspirou na Lei de Poderes de Investigação do Reino Unido de 2016 (ver "*Investigatory Powers Act* 2016", Reino Unido, disponível em https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted); e (b) numerosas recomendações para alterações adicionais à LATO estão sendo consideradas, e dada a sua complexidade e das leis que ela sobrepõe e altera, está além do escopo deste relatório fornecer uma análise jurídica completa da LATO e de até que ponto quais das suas capacidades são verdadeiramente novas. Os juristas podem discordar quanto à interpretação das alterações na LATO e até que ponto a legislação pré-LATO, que faz parte da estrutura legal relacionada ao acesso legal do governo às informações, pode ser interpretada como a concessão de algum nível de poderes do governo para contornar a criptografia.

[28] Páginas 14-18 da LATO, Nota 10 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

legislação internacional, e atividades de segurança (incluindo coleta de informações).[29] A autorização legal concedida a diferentes Autoridades pela LATO é definida em vários graus de especificidade. Por exemplo, o número de Autoridades que podem emitir TARs (voluntários) é mais amplo que o número das que podem emitir TANs ou TCNs (obrigatórios).[30] Muitas das emendas propostas e as preocupações levantadas sobre a LATO estão relacionadas à necessidade de uma melhor supervisão para ajudar a garantir que as novas ferramentas para acessar dados digitais e contornar a criptografia não sejam abusadas. Várias dessas alterações tomam a forma de revisão das restrições sobre quem pode emitir avisos da LATO, as circunstâncias em que podem ser emitidos, o processo de revisão antes de serem aprovados, e diversas outras medidas relacionadas à supervisão. Uma revisão legal completa ou avaliação da eficácia dessas disposições de supervisão, e dos esforços para limitar o escopo do impacto da LATO está além do escopo deste relatório, mas basta dizer que foram feitas uma série de recomendações significativas para alterações.[31]

Em suma, a LATO cria significativas novas ferramentas para uma ampla gama de Autoridades requererem ou determinarem a assistência de uma imensa gama de entidades de TIC a fim de obterem acesso a dados digitais confidenciais e contornarem a criptografia. Além disso, a natureza e os limites desses poderes estão sujeitos a incertezas significativas.

3.1.2. Detalhes sobre os avisos da LATO e outras previsões importantes

Uma distinção importante entre os diferentes tipos de avisos da LATO é que, para o destinatário, a observância a uma TAR é voluntária, enquanto a uma TAN ou TCN é obrigatória. Esta distinção é importante porque o não cumprimento de uma TAN (um pedido obrigatório de "assistência") ou uma TCN (um pedido obrigatório de desenvolvimento de uma "ferramenta") torna o destinatário sujeito a sanções na forma de responsabilidade civil, penalidades, medidas judiciais, ou processos criminais. *Como os destinatários podem ver a recusa a um TAR como uma precursora de um TAN ou TCN, a distinção entre uma notificação voluntária e uma obrigatória pode ser menos importante do que parece à primeira vista.* Na medida em que os destinatários interpretem o cumprimento da TAR como não exatamente "voluntária", o incentivo para cumprir será maior.

[29] As Autoridades que são especificamente identificadas como capazes de emitir avisos da LATO incluem a Organização Australiana de Inteligência de Segurança (ASIO, de "*Australian Security Intelligence Organization*"), várias agências de interceptação (IA, de "*Interception Agencies*") tais como as muitas autoridades policiais, o Serviço Australiano de Inteligência da Segurança (ASIS, de "*Australian Security Intelligence Service*") e a Diretoria Australiana de Sinais (ASD, de "*Australian Signals Directorate*").

[30] Por exemplo, a ASIO e as IA podem emitir todos os três tipos de notificações (sujeitos a diferentes restrições para diferentes tipos de notificações), mas o ASIS e a ASD podem apenas emitir TARs.

[31] Por exemplo, conforme explicaremos adiante na discussão da história da LATO, o relatório da INSLM pede uma grande mudança na alocação da autorização legal para emitir avisos da LATO (ver Nota 40 *infra*).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Em todos os casos, os destinatários ficam proibidos de divulgar o conteúdo e as circunstâncias relacionadas à emissão de um aviso da LATO. A divulgação ilegal, tal como o não cumprimento de notificações obrigatórias, pode resultar em sanções legais. Além disso, os relatórios são bastante limitados, sem divulgação de quem as recebeu e apenas estatísticas gerais relataram o número emitido.[32] As restrições de divulgação e as limitações dos relatórios sobre como a LATO está sendo usada tornam a supervisão eficaz um desafio, e complicam os esforços para avaliar o impacto econômico da Lei.[33]

Outra previsão importante é a garantia de "portos seguros", protegendo os Provedores destinatários de avisos da LATO das responsabilidades associadas ao seu cumprimento. Sob o regime anterior, nem sempre estava claro quando a cooperação da indústria no fornecimento de acesso a dados digitais poderia torná-la responsável por violar outras proteções legais de segurança ou privacidade. Além disso, a LATO prevê o reembolso dos custos sofridos no

[32] O registro sobre precisamente quantos avisos da LATO foram emitidos até o momento não está claro. A falta de transparência mesmo com relação ao número de emissões torna qualquer tentativa de estimar empiricamente o impacto econômico da LATO extremamente difícil, senão totalmente inviável. Em acréscimo, complica ainda mais o desafio a falta de transparência em relação às empresas (ou mesmo ao seu tipo) que receberam avisos da LATO, a que tipo de assistência foi solicitada, e a como os destinatários responderam.

Não obstante, acreditamos ser fato que, até o momento, apenas tenham sido emitidas TAR do tipo voluntária, e em número provavelmente inferior a 50. Não vimos nenhum relatório sobre a emissão de TAN ou TCN. Nossa estimativa sobre o número de TAR se baseia em dois relatórios oficiais e em discursos. Os dois relatórios documentam a emissão de 18 TARs, entre dezembro de 2018 e junho de 2020: 1 da Comissão Australiana de Inteligência Criminal (ACIC, de "*Australian Criminal Intelligence Commission*"); 8 da Polícia Federal Australiana (AFP, de "*Australian Federal Police*"); 9 da Polícia de Nova Gales do Sul (NSW, de "*New South Wales*") [ver Tabela 45 em DHA (2019), "Relatório Anual 2018-19 da Lei de (Interceptação e Acesso a) Telecomunicações de 1979", do Ministério do Interior australiano (DHA, de "*Department of Home Affairs*"), disponível em https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-18-19.pdf; e Tabela 44 em DHA (2020), "Relatório Anual 2019-20 da Lei de (Interceptação e Acesso a) Telecomunicações de 1979", do DHA, disponível em https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-19-20.pdf].

Ademais, em agosto de 2020, o Diretor-Geral da ASIO informou, à Comissão Parlamentar Mista de Inteligência e Segurança (PJCIS, de *Parliamentary Joint Committee on Intelligence and Security*), que "*usamos os poderes de assistência da indústria menos de vinte vezes*" (ver https://www.asio.gov.au/publications/speeches-and-statements/director-general-opening-statement-pjcis-august-2020.html). Não está claro no discurso se esta é uma referência aproximada aos TARs emitidos pelas agências específicas mencionadas acima, ou se essas "*vinte*" notificações são adicionais às observadas em outros relatórios. Em qualquer caso, seja o número 18 ou 50 (e nenhum dado sugere que seja maior), o uso governamental da LATO tem sido bastante limitado até agora.

[33] Algumas limitações na divulgação da atividade de avisos da LATO podem ser justificadas como necessárias para proteger a eficácia das ações das Autoridades.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

cumprimento dos avisos da LATO. Juntos, os portos seguros e as disposições de reembolso dos custos têm o efeito de aumentar os incentivos dos destinatários para as cumprirem.

Conforme explicamos nos capítulos seguintes, aumentar a probabilidade de que destinatários (desconhecidos) de avisos da LATO (desconhecidas) possam realizar atividades (desconhecidas) de eventual contorno de criptografia aumenta a amplitude potencial dos impactos econômicos da Lei e o risco (percebido) de que ela enfraquece a segurança digital.

3.2. História da LATO

A motivação para a aprovação da LATO deriva da preocupação crescente na Austrália e em todo o mundo de que o maior uso de criptografia seria uma ameaça à capacidade de as Autoridades acessarem dados digitais no curso de seus esforços de segurança e aplicação da lei. A partir do final de 2017, o governo australiano agiu com relativa rapidez para propor a LATO e fornecer às Autoridades mais ferramentas de remoção e contorno à criptografia.[34]

Em julho de 2017, o governo sinalizou sua intenção de resolver o problema.[35] Em agosto de 2018, a Austrália se reuniu com as outras nações dos Cinco Olhos[36] e uma posição conjunta foi alcançada.[37] A minuta da LATO foi publicada para comentários públicos em 14 de agosto de 2018.[38] O Ministério do Interior Australiano (DHA, de "*Department of Home Affairs*", o principal órgão governamental responsável pela LATO) recebeu mais de 340 sugestões. O projeto de lei com as emendas propostas foi apresentado na Câmara dos Representantes em 20 de setembro de 2018 e encaminhado à Comissão Parlamentar Conjunta de Inteligência e Segurança (PJCIS, de *Parliamentary Joint Committee on Intelligence and Security*) para análise, com relatório publicado no início de dezembro. A PJCIS realizou audiências públicas a partir de 19 outubro a 30 de novembro, e também abriu chamada para outros comentários.

---

[34] WALKER-MUNRO, Brendan (2019), "A shot in the dark: Australia's proposed encryption laws," Adelaide Law Review 40(3).

[35] Malcom Turnbull, "Conferência de imprensa com o Procurador-Geral e Comissário Interino da AFP — Sydney — 14 de Julho de 2017" (Conferência de Imprensa, 14 de Julho de 2017, https://www.malcolmturnbull.com.au/media/press-conference-with-attorney-general-and-acting-commissioner-of-the-afp-s).

[36] A Aliança dos Cinco Olhos ("*Five Eyes Alliance*") é uma aliança de compartilhamento de inteligência estabelecida sob o Acordo UKUSA entre Canadá, Nova Zelândia, Reino Unido, Estados Unidos da América e Austrália. Ela se propõe a facilitar o compartilhamento irrestrito e oportuno de informações de inteligência e segurança nacional.

[37] "Statement of Principles on Access to Evidence and Encryption", Procuradoria Geral ("*Attorney-General's Department*"), agosto de 2018, disponível em https://www.ag.gov.au/sites/default/files/2020-03/joint-statement-principles-access-evidence.pdf.

[38] A estrutura da LATO se inspirou fortemente na Lei de Poderes Investigativos do Reino Unido que foi aprovada em 2016 (ver "*Investigatory Powers Act* 2016," Reino Unido, disponível em https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

No total (incluindo confidenciais e retidas), 105 sugestões foram recebidas, sendo onze de agências governamentais, policiais ou comissões criminais, em apoio à proposta. Houve muitas outras contrárias à LATO, provenientes de representantes da indústria de tecnologia da informação da Austrália.

À luz do número de comentários que expressaram preocupação quanto ao impacto sobre as empresas, especialmente as pequenas, ao cumprirem as medidas de assistência da indústria, a PJCIS perguntou ao Ministério do Interior australiano se o governo havia preparado uma declaração de impacto regulatório sobre o Projeto de Lei. O Ministério respondeu ter sido feita uma declaração resumida de impacto regulamentar, com a conclusão de que "o impacto regulamentar das medidas de assistência à indústria será mínimo".[39]

Em 22 de novembro de 2018, a PJCIS recebeu do Ministro do Interior o parecer de que havia uma ameaça imediata, sendo necessário fornecer poderes adicionais às Autoridades e aprovar o projeto de lei na última sessão de 2018. Embora a PJCIS não tenha chegado a um acordo completo sobre todos os aspectos do projeto da LATO, a Comissão apresentou um Relatório Consultivo em 5 de dezembro de 2018,[40] que concluiu que:

> "(...) há uma necessidade genuína e imediata de as agências terem instrumentos para responderem ao desafio das comunicações criptografadas. A ausência desses instrumentos resulta em um crescimento do risco e tem dificultado as investigações das agências ao longo de vários anos. (...) Em resposta a esses riscos crescentes, a Comissão recomenda que o Parlamento considere urgentemente o projeto de lei e sua aprovação imediata".[41]

Apesar do envio de muitos comentários e relatórios de comissões a respeito das emendas propostas, a PJCIS apenas fez recomendações modestas ao texto da LATO. O projeto de lei foi

[39] Ver página 13 da "Emenda 18 – Suplementar à Emenda 6 (Resposta do DHA às Questões em Exame) da Revisão da Lei de Alteração das Telecomunicações e Outras Legislações (de Assistência e Acesso) de 2018" ("*Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Submission 18 – Supplementary Submission 6: Department of Home Affairs responses to Questions on Notice*"), Ministério do Interior da austrália, novembro de 2018, disponível em https://www.aph.gov.au/DocumentStore.ashx?id=13d6d87f-a64e-4e7c-8cc1-83d939e9fe1d&subId=660956 (daqui em diante, Emenda DHA à Tola).

[40] PJCIS (2018), "Relatório Consultivo sobre o Projeto de Lei de Alteração das Telecomunicações e de Outras Legislações (de Assistência e Acesso) de 2018" ["*Advisory Report on the Telecommunications and Other Legislation (Assistance and Access) Bill 2018*"], Comissão Parlamentar Mista de Inteligência e Segurança (PJCIS), dezembro de 2018, disponível em https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1.

[41] Biddington, M. (2019), "(Emendas diversas ao) Projeto de Emenda às Telecomunicações e Outras Legislações de 2019" ("Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 – Law and Bills Digest Section") 27 de março de 2019, disponível em https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6581692/upload_binary/6581692.pdf.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

alterado para esclarecer certas definições e inseriu previsões de que um prestador de serviço seja consultado e obtenha aconselhamento sobre o cumprimento de uma notificação obrigatória para desenvolver ferramentas de ajuda às Autoridades.[42] As previsões relativas a requisições e notificações de ajuda também foram alteradas para garantir que não pudessem ser utilizadas como atalhos aos processos já existentes que exigiam um mandado judicial. Não obstante, várias preocupações permaneceram.[43] A Comissão Parlamentar Permanente para o Exame de Projetos de Lei também apreciou o projeto de lei.[44] Embora uma análise completa das conclusões dessa Comissão Permanente esteja além do escopo deste estudo, ela levantou preocupações adicionais sobre a potencial natureza inconstitucional (i) de se excluir a revisão judicial dos avisos da LATO, prevista nos termos da Lei de (Revisão Judicial das) Decisões Administrativas de 1977,[45] (ii) de se enfraquecer a doutrina da separação de poderes,[46] bem como (iii) da incompatibilidade com a orientação política do próprio Procurador-Geral.[47]

O projeto foi aprovado em ambas as Casas em 6 de dezembro de 2018 e recebeu o Consentimento Real em 8 de dezembro de 2018 para se tornar parte do ordenamento jurídico australiano. A tramitação da lei desde o texto do projeto até à promulgação levou menos de quatro meses e foi descrita por alguns como precipitada, e o respectivo processo de consulta como limitado.[48]

---

[42] Ver páginas 5-7 do Relatório PJCIS (2018), Nota 40 *supra*.

[43] Tais como nas definições de vulnerabilidade e fraqueza sistêmicas, tecnologia alvo, imposição de objetivos relevantes para a emissão dos avisos da Parte 15, bem como um processo para que as agências de interceptação estaduais e territoriais se candidatem perante o Comissário da AFP para tais notificações.

[44] Comissão Parlamentar Permanente Para O Exame de Projetos de Lei (*Parliamentary Standing Committee for the Scrutiny of Bills*), Parlamento da Australia, Resumo do Exame ("*Scrutiny Digest*") (Resumo ("*Digest*") nº 14 de 2018, 28 de novembro de 2018) 23-82, disponível em https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Scrutiny_Digest/2018, daqui em diante Resumo do Exame 2018.

[45] Ver Resumo do Exame 2018, Nota 44 *supra*, página 42. A Lei de (Revisões Judiciais de) Decisões Administrativas de 1977, da *Commonwealth* (*Cth*), ou ADJR (de "*Administrative Decisions (Judicial Review) Act*") está disponível em https://www.legislation.gov.au/Details/C2021C00035/Download.

[46] Agentes públicos do Poder Executivo poderiam oferecer imunidade civil a Provedores que cumprissem as notificações da LATO (ver Resumo do Exame 2018, Nota 44 *supra*, páginas 47, 81).

[47] Ver Resumo do Exame 2018, Nota 42 *supra*, página 47. E "Um guia para o enquadramento de Ofensas à Commonwealth, Notificações de violação e Poderes de execução" ("*A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*"), Departamento do Procurador-Geral, setembro de 2011, disponível em https://www.ag.gov.au/legal-system/publications/guide-framing-commonwealth-offences-infringement-notices-and-enforcement-powers.

[48] Ver HARDY, K. (2020), "Leis de criptografia da Austrália: necessidades práticas ou estratégia política" ("*Australia's encryption laws: practical need or political strategy?*"), Internet Policy Review, 9(3), disponível em https://policyreview.info/articles/analysis/australias-encryption-laws-

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

A PJCIS solicitou que o Monitor Independente de Legislação de Segurança Nacional (INSLM, de "*Independent National Security Legislation Monitor*") iniciasse uma revisão da LATO em 26 de março de 2019. Essa revisão pelo INLSM foi encomendada pouco antes de a própria PJCIS concluir seu segundo relatório sobre a LATO em 3 de abril de 2019, recomendando (i) que recursos suficientes fossem disponibilizado ao INLSM para possibilitar sua revisão; (ii) que a PJCIS seja obrigada a produzir um terceiro relatório até junho de 2020; e (iii) que o Inspetor Geral de Inteligência e Segurança e o Ombudsman da Commonwealth tenham recursos suficientes para garantir que possam executar adequadamente suas responsabilidades adicionais no âmbito da LATO.[49]

O INSLM apresentou o seu relatório à PJCIS em 30 de junho de 2020, com uma série de recomendações para emendas à LATO:[50] que o poder de emitir e autorizar avisos da LATO fosse retirado dos chefes de agência e do governo, e entregue a um novo órgão de supervisão judicial; também pediu uma nova definição de "fraqueza sistêmica" e que a "vulnerabilidade sistêmica" fosse totalmente removida do projeto de lei.[51] Originalmente, o relatório do INSLM destinava-se a informar um terceiro relatório da PJCIS, programado para ser entregue ao governo em junho de 2020. Esse terceiro relatório foi adiado para setembro de 2020, mas até março de 2021, a PJCIS não o havia entregue.

Assim, dois anos após a aprovação da LATO, a lei continua controversa. Em parte, provavelmente, por ter sido redigida e aprovada às pressas, sem uma avaliação adequada do seu impacto potencial ou esperado. Durante a primeira investigação da PJCIS sobre a LATO

---

practical-need-or-political-strategy; r MILEY, V. (2019), "Leis de tecnologia escritas às pressas ameaçam a privacidade e a segurança online" ("*Hastily written tech laws threaten online privacy and security*"), GreenLeft, disponível em https://www.greenleft.org.au/content/hastily-written-tech-laws-threaten-online-privacy-and-security

[49] PJCIS (2019), "Revisão da Lei de Alteração das Telecomunicações e Outras Legislações (de Assistência e Acesso) de 2018" ("*Advisory Report on the Telecommunications and Other Legislation (Assistance and Access) Bill 2018*"), Comissão Parlamentar Mista de Inteligência e Segurança (PJCIS), dezembro de 2019, disponível em https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct/Report.

[50] INSLM (2020a), "Confie, mas verifique: Um relatório sobre a Lei de Alteração das Telecomunicações e de Outras Legislações (de Assistência e Acesso) de 2018 e assuntos relacionados" ["*Trust but Verify: A report concerning the Telecommunications and Other Legislation (Assistance and Access) Act 2018 and related matters*"], Monitor de Legislação de Segurança Nacional Independente Australiano (INSLM), Comunidade da Australia (*Commonwealth of Australia*), 9 de julho de 2020, disponível em https://www.inslm.gov.au/reviews-reports/telecommunications-and-other-legislation-amendment-act-2018-related-matters; e ver INSLM (2020b), "Confie, mas verifique: Resumo das Recomendações" ("*Trust but Verify: Summary of Recommendations*"), disponível em https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Additional_Documents.

[51] Ver Recomendações 3, 9, e 10 do INSLM (2020a), Nota 50 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

antes de sua promulgação em dezembro de 2018, o DHA foi questionado se o governo havia preparado uma declaração de impacto regulatório (RIS, de "Regulatory Impact Statement")[52] para avaliar seu provável efeito econômico sobre as empresas e a competitividade global. O DHA respondeu por escrito que o governo havia preparado apenas uma declaração de impacto regulamentar de formato reduzido,[53] que concluiu: "o impacto regulamentar das medidas de assistência pelo setor será mínimo".[54]

Não foi possível encontrar nenhuma evidência substantiva de que o impacto econômico potencial da LATO tenha sido detalhadamente considerado. Não temos conhecimento de nenhuma tentativa séria de quantificar ou mesmo detalhar como a LATO poderia realmente oferecer benefícios (por exemplo, melhorar a segurança nacional ou a aplicação da lei);[55] ou os potenciais danos econômicos que ela poderia causar se prejudicasse as perspectivas econômicas das empresas australianas ou ameaçasse a confiança no ecossistema digital.[56]

Nos capítulos subsequentes, explicamos (i) por que a criptografia é crítica para promover a segurança digital; e, dada a importância da informação digital para a economia australiana e global, como (ii) uma ameaça à criptografia representa um risco de danos econômicos significativos. Exploramos os vários mecanismos pelos quais a LATO poderia ameaçar a confiança digital e prejudicar a economia australiana.

---

[52] De acordo com o "Guia de Regulamentação do Governo Australiano de 2014" ("*Australian Government Guide to Regulation*") (o Guia) que se aplicava no momento da introdução e aprovação do LATO: "*cada proposta de política destinada a introduzir ou abolir a regulamentação deve ser acompanhada agora por uma Declaração de Impacto da Regulamentação do Governo Australiano, ou RIS* [de "Regulation Impact Statement"] *(...) [que] deve ter sido desenvolvida no início do processo de formulação da política*" (ver página 4 do 2014 do Guia, disponível em https://apo.org.au/sites/default/files/resource-files/2014-03/apo-nid270966.pdf).

[53] O primeiro passo na preparação de uma RIS em 2018 foi o órgão responsável fornecer um resumo escrito conhecido como Avaliação Preliminar do Escritório de Regulamentação das Melhores Práticas (OBPR, de "*Office of Best Practice Regulation*") do Departamento do Primeiro Ministro. Desde que a RIS forneça informações suficientes para ajudar o OBPR a compreender a natureza das questões de política tratadas, ele deve responder em 5 dias úteis, confirmando se a RIS é ou não necessária e, em caso afirmativo, de que tipo. Havia três tipos de RIS: formulário longo, formulário padrão e formulário curto. Em todos os casos, a agência deve realizar uma estimativa dos custos regulatórios (incluindo compensações), independentemente do tipo de RIS pelo qual opte (ver o Guia, Nota 52 *supra*, página 11).

[54] Página 13 da Emenda DHA à Tola, Nota 39 *supra*.

[55] Apenas dizer que existem crimes (terrorismo, tráfico de pessoas, etc.) que são hediondos e que representam uma séria ameaça à segurança e proteção nacional, embora certamente seja verdade, não é suficiente para demonstrar uma avaliação do impacto a respeito de como a LATO mesma, de fato, lida com esses e outros tipos de crimes para os quais ela poderia ser usada.

[56] Um pedido de acesso à informação para uma cópia da versão resumida do RIS foi apresentado ao Ministério do Interior em 1 de outubro de 2020. O DHA informou em 1 de março de 2021 que o RIS era um documento isento e não seria divulgado.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

4. Considerações de tecnologia

Nosso escritório LECA (iniciais de "*Law and Economics Consulting Associates*") foi contratado para avaliar a hipótese de que as tentativas legislativas e outras formas jurídicas de minar a criptografia podem ter um impacto negativo sobre aspectos econômicos, tais como negócios, inovação, comércio e investimento interno. Embora este relatório seja uma análise econômica, minar a criptografia (ou, como a LATO descreve, "*remover a criptografia*") envolve tecnologia. Com esse propósito, esta seção do estudo considera as implicações técnicas de se remover ou contornar a criptografia, e fornece uma moldura de referência que relaciona como as considerações tecnológicas podem afetar as questões econômicas. O nosso objetivo não é fornecer uma análise técnica em profundidade, mas apenas um contexto para a análise econômica.

Reconhece-se amplamente que a criptografia forte é essencial para elementos críticos de nossa sociedade, como comércio, liberdade, liberdade de expressão e segurança nacional.[57] Sem distinção, a criptografia forte também pode permitir que os criminosos se comuniquem sem serem observados ou terem suas mensagens decifradas pelas Autoridades, que por isso consideram ser a criptografia prejudicial à sua capacidade de conduzir suas missões. Nesse sentido, as Autoridades têm pleiteado leis que obriguem os Provedores que oferecem produtos e serviços criptografados a ajudar no fornecimento de acesso não criptografado a comunicações alvo com base em uma ordem judicial ou notificação por autoridade. Esse tipo de acesso lícito por terceiros costuma ser chamado de *acesso excepcional*[58] ao conteúdo criptografado.

Há um forte consenso entre os especialistas técnicos de que tais intervenções, mesmo que da maneira mais bem direcionada, aumentam o risco e têm o impacto adverso de corroer a confiança nos serviços criptografados.[59] Em uma análise de métodos de acesso excepcionais

[57] INTERNET SOCIETY (2017). "Mesa Redonda Chatham House da Internet Society sobre Criptografia e Acesso Legal" ("*Internet Society-Chatham House Roundtable on Encryption and Lawful Access*"), 26 outubro de 2017, disponível em https://www.internetsociety.org/resources/doc/2018/internet-society-chatham-house-roundtable-on-encryption-and-lawful-access/.

[58] Os requisitos de acesso excepcional se referem a alguns meios para permitir às autoridades policiais a prerrogativa de acessar legalmente, de uma forma legível, o conteúdo de comunicações e dados criptografados. Ver INTERNET SOCIETY (2018), Resumo sobre criptografia ("*Encryption Brief*"), 11 de junho de 2018, disponível em https://www.internetsociety.org/resources/doc/2018/encryption-brief/.

[59] ABELSON, Harold & ANDERSON, Ross & BELLOVIN, Steven & BENALOH, Josh & DIFFIE, Whitfield & GILMORE, John & GREEN, Matthew & NEUMANN, Peter & LANDAU, Susan & RIVERST, Ronald & SCHILLER, Jeffrey & SCHNEIER, Bruce & SPECTER, Michael & WEITZNER, Daniel & BLAZE, Matthew (2015), "Chaves sob capachos: insegurança obrigatória por exigência de acesso do Estado a todos os dados e comunicações" ("*Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*"), Journal of Cybersecurity, Volume 1, Issue 1, Setembro de 2015, Páginas 69–79. DOI: 10.1093/cybsec/tyv009. Disponível em https://doi.org/10.1093/cybsec/tyv009 e https://www.csail.mit.edu/research/keys-under-doormats; e NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

sob discussão na União Europeia, os principais especialistas em segurança cibernética observaram que qualquer método de acesso excepcional traria vulnerabilidades que poderiam ser exploradas por terceiros (p. ex., criminosos) contra quaisquer usuários.[60] A própria possibilidade de acesso excepcional poderia diminuir a confiança e o uso de criptografia e de serviços que dependem dela, como comércio ou finanças eletrônicas.

A seguir, investigamos questões específicas sobre a permissão de acesso a dados criptografados, conforme prevê a LATO.[61] Abordamos em linhas gerais as seguintes questões:

- O que é criptografia, como ela é usada e qual é seu valor?
- Como o acesso aos dados criptografados pode ser fornecido e como isso é definido na Lei?
- Quais são as possíveis consequências técnicas da LATO?

Para resumir esta seção, nós descrevemos os desafios de criar uma intervenção direcionada em um serviço de criptografia, e indicamos como tais intervenções podem ser maliciosamente aplicadas para além do alvo, a despeito das melhores intenções das Autoridades ou dos Provedores. Descobrimos que a linguagem vaga, com os requisitos e obrigações adotados de forma imprecisa na Lei, aumenta as preocupações a respeito da prerrogativa de elas criarem uma intervenção direcionada. Embora seja difícil quantificar o impacto associado a qualquer esforço que remova ou enfraqueça a criptografia, vemos um aumento do risco, e potencial para a diminuição da confiança nesses sistemas criptografados. A LATO pode minar e erodir a confiança pública nos muitos serviços criptografados que todos nós usamos diariamente. A simples percepção de criptografia mais fraca, ou a ameaça de agências governamentais terem a prerrogativa de coletar informações, mina a confiança no ecossistema digital.

4.1. O que é criptografia?

Existem muitas definições de cifragem de texto, mas uma simples e completa o bastante é: "*qualquer procedimento usado em procedimento criptográfico para converter um texto claro em um texto cifrado para evitar que qualquer pessoa, exceto o destinatário pretendido, leia*

(2018), Decifrando o Debate sobre Criptografia: Uma Moldura para Tomadores de Decisão" ("*Decrypting the Encryption Debate: A Framework for Decision Makers*"), Washington, DC: The National Academies Press. doi: https://doi.org/10.17266/25010. Disponível em https://www.nap.edu/read/25010.

[60] GLOBAL ENCRYPTION COALITION, "Quebrando mitos da criptografia" ("*Breaking Encryption Myths*"), 19 de novembro de 2020. Disponível em https://www.globalencryption.org/2020/11/breaking-encryption-myths.

[61] Essas descobertas foram extraídas a partir da análise da lei proposta, de uma revisão sobre a imprensa especializada e publicações acadêmicas, dos comentários enviados como parte do registro público, bem como de entrevistas com vários provedores de comunicação que oferecem serviços criptografados.

aqueles dados".[62] É claro que, no contexto do problema em questão, "texto" pode significar qualquer tipo de comunicação, tais como voz, imagens, caracteres, vídeo, conversa, sites e outros.[63] A intenção da cifragem é fornecer um meio de impedir o entendimento do conteúdo por outras pessoas que possam interceptar uma comunicação ou acessar informações. Um algoritmo de cifragem é usado sobre o texto claro em combinação com uma "chave" para gerar um texto cifrado. Os algoritmos de decifragem empregados no destino da mensagem revertem esse processo para recuperar o texto original. Isso significa que o destinatário pretendido da mensagem criptografada deve ter a chave para poder realizar a leitura. Podemos pensar na criptografia como um sistema de cifragem e decifragem, incluindo muitos elementos que operam em conjunto na Internet. Ela não consiste apenas em elementos matemáticos do *software*, mas também em um amplo grupo de algoritmos e funções críticas, como a troca segura de chaves. O pressuposto é que ninguém, exceto remetente e destinatário pretendido, deve ter as chaves.[64]

O sigilo proporcionado pela criptografia é tão forte quanto a força da implementação dela. A criptografia forte pode ser considerada como um cofre forte de um banco, que torna o acesso ao que está dentro impraticável, visto que seria necessário muito tempo, dinheiro, recursos e/ou experiência para arrombá-lo. Quebrar criptografia envolveria, de maneira análoga, muito esforço. Se um algoritmo criptográfico for fraco, o texto claro pode ser recuperado facilmente por um interceptor. Seria como uma fechadura simples no cofre, mas de nada adianta uma fechadura forte se você puder cortar as dobradiças e levantar a porta. Todas as partes do sistema da criptografia devem contribuir para sua força. Com uma cifragem cada vez mais forte, torna-se muito difícil, quase impossível, quebrar a criptografia. Também é crucial garantir que as chaves privadas sejam distribuídas apenas aos destinatários pretendidos, e não a quaisquer terceiros que possam usá-las para acessar os dados criptografados. Para seguir adiante na analogia, mesmo o mais forte dos cofres se abrirá se você tiver acesso às chaves.

---

[62] Definição para "Encriptação" ("*Encryption*") em AYERS, Rick; BROTHERS, Sam; JANSEN, Wayne. "Diretrizes sobre Análise Forense de Dispositivos Móveis" ("*Guidelines on Mobile Device Forensics*"). National Institute of Standards and Technology (NIST) Special Publication 800-101 Revisão 1, 87 páginas. Maio de 2014. U.S. Department of Commerce, 800-101r1 CODEN: NSPUE2 Disponível em http://dx.doi.org/10.6028/NIST.SP.

[63] Também podem surgir preocupações de segurança e privacidade associadas aos metadados de comunicações seguras, embora esse conteúdo possa não ser protegido por criptografia. Isso inclui informações sobre a origem e o destino das comunicações, os aplicativos usados, a hora em que as comunicações ocorreram e muito mais. Muitas das mesmas preocupações surgem em torno da proteção de metadados como uma camada adicional de segurança para o conteúdo das comunicações e, como tal, eles ficariam legalmente protegidos e requereriam um mandado para agências governamentais obterem seu teor.

[64] Os detalhes sobre troca de chaves, criptografia simétrica e assimétrica, e questões relacionadas, embora importantes, estão além do escopo deste relatório. Para um tratamento mais detalhado sobre o tema da criptografia, ver INTERNET SOCIETY (2018), "Criptografia" ("*Encryption*"), 26 de julho de 2018, disponível em https://www.internetsociety.org/issues/encryption/.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Também vale a pena mencionar que a criptografia pode ser implementada em uma variedade de pontos da rede e por uma variedade de entidades. Na verdade, agora é trivial para os usuários implementarem seus próprios serviços com criptografia forte de ponta a ponta sem fazer uso de um serviço comercial. Como discutiremos, isso tem implicações para as Autoridades.

4.2. Como a criptografia é usada e qual é seu valor?

A criptografia possui uma grande variedade de aplicações. É usada principalmente para proteger dados em armazenamento ("dados em repouso") ou em transmissão ("dados em trânsito"), mantendo-os confidenciais e íntegros. Claro, as pessoas desejam que seus dados sejam protegidos tanto em trânsito quanto em repouso. A criptografia tem uma ampla gama de usos, com exemplos que incluem: a proteção de transações financeiras e registros de saúde; o armazenamento seguro de arquivos; a garantia de integralidade de discos; o bloqueio de dispositivos; a verificação de credencial para acessar redes privadas virtuais, a segurança na navegação web, em mensagens privadas ou anônimas; segurança em nuvem; etc.[65] No fornecimento dessas proteções, a criptografia desempenha um papel importante ao habilitar partes críticas de nossa economia, mediante a garantia de confiança nas modalidades eletrônicas de comércio, finanças, saúde e edução; de segurança no armazenamento de informações e nas comunicações privadas seguras; e de nossas liberdades civis, como privacidade, liberdade de expressão e liberdade de associação.

Embora algumas pesquisas (conforme descrito na seção de economia deste artigo) tenham tentado atribuir um valor monetário à criptografia, é uma tarefa difícil dada a maneira como ela é costurada ao tecido de nossa existência moderna, às inúmeras maneiras nas quais confiamos nela em nosso cotidiano, e os inúmeros efeitos de segunda e terceira ordem que ela agora exerce em nossas vidas.[66] Conforme descrito anteriormente, a criptografia fornece a base para a confiança na Internet, e é essa confiança que possibilitou o enorme crescimento dos serviços de comunicações, comércio, finanças e saúde por toda a rede e o mundo. Durante a pandemia do COVID-19, a criptografia possibilitou a flexibilidade de trabalhar em casa para

[65] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE (2018). "Decifrando o Debate da Criptografia: Uma moldura para Tomadores de Decisão" ("*Decrypting the Encryption Debate: A Framework for Decision Makers*"). Washington, DC: The National Academies Press, 2018. DOI: https://doi.org/10.17266/25010. Disponível em https://www.nap.edu/read/25010/chapter/1#v.

[66] As estimativas de investimento em segurança cibernética são da ordem de centenas de bilhões de dólares. Ver LEECH, David P.; SCOTT, John (2018), "Os impactos econômicos do padrão de criptografia avançado, de 1996 a 2017" ("*The Economic Impacts of the Advanced Encryption Standard, 1996-2017*"), preparado para o Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards and Technology*) dos EUA, NIST GCR 18-017, disponível em https://doi.org/10.6028/NIST.GCR.18-017; publicado como artigo LEECH, David P.; FERRIS, Stacey; & SCOTT, John T. (2019). The Economic Impacts of the Advanced Encryption Standard, 1996–2017. Annals of Science and Technology Policy: Volume 3, Número 2, pp. 142-257. http://dx.doi.org/10.1561/110.00000010.

muitas empresas – permitindo que o comércio continuasse, apesar das restrições impostas pela COVID e da realidade prática de uma pandemia.

O valor da criptografia está em proteger esses serviços e fornecer uma base para a confiança. Sem criptografia forte, essa confiança não existe e essa falta de confiança prejudica os serviços mencionados. A confiança por meio da criptografia é a base de todas essas atividades na Internet e, sem ela, os indivíduos e entidades podem não estar dispostos a se envolver nessas atividades online. Na verdade, à medida que nossa sociedade continua mudando para uma economia de informação e dados, mais criptografia é necessária, e não menos, e minar sua força nos leva na direção errada.

Como a Apple apontou, "*Todos os dias, mais de um trilhão de transações ocorrem com segurança na Internet como resultado de comunicações criptografadas*".[67] Fato é que a melhor maneira de promover a segurança cibernética é promover uma adoção mais ampla de criptografia digital forte de ponta a ponta.[68]

---

[67] APPLE, Inc. "Revisão do Projeto de Lei de Telecomunicações e Outras Legislações (de Assistência e Acesso) de 2018, Submissão 53" ("*Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Submission 53*"), 12 de outubro de 2018, p. 1, disponível em https://www.aph.gov.au/DocumentStore.ashx?id=ecd6be12-ab84-43de-be61-1599e1db2a74&subId=661073.

[68] Existem numerosas declarações oficiais sobre o valor da cibersegurança, dadas por autoridades em países mundo afora. Por exemplo:

- O procurador-geral William Barr, em sua defesa do acesso execepcional em determinados contextos, reconheceu implicitamente que não havia maneira de fornecer para o governo acesso um dados criptografados sem que fossem criadas vulnerabilidades passíveis de serem também ser exploradas por outros agentes, mal-intencionados. Ainda assim, ele argumentou que esse risco era "*aceitável porque 'nós estamos falando de produtos e serviços de consumo, como mensagens, telefones inteligentes, e-mail e aplicativos de voz e dados', e 'não falando sobre a proteção dos códigos do país para lançamento nuclear*" [ver "O procurador-geral dos EUA William Barr diz que estadunidenses deveriam aceitar os riscos de segurança de portas dos fundos em criptografia" ("*US Attorney general William Barr says Americans should accept security risks of encryption backdoors*"), TechCrunch, 23 de julho de 2019, disponível em https://techcrunch.com/2019/07/23/william-barr-consumers-security-risks-backdoors/?guccounter=1];
- Ash Carter, ex-Secretário de Defesa dos EUA, argumentou que "*não adianta comprar todos esses aviões, navios e tanques e ter soldados, marinheiros, aviadores e fuzileiros navais se não posso conectá-los ... então a segurança dos dados é uma necessidade absoluta para nós ... portanto, estamos totalmente atrás de uma forte segurança de dados, incluindo criptografia forte ... sem dúvida*" [ver "Comentários do Secretário Carter em um bate-papo 'Fireside' com Ted Schlein em San Francisco" ("*Remarks of Secretary Carter in a 'Fireside' Chat with Ted Schlein in San Francisco*"), transcrição, Departamento de Defesa dos EUA ("*US Department of Defense*"), 2 de março de 2016, disponível em https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/684858/remarks-by-secretary-carter-in-a-fireside-chat-with-ted-schlein-in-san-francisc/];

4.3. Como o acesso excepcional pode ser fornecido?

Os mesmos recursos criptográficos que a tornam uma parte crítica da Internet podem ser usados por criminosos para ocultar atividades ilegais em um amplo conjunto de tecnologias e aplicativos. Isso impede que as Autoridades interceptem e visualizem facilmente o conteúdo das comunicações de um alvo sob investigação. Medidas de "acesso excepcional" buscam fornecer uma maneira de as Autoridades obterem acesso, em texto claro, ao conteúdo das comunicações criptografadas.

Em linhas gerais, podemos pensar em acesso excepcional pela:

- remoção de criptografia ou autenticação;
- inserção de fraquezas ou vulnerabilidades; ou

- Robert Hannigan, ex-Diretor do Quartel General de Comunicações do Governo - GCHQ (de "*Government Communications Headquarters*") do Reino Unido: "*A criptografia é uma coisa extremamente boa — ela nos mantém seguros e protegidos ... Embutir portas dos fundos é uma ameaça para todos e não é uma boa ideia enfraquecer a segurança de todos para lidar com um minoria*" [ver "*O ex-chefe da espionagem do Reino Unido avisa ser perigoso o plano de Amber Rudd de aprovar uma nova lei de criptografia em smartphones*" ("*UK's ex-spy chief warns Amber Rudd's plan to pass new smartphone encryption law is dangerous*"), The Independent, 10 de julho de 2017, disponível em https://www.independent.co.uk/news/uk/politics/uk-ex-spy-chief-amber-rudd-home-secretary-smartphone-encryption-law-dangerous-terrorism-isis-whatsapp-a7833211.html];

- O Comitê Permanente de Segurança Pública e Segurança Nacional ("*Commons' Standing Committee on Public Safety and National Security*") da Câmara dos Comuns ("House of Commons'") do Canadá canadense concluiu seu relatório de 2019 sobre "*Cibersegurança no Setor Financeiro como uma Questão de Segurança Nacional*", concordando que "*é importante, por razões de segurança e privacidade, que todo canadense tenha acesso à criptografia forte*" e recomendando que o governo do Canadá "*rejeite abordagens de acesso legal que enfraqueceriam a segurança cibernética*" [ver "Cibersegurança no Setor Financeiro como uma Questão de Segurança Nacional" ("*Cybersecurity in the Financial Sector as a National Security Issue*"), Câmara dos Comuns do Canadá, junho de 2019, disponível em https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP10589448/securp38/securp38-e.pdf]; e,

- De acordo com a Comissão Europeia, "*a criptografia forte é a base para sistemas de identificação digital seguros que desempenham um papel fundamental na segurança cibernética eficaz; também mantém a propriedade intelectual das pessoas segura e permite proteger os direitos fundamentais, como a liberdade de expressão e a proteção de dados pessoais, e garante o comércio online seguro*" [ver "Resiliência, dissuasão e defesa: construindo uma forte cibersegurança para a UE" ("*Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*"), Comissão Europeia, Bruxelas, 13 de setembro de 2017, pp. 9-10, disponível em https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450].

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

- inserção de hardware ou software para fornecer acesso a conteúdo descriptografado.

Isso pode ser habilitado por abordagens como depósito de chave ("*key escrow*"); alteração do gerenciamento de chaves; adição de fraqueza ou vulnerabilidade a criptografia, métodos, protocolos, ou implementações de um serviço de criptografia; ou simplesmente desligando a criptografia.[69]

Na Austrália, a LATO permite que as Autoridades imponham obrigações legais aos Provedores, exigindo que eles as ajudem no fornecimento de acesso a serviços criptografados e seus dados. O que a LATO não diz é como esse acesso pode ser fornecido. Não tentaremos discutir exaustivamente as abordagens técnicas para fornecimento de acesso a dados criptografados (isso está além do escopo deste relatório); em vez disso, simplesmente consideramos e discutimos as implicações técnicas gerais da LATO.[70]

O depósito de chave - no qual um conjunto adicional de chaves de decifragem é mantido por um terceiro "confiável", em "depósito", que as forneceria para as Autoridades quando legalmente apropriado - fornece um tipo de acesso para terceiros autorizados (ou seja, agências de aplicação da lei e de inteligência); no entanto, devido a preocupações sobre quem poderia obter acesso a essas chaves (por exemplo, elas podem ser roubadas, abusadas, perdidas ou compartilhadas) e porque o governo não depende das previsões da LATO para adotar medidas de depósito de chaves, não abordaremos mais esse tipo de técnica neste estudo, a não ser para observar que a comunidade técnica tem sido historicamente (e continua até hoje) contrária a essa abordagem.[71]

---

[69] Os meios técnicos para fornecer acesso a conteúdo criptografado podem incluir uma ampla gama de abordagens (algumas além do escopo da LATO), tais como: tirar proveito das vulnerabilidades descobertas; inserção de vulnerabilidades; ataques mais amplos com ferramentas como keyloggers ou ferramentas de espionagem; remoção de controles de segurança de um sistema, software ou dispositivo específicos; desabilitação ou rebaixamento dos serviços de criptografia; interrupção das sessões de criptografia entre o navegador e o servidor; troca de chaves; depósito de chave; ou outras abordagens possíveis. Novamente, uma discussão mais extensa está além do escopo deste artigo.

[70] A Austrália já possui leis que fornecem acesso legal a dados que proveriam às agências de aplicação da lei e de inteligência um caminho lícito para obter dados criptografados de um grande número de provedores de serviços. Conforme observado no capítulo jurídico, a LATO parece ampliar a legislação existente na medida em que menciona explicitamente a remoção da criptografia e alarga esse poder aos Provedores que não são transmissores de dados, provedores de serviços de transmissão e operadoras de rede e recursos de telecomunicações; e serviços que não são estritamente de telecomunicações, muitos dos quais já estavam (antes da LATO) sujeitos a extensa legislação da Comunidade de Inteligência Nacional. A legislação anterior inclui a *Lei de (Interceptação e Acesso a) Telecomunicações de 1979* (TIA) e a posterior legislação relevante que se seguiu aos ataques terroristas de 11 de setembro de 2001, desde os quais o Parlamento australiano aprovou mais de 124 leis alterando o quadro normativo da Comunidade de Inteligência Nacional.

[71] ABELSON, Harold & ANDERSON, Ross & BELLOVIN, Steven & BENALOH, Josh & DIFFIE, Whitfield & GILMORE, John & GREEN, Matthew & NEUMANN, Peter & LANDAU, Susan & RIVERST, Ronald & SCHILLER, Jeffrey & SCHNEIER, Bruce & SPECTER, Michael & WEITZNER, Daniel & BLAZE, Matthew (2015). "Chaves sob capachos: insegurança obrigatória por

Outra forma de implementar esse acesso é incorporar uma fraqueza ou vulnerabilidade do tipo "porta dos fundos"[72] em um mecanismo de criptografia subjacente ou software relacionado. O problema é que, por design, esse processo adiciona uma fraqueza ou vulnerabilidade, e a consequência de tal manipulação prejudica a criptografia. Adicionar fraquezas também simplesmente contraria o rigor das regras de desenvolvimento e auditoria da criptografia forte, bem como o processo de descobrir, notificar e corrigir tais fraquezas. Isso não apenas enfraquece a implementação real da criptografia, mas também corrói a confiança no conceito de criptografia como uma ferramenta que sustenta muito do que fazemos como uma sociedade online.[73]

4.3. Como esse acesso é definido?

Como discutiremos, a redação atual da LATO deixa uma série de perguntas e preocupações sobre sua implementação. Embora não seja incomum que aspectos da redação legislativa sejam intencionalmente amplos em escopo e aplicação, a única mensagem clara que ouvimos de todas as empresas que entrevistamos é que elas simplesmente não sabem o que esperar. Destacamos a falta de clareza e consideramos suas consequências.

Uma das primeiras coisas que observamos ao ler a LATO é que ela diz mais sobre o que um aviso não pode exigir, do que sobre o que ele pode exigir. Não surpreendentemente, essa abordagem é uma forma de reduzir o escopo de maneira a torná-lo mais aceitável, e mais difícil discordar de seu teor. No entanto, a redação tem um significado de difícil compreensão e a leitura por uma pessoa comum deixa incertezas quanto às definições e obrigações.

---

exigência de acesso do Estado a todos os dados e comunicações" ("*Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*"). Journal of Cybersecurity, Volume 1, Issue 1, September 2015, Pages 69–79. DOI: 10.1093/cybsec/tyv009. Disponível em https://doi.org/10.1093/cybsec/tyv009; e para uma versão ampliada do artigo, ver Relatório Técnico ("*Technical Report*") MIT-CSAIL-TR-2015-026, 6 de julho de 2015, disponível em https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[72] Conforme mencionado anteriormente, um método de obter acesso alternativo ao conteúdo das comunicações criptografadas é conhecido como "porta dos fundos" (do inglês "*backdoor*"), da mesma forma que uma porta dos fundos permite um acesso alternativo a um edifício. Claro, a maioria de nós não gostaria de uma porta dos fundos com uma fraqueza conhecida em nossa casa (ou seja, segurança enfraquecida), e a maioria de nós não gostaria de fornecer as chaves da porta para o governo (ou seja, depósito de chaves).

[73] Por exemplo, a backdoor Juniper do gerador de números randômicos DUAL-EC-DRBG [CHECKOWAY, Stephen; MASKIEWICZ, Jacob; GARMAN, Christina; FRIED, Joshua; COHNEY, Shaanan; GREEN, Matthew; HENINGER, Nadia; WEINMANN, Ralf-Philipp; RESCORLA, Eric; SHACHAM, Hovav (2016). A Systematic Analysis of the Juniper Dual EC Incident. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 468–479. DOI:https://doi.org/10.1145/2976749.2978395. Disponível em https://dl.acm.org/doi/pdf/10.1145/2976749.2978395].

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Por exemplo, a LATO prevê que "*não se deve solicitar ou exigir de um provedor de comunicações designado que implemente ou desenvolva uma fraqueza sistêmica ou vulnerabilidade sistêmica etc.*" Afirma ainda que as notificações não devem ter o efeito de "*(a) solicitar ou exigir que um provedor de comunicações designado implemente ou desenvolva uma fraqueza sistêmica, ou vulnerabilidade sistêmica, em uma forma de proteção eletrônica; ou (b) impedir que um provedor de comunicações designado corrija uma fraqueza sistêmica, ou vulnerabilidade sistêmica, em uma forma de proteção eletrônica.*" Ela afirma que as notificações não podem exigir que um provedor "*implemente ou desenvolva um novo recurso de decifragem*"; ou "*torne métodos sistêmicos de autenticação ou criptografia menos eficazes*"; ou introduza uma vulnerabilidade ou fraqueza "*seletiva*" que "*colocaria em risco a segurança de qualquer informação mantida por qualquer outra pessoa*"; ou crie "*um risco material de que informações seguras possam ser acessadas por um terceiro não autorizado*".[74]

As seguintes definições foram adicionadas à legislação:[75]

- *vulnerabilidade sistêmica* significa uma vulnerabilidade que afeta toda uma classe de tecnologia, mas não inclui uma vulnerabilidade que é introduzida seletivamente a uma ou mais tecnologias alvo que estão conectadas a uma pessoa específica. Para este efeito, é irrelevante se a pessoa pode ser identificada.
- *fraqueza sistêmica* significa uma fraqueza que afeta toda uma classe de tecnologia, mas não inclui uma fraqueza que é introduzida seletivamente em uma ou mais tecnologias alvo que estão conectadas a uma pessoa específica. Para este efeito, é irrelevante se a pessoa pode ser identificada.

Embora essas definições tentem reduzir o risco para usuários que não sejam alvo, ainda há uma falta de clareza e implicações para possíveis consequências. Esclarecer o que significa uma tecnologia alvo é o primeiro passo. Também seria útil entender como as vulnerabilidades introduzidas seletivamente em tecnologias alvo não poderiam ser usadas de forma mais geral no nível sistêmico, um ponto que foi observado por especialistas técnicos como um problema inerente a essa abordagem.[76] A abordagem adotada para implementar uma vulnerabilidade alvo (ou possivelmente a implementação real) tem uma alta probabilidade de vazar ou ser descoberta e explorada por outros. Nesse ponto, ela pode ser aplicada a um ou a muitos outros alvos.

Embora existam alguns métodos básicos para fornecer acesso a coisas como comunicações de voz por celular e certos dispositivos bloqueados, muitos serviços atuais de Internet usam

[74] Para essas e outras citações anteriores neste parágrafo, consulte as páginas 84-85 da LATO, Nota 2 *supra*.

[75] Página 12 da LATO, Nota 2 *supra*.

[76] Sobre o *EternalBlue*, ver SMITH, Brad. "A necessidade de uma ação coletiva urgente para manter as pessoas seguras online: Lições do ataque cibernético da semana passada" ("*The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*"), Microsoft On The Issues, Miscrosoft, 14 de maio de 2017, disponível em https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

criptografia forte de ponta a ponta, o que poderia limitar a capacidade do provedor de serviços em auxiliar no fornecimento de acesso excepcional (isso é reconhecido pela LATO).[77] Além disso, agora é simples implementar ou obter um serviço de comunicações com criptografia forte ponta a ponta sem depender dos serviços de um intermediário, de modo que este não teria capacidade de revelar o conteúdo se fosse pedido pelas Autoridades.

Na verdade, programas de código aberto podem ser baixados e instalados só para esse tipo de função, tornando cada vez mais difícil introduzir uma vulnerabilidade sem detecção. É possível que nenhum provedor (incluindo o criador do programa de código aberto – presumindo que a LATO possa até mesmo chegar legalmente a esse provedor) seja capaz de fornecer às agências governamentais as informações que procuram a partir de tal acesso.[78] A questão é que não é possível na prática impedir que as pessoas usem criptografia forte de ponta a ponta se estiverem motivadas para isso. É irreal esperar que algoritmos de criptografia sejam des-inventados ou des-publicados, assim como não é razoável esperar que sejam abolidos programas criptográficos de código aberto.

4.5. Quais são as consequências da LATO?

Numerosos estudos técnicos, econômicos e de negócios discutiram as preocupações pelo fornecimento de acesso excepcional à criptografia.[79] Essa gama vai desde a indicação de como

[77] As empresas que oferecem serviços que eliminam uma das extremidades do canal criptografado apresentam um padrão mais baixo para interceptarem comunicações. Elas têm acesso ao conteúdo não criptografado. Nesses casos, responder à solicitação de uma porta dos fundos deve impor custos diretos mínimos. [NdT. 4: esta nota se refere a casos como, por exemplo, o envio de um e-mail pela pessoa A para a pessoa B. Se A usa uma sessão https (ou seja, protegida por um protocolo *Transport Layer Security* - TLS) para enviar a mensagem ao servidor de e-mails, a mensagem estará protegida durante este trecho da transmissão. Entretanto, pode ser que B acesse o servidor de e-mails por uma sessão sem o protocolo TLS, e esta segunda parte da transmissão estará desprotegida. A criptografia pode proteger a mensagem durante apenas alguns trechos do envio, e não necessariamente em todos.]

[78] Por exemplo, malfeitores que sabem que são alvos potenciais das agências de aplicação da lei ou de inteligência podem ter maior probabilidade de empregar camadas adicionais de proteção de segurança amplamente disponíveis, o que tornaria ineficaz o acesso amparado pela LATO.

[79] NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE (2018), Decifrando o Debate sobre Criptografia: Uma Moldura para Tomadores de Decisão" ("*Decrypting the Encryption Debate: A Framework for Decision Makers*"), Washington, DC: The National Academies Press. doi: https://doi.org/10.17266/25010. Disponível em https://www.nap.edu/read/25010; BELLOVIN, Stephen M.; BLAZE, Matt; BONEH, Dan; LANDAU, Susan; RIVEST, Ronald L. (2018), "Análise do protocolo CLEAR de acordo com o Método da National Academies" ("*Analysis of the CLEAR Protocol per the National Academies Framework*") Relatório Técnico CUCS-003-18, Department of Computer Science, Columbia University, 10 de maio de 2018. Disponível em https://mice.cs.columbia.edu/getTechreport.php?techreportID=1637; BELLOVIN, Stephen M.; BLAZE, Matt; CLARK, Sandy; LANDAU, Susan (2014). "Hacking legal: usando vulnerabilidades existentes para grampear na Internet" ("*Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*"), Northwestern Journal of Technology and Intellectual Property, Volume 12, Issue 1, Article 1. Abril de 2014. Disponível em

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

a criptografia seria enfraquecida, passando pelos problemas apresentados pela erosão da confiança, até as preocupações mais amplas de uma Internet fragmentada. O acesso excepcional tem sido repetidamente recebido com forte resistência por especialistas técnicos nas últimas três décadas, e os esforços recentes de apoio ao acesso excepcional não mostraram um caminho que supere as preocupações técnicas; isso inclui a abordagem proposta na LATO. Nesta seção, tentamos fornecer uma perspectiva sobre os desafios e consequências do acesso excepcional e, mais especificamente, as dificuldades que a implementação da LATO apresenta. No restante deste capítulo, consideramos questões relacionadas a: enfraquecimento da criptografia; definição pouco clara do alvo; métodos de desenvolvimento e retenção; reuso; agravamento; vazamento e compartilhamento; e incerteza de processos e obrigações.

Enfraquecimento da criptografia

A LATO afirma que "*não se pode solicitar a um provedor de comunicações que: desenvolva ou implemente uma fraqueza ou vulnerabilidade sistêmica em uma forma de proteção eletrônica; ou impedir que um provedor de comunicações designado corrija uma fraqueza ou vulnerabilidade sistêmica em uma forma de proteção eletrônica*".[80] Aqui, os legisladores estavam tomando medidas para prevenir a criação de vulnerabilidades sistêmicas. No entanto, não solicitar a um provedor que desenvolva ou implemente uma fraqueza ou vulnerabilidade sistêmica não os impede de fazê-lo.

Em vez de dizer que o Provedor não será impedido de corrigir uma fraqueza ou vulnerabilidade, a linguagem deveria declarar que o provedor de comunicações designado é obrigado[81] a seguir as melhores práticas da indústria com relação à correção imediata de vulnerabilidades e fraquezas conhecidas.

---

https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1; ABELSON, Harold & ANDERSON, Ross & BELLOVIN, Steven & BENALOH, Josh & DIFFIE, Whitfield & GILMORE, John & GREEN, Matthew & NEUMANN, Peter & LANDAU, Susan & RIVERST, Ronald & SCHILLER, Jeffrey & SCHNEIER, Bruce & SPECTER, Michael & WEITZNER, Daniel & BLAZE, Matthew (2015). "Chaves sob capachos: insegurança obrigatória por exigência de acesso do Estado a todos os dados e comunicações" ("*Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*"). Journal of Cybersecurity, Volume 1, Issue 1, September 2015, Pages 69–79. DOI: 10.1093/cybsec/tyv009. Disponível em https://doi.org/10.1093/cybsec/tyv009; e Relatório Técnico ("*Technical Report*") MIT-CSAIL-TR-2015-026, 6 de julho de 2015, disponível em https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf; ALI, Mohamad (2016), "A descriptografia do governo com porta dos fundos prejudica o meu negócio e o seu" ("*Backdoor Government Decryption Hurts My Business and Yours*"), Harvard Business Review, 15 de setembro de 2016, disponível em https://hbr.org/2016/09/backdoor-government-decryption-hurts-my-business-and-yours.

[80] Seção 317 ZG, Página 84 da LATO, Nota 2 *supra*.

[81] Sempre há a chance de existirem vulnerabilidades, mas a responsabilização com relação às vulnerabilidades desconhecidas para o provedor depende de como é atribuído o padrão de dever fiduciário ou de obrigação de agir com a devida diligência, mas presume-se que, normalmente, não se constituiria uma responsabilidade ilimitada.

O risco é que a LATO possa criar incentivos para que as empresas mantenham (ou seja, não divulguem) vulnerabilidades conhecidas. Fazer isso deixa sob maior risco o público em geral; há um interesse público predominante em serem as vulnerabilidades relatadas, consertadas e remendadas o mais rapidamente possível, especialmente para reduzir o risco e o impacto de ataques "*zero day*".

Da mesma forma, algumas técnicas, como varredura do lado do cliente e a "proposta fantasma" do Reino Unido, são frequentemente apresentadas por seus proponentes como se utilizassem recursos existentes, em vez de inserirem novas fraquezas ou vulnerabilidades.[82] Essas técnicas, na verdade, inserem novas vulnerabilidades. Por exemplo, a proposta fantasma fornece um mecanismo para contornar efetivamente o processo de criptografia, permitindo que um terceiro entre em uma sessão sem que os participantes legítimos saibam. Como esse mecanismo é algo que um Provedor pode replicar em toda a base de usuários, ele se torna efetivamente um processo amplamente aplicável.

Segmentação pouco clara
Embora limitar a solicitação ou notificação a um alvo específico seja a abordagem correta, a fim de limitar o seu alcance, ainda não está claro como a segmentação poderia ser realizada sem expor usuários que não estejam no alvo. Parece ser responsabilidade dos Provedores tomarem essa decisão, e não há garantia de que eles o farão corretamente. Também não está claro como um Provedor irá implementar a remoção direcionada ou contornar a criptografia (se as atualizações podem ser necessárias, e como elas são direcionadas ao alvo e não vazadas). Isso levanta a questão: onde em um sistema se implementa o método de acesso excepcional e como ele é entregue?

Métodos de desenvolvimento e retenção
Embora a LATO tente proteger a criptografia forte declarando que não se deve solicitar ou exigir que os provedores implementem vulnerabilidades e fraquezas sistêmicas, isso não os impede de fazer isso. Embora se possa argumentar que uma empresa não está disposta ou inclinada a implementar tais vulnerabilidades sistêmicas, uma proibição nesse sentido permitiria maior confiança do consumidor na criptografia. Dado que a LATO permite que certas Autoridades solicitem ou exijam a implementação de vulnerabilidades ou pontos fracos seletivos, como essa vulnerabilidade é controlada e qual é o processo para evitar aplicações futuras dessa vulnerabilidade?

[82] Ver CALLAS, Jon (2019). "O esquema do 'usuário fantasma' para quebrar a criptografia não vai funcionar" ("*The 'Ghost User,' Ploy to Break Encryption Won't Work*"), post no blog da ACLU - American Civil Liberties Union, 23 de julho de 2019, disponível em https://www.aclu.org/blog/privacy-technology/ghost-user-ploy-break-encryption-wont-work. Para mais informações sobre a proposta Fantasma que foi apresentada pela primeira vez no Reino Unido, ver LEVY, Ian; ROBINSON, Cripin (2018). "Princípios para um debate mais informado sobre o acesso excepcional" ("*Principles for a more informed exceptional access debate*"), Blog da LawFare, 29 de novembro de 2018, disponível em https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Reuso

Embora possa parecer a direção certa, em princípio, limitar as obrigações ao desenvolvimento apenas de vulnerabilidades ou fraquezas alvo, na realidade, o mero ato de criar o mecanismo de acesso excepcional, não importa o quão direcionado, abre o sistema para usos indevidos e malfeitores de forma muito mais ampla. Uma intervenção específica pode levar a usos não intencionais, que não fazem parte da Requisição ou Notificação da LATO, criando uma porta dos fundos amplamente aplicável.

Além disso, desenvolver uma intervenção significa que uma rota de entrada agora seja conhecida. O conhecimento do método (ou pior, ferramentas de software ou uma implementação) pode causar a liberação não intencional ou consciente para terceiros não autorizados. A incerteza sobre a quem pode ter sido solicitado o desenvolvimento de uma intervenção de acesso excepcional diminui a confiança em toda a cadeia de valor.

Agravamento

Um desafio fundamental em obrigar os provedores a desenvolver o acesso direcionado é que não há garantia de que ele não será aplicado de forma mais ampla, vindo a se tornar parcial ou totalmente sistêmico. Ao se desenvolver um ataque sistêmico, a primeira etapa geralmente é definir um ataque restrito e, em seguida, determinar como aplicá-lo de forma mais ampla. Assim, exigir que os provedores tentem desenvolver intervenções direcionadas é um primeiro passo para a criação de vulnerabilidades sistêmicas. Além disso, uma intervenção direcionada, se necessária com mais frequência, provavelmente teria seu uso facilitado e mais automatizado e, portanto, começaria a abordar uma intervenção sistêmica.

É mais provável que uma intervenção direcionada se torne sistêmica quando o conhecimento sobre a fraqueza for descoberto, criado ou compartilhado. Até mesmo a possibilidade de que exista também pode encorajar malfeitores a procurá-la. Uma vulnerabilidade ou fraqueza direcionada pode ser agravada para uma vulnerabilidade sistêmica simplesmente replicando ou amplificando a vulnerabilidade em uma base de usuários (por meio de atualizações, vírus ou outros métodos).

Vazamento e compartilhamento

Intervenções direcionadas podem vazar e se tornar disponíveis para uma comunidade mais ampla, incluindo malfeitores que poderiam usá-las para atacar o público.[83] Além disso, as

[83] Em artigo sobre a CALEA II, apontou-se como tais vazamentos podem ocorrer: ADIDA, Ben; ANDERSON, Collin; ANTON, Annie I.; BLAZE, Matt; DINGLEDINE, Roger; FELTEN, Edward W.; GREEN, Matthew D.; HALDERMAN, J. Alex; JEFFERSON, David R.; JENNINGS, Cullen; LANDAU, Susan; MITTER, Navroop; NEUMANN, Peter G.; RESCORLA, Eric; SCHNEIDER, Fred B.; SCHNEIER, Bruce; SHACHAM, Hovav; SHERR, Micah; WAGNER, David; ZIMMERMANN, Philip (2013). "CALEA II: Riscos de modificações de grampos em terminais" ("*CALEA II: Risks of Wiretap Modifications to Endpoints, Center for Democracy & Technology*"), Centro para Democracia e Tecnologia ("*Center for Democracy & Technology*") 17 de maio de 2013, disponível em https://cdt.org/wp-content/uploads/pdfs/CALEAII-techreport.pdf. E sobre EternalBlue, ver SMITH, Brad. "A necessidade de uma ação coletiva urgente para manter as pessoas seguras online: Lições do ataque cibernético da semana passada" ("*The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*"), Microsoft On The Issues, Miscrosoft,

vulnerabilidades "descobertas" podem não ser corrigidas, mas retidas. Uma vez que as intervenções sejam conhecidas, é imperativo que os Provedores trabalhem por meio dos processos de notificação e correção bem estabelecidos nas comunidades de segurança, embora a LATO não exija isso deles. É razoável dizer: uma vez que uma vulnerabilidade ou fraqueza exista, é apenas uma questão de tempo até que seja descoberta, compartilhada, vazada, roubada ou submetida a engenharia reversa.

Processo e obrigações incertos

De acordo com a LATO, os Provedores podem ser solicitados a reter vulnerabilidades inadvertidas em seus sistemas para uso futuro, o que pode criar incerteza para esses provedores sobre quando e como devem participar da divulgação de vulnerabilidades. A divulgação clara da vulnerabilidade envia um forte sinal de que a criptografia robusta será mantida, aumentando a confiança dos usuários - entidades comerciais e usuários finais individuais. Também há incerteza sobre o que uma Requisição ou Notificação da LATO pode exigir de uma empresa; mais especificamente, até que ponto os provedores são obrigados a ajudar no processo de interceptar ou decifrar comunicações. A incerteza em torno da LATO significa que as empresas não têm certeza de quais métodos seriam necessários para cumprir uma Requisição ou Notificação da LATO, e isso significa que os oficiais de segurança da empresa devem se esforçar ao tomarem decisões sobre a adoção de tecnologia, a contratação de funcionários de segurança e até a consequência de uma parceria com outras empresas ou de um compartilhamento de dados. Esta é uma área que se beneficiaria de uma abordagem inteligente, personalizada e transparente.

Por design, é difícil (ou pelo menos deveria ser difícil)[84] quebrar criptografia forte, e não está claro como cada Provedor lidará com cada solicitação de acesso. Esta afirmação de falta de clareza é baseada em discussões do LECA com uma série de grandes Provedores. Com base em nossas entrevistas, as empresas não têm certeza sobre suas obrigações e não sabem quais métodos seriam necessários para cumprir uma Requisição ou Notificação da LATO.

Ademais, diferentes partes do ecossistema (ou seja, diferentes Provedores) precisarão adotar abordagens diferentes para remover ou contornar a criptografia. Descobrimos em nossas entrevistas que diferentes classes de Provedores têm diferentes perspectivas sobre o quão desafiador ou prejudicial pode ser remover ou contornar a criptografia. Descobrimos que as operadoras tradicionais (ou seja, ex-provedores de serviço de telefonia) têm uma visão menos crítica sobre a implementação de requisições da LATO em comparação com serviços da web, aplicativos e outros provedores de serviços de Internet.

Para resumir, a LATO poderia minar e erodir a confiança pública nos muitos serviços criptografados que todos nós usamos diariamente. A simples percepção de criptografia mais

14 de maio de 2017, disponível em https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/.

[84] O uso de métodos como o *Ghosting* permite a um terceiro ser adicionado silenciosamente a uma sessão segura, e pode-se argumentar que isso não é difícil, então adicionamos esta qualificação.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

fraca ou a ameaça de agências governamentais terem a capacidade de coletar informações prejudica a confiança em sistemas inteiros.

Os consumidores, sejam eles entidades comerciais ou indivíduos, podem evitar conduzir negócios em um ambiente de confiança comprometida. As empresas também enfrentarão decisões sobre se desejam enfrentar as dificuldades legais, operacionais e logísticas que podem surgir ao fazerem negócios na Austrália (este ponto foi levantado por várias empresas importantes durante nossas entrevistas). Inúmeras empresas de tecnologia com sede na Austrália expressaram suas preocupações com a LATO.

Por exemplo, em 2020, Patrick Zhang, Chefe de Política e Assuntos Governamentais da Atlassian, afirmou que "*A viabilidade e o crescimento contínuos da inovação e fabricação de tecnologia na Austrália serão em grande parte baseados na segurança real e na segurança percebida em relação às tecnologias que sustentam a economia digital e seu ecossistema*".[85] Essas alegações de dano não são apenas especulativas. A Vault Systems, provedora de serviços em nuvem australiana, afirmou que está sendo "*materialmente e prejudicialmente impactada*" pela LATO.[86]

Consequentemente, pode ser mais fácil simplesmente situar os serviços em outro país para evitar a miríade de desafios e incertezas econômicas. O Conselho de Arquitetura da Internet (IAB, de *Internet Architecture Board*) declarou: "*Este risco pode fazer com que alguns provedores de infraestrutura realoquem, reduzam o serviço ou mesmo bloqueiem o serviço para usuários australianos. Essa fragmentação da Internet é uma das principais preocupações que temos hoje, pois reduz o valor de uma Internet globalmente conectada*".[87]

[85] SADLER, Denham. "Leis de criptografia prejudicam o potencial: Atlassian" ("*Encryption laws damage potential: Atlassian*"), InnovationAus, 24 de junho de 2020, disponível em https://www.innovationaus.com/encryption-laws-damage-potential-atlassian/.

[86] STILGHERRIAN (2019). "O enorme escopo da nova lei de segurança nacional da Austrália se revela", ("*Huge scope of Australia's new national security law reveals itself*"), Post no blog The Full Tilt, ZDNet, 6 de junho de 2019, disponível em https://www.zdnet.com/article/huge-scope-of-australias-new-national-security-laws-reveals-itself/; e DUCKETT, Chris (2019). "As leis de criptografia estão criando um êxodo de dados da Austrália: Vault" ("*Encryption laws are creating an exodus of data from Australia: Vault*") ZDNet, 5 de julho de 2019, disponível em https://www.zdnet.com/article/encryption-laws-are-creating-an-exodus-of-data-from-australia-vault/.

[87] HARDIE, Ted. "Comentário do Conselho de Arquitetura da Internet (IAB) sobre o Projeto de Lei de Assistência e Acesso australiano de 2018" ("*Internet Architecture Board (IAB) comments on the Australian Assistance and Access Bill 2018*"), 9 de setembro de 2018, disponível em https://www.iab.org/wp-content/IAB-uploads/2018/09/IAB-Comments-on-Australian-Assistance-and-Access-Bill-2018.pdf.

5. Quadro Econômico

O principal objetivo desta pesquisa é avaliar todas as evidências disponíveis sobre o impacto econômico da LATO. Seria de se esperar que tal esforço tivesse sido empreendido antes da passagem da LATO, mas, como explicamos anteriormente, isso não aconteceu. Um pouco mais surpreendente para nós é a observação de que não existem em nenhum lugar estudos estimando o impacto econômico de leis como a LATO que possamos encontrar em lugar, seja por meio de nossa revisão da literatura publicada, ou no curso de nossa pesquisa original envolvendo entrevistas em profundidade com grandes Provedores multinacionais (discutidos mais detalhadamente no Capítulo 6). Os defensores e críticos das normas jurídicas dessa modalidade tenham contribuído para um grande corpo de literatura acadêmica, e enviado comentários nos procedimentos da LATO (como já observado) e em procedimentos semelhantes associados a outra legislação, como o Projeto de Lei de Poderes Investigativos (*Investigatory Powers Bill*) do Reino Unido (2016).[88] Não obstante, em todo esse material, há uma notável escassez de tentativas de quantificar os custos ou benefícios econômicos que podem ser esperados.

Em um mundo ideal, seria possível encontrar um estudo que já tivesse identificado todos os custos e benefícios potenciais, traduzido-os em termos monetários e, em seguida, agregado os dados para formular uma estimativa sobre o saldo efetivo dos benefícios econômicos que a LATO deve produzir. Se alguém tivesse essa estimativa, poderia ajudar a informar uma avaliação sobre se os benefícios da LATO são susceptíveis de exceder seus custos. É claro que uma estimativa monetária do efetivo saldo do impacto econômico agregado, por si só, não seria tudo o que os formuladores de políticas considerariam para avaliar a eficácia da LATO. Alguns impactos são inerentemente difíceis de traduzir em termos monetários (por exemplo, segurança nacional e prevenção ou repressão ao crime); e a distribuição dos efeitos econômicos também é um aspecto importante (tanto no que diz respeito à alocação de custos e benefícios, quanto no modo em que eles são experimentados ao longo do tempo).

Não vivemos em um mundo ideal e este relatório não pode produzir uma estimativa monetária quantitativa do impacto da LATO. Em vez disso, examinamos qualitativamente os diferentes mecanismos pelos quais a LATO pode resultar em efeitos econômicos. Essa análise identifica prontamente muitos mecanismos pelos quais a LATO pode produzir custos diretos e indiretos para Provedores, outras empresas e consumidores em toda a economia. Os custos relevantes não se limitam aos custos diretos para Provedores que podem receber notificações da LATO, ou mesmo apenas aos custos indiretos para empresas no setor de TIC, mas incluem também custos indiretos para outras empresas e consumidores de forma mais ampla. Além disso, espera-se que os custos se acumulem com o tempo, à medida que a nova autorização legal criada pela LATO venha a ser utilizada pelo governo.

Nossa análise nos leva a concluir que a LATO tem o potencial de resultar em danos econômicos significativos para a economia australiana e produzir repercussões negativas que amplificarão esses danos globalmente.

[88] Ver Nota 27 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Explicamos por que quantificar os componentes de custo e benefício seria um desafio, mesmo se melhores dados estivessem disponíveis, enquanto observamos a quase completa falta de dados relevantes. Além disso, explicamos por que quantificar os custos que a LATO provavelmente causará, pelo menos parcialmente, é um desafio inerentemente mais factível do que quantificar os benefícios que ela pode oferecer.

Nossa análise nos leva a concluir que a fonte potencial mais significativa de custos relacionados à LATO está associada à ameaça que ela representa para a confiança online. Como explicamos, mesmo um pequeno impacto na confiança pode levar a danos econômicos amplamente distribuídos, resultando em impactos econômicos adversos na casa dos bilhões de dólares. Em comparação com os custos indiretos que se acumularão ao longo do tempo, os custos diretos sentidos por empresas cujas perspectivas de negócios individuais podem ser prejudicadas pela LATO são provavelmente muito menores no agregado, mas ainda significativos para as empresas impactadas e em termos monetários agregados. Por exemplo, uma das multinacionais que entrevistamos contou como já havia perdido mais de um bilhão de dólares australianos ($AUS) em receita como consequência da LATO, e vários dos entrevistados em nossa pesquisa relataram já terem incorrido em perdas de receita de dois dígitos percentuais. Infelizmente, esses pontos de dados individuais não fornecem uma base confiável para derivar uma estimativa de custos agregados para toda a economia.

5.1. Estrutura para entender os impactos econômicos da LATO

O marco de referência apropriado para fazer tal avaliação é comparar o que aconteceu (ou é provável que aconteça) no mundo em que a LATO foi adotada com um hipotético mundo "controle" no qual ela não foi.[89] Isso levanta muitos e complexos desafios teóricos e empíricos, por várias razões, incluindo a necessidade de ampliar o esforço, abordando as seguintes questões:

1. Quais impactos econômicos devem ser considerados?
2. O foco deve ser nos impactos australianos ou globais?
3. Como equilibrar o foco nos custos e benefícios da LATO?
4. A análise dos impactos é de longo ou curto prazo?
5. Como se caracteriza o mundo "controle"?
6. Como coletar dados sobre os impactos da LATO?

Cada um desses desafios é tratado nas subseções a seguir.

[89] Note-se que a perspectiva de adoção da LATO provavelmente afetou o comportamento e os resultados antes mesmo de sua adoção em dezembro de 2018. Além disso, a incerteza persistente sobre futuras reformas regulatórias ou legislativas, e divergências em relação à interpretação legal da LATO e como ela é (ou será) usada, contribuíram para distorcer o desafio de identificar um conjunto de comparações claras entre antes e depois, ou com e sem a LATO, para se avaliarem os impactos econômicos. Como discutiremos mais adiante, um motivo pelo qual podemos falhar em observar os impactos mensuráveis no comportamento decorrente da LATO é porque ela ainda não está totalmente "eficaz", em razão das preocupações com os desafios contínuos da LATO.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

5.1.1. Quais impactos econômicos devem ser considerados?

A avaliação do impacto econômico da legislação depende da capacidade de avaliar como as empresas e os consumidores impactados pela LATO, direta ou indiretamente, mudarão seu comportamento como resultado da LATO, o que é desafiador porque o comportamento depende das expectativas. Idealmente, gostaríamos de quantificar os impactos mensuráveis no excedente total, que é a soma do excedente do produtor e do consumidor em termos monetários ($AUS). Os efeitos monetários da LATO sobre o excedente do produtor e do consumidor não são diretamente observáveis e devem ser estimados a partir da coleta de dados monetários e outros relacionados a resultados. Os tipos de impactos comportamentais e relacionados a resultados podem ser interpretados de forma ampla para incluir o efeito potencial da LATO nas receitas de negócios, investimentos e planos estratégicos. Por exemplo, o excedente do produtor pode ser estimado a partir de diversos dados relacionados ao resultado, como dados sobre receitas de negócios, custos operacionais e investimentos, que podem ser estimados a partir de dados de vendas por unidade e preço por unidade, e dados de custo. Atribuir mudanças em tais variáveis a um único efeito, como a LATO, requer dados adicionais para controlar outros efeitos.

Estimar o excedente do consumidor é ainda mais difícil, mas inclui considerar até que ponto a demanda do consumidor inframarginal excede os preços pagos (ou seja, até que ponto a disposição de pagar excede o preço).[90] Além disso, o excedente do consumidor também depende da escolha (seleção) e da qualidade do produto.[91]

As respostas comportamentais incluem mudanças nas práticas de emprego das empresas, comportamento de investimento e atividade de inovação, que são relacionadas. Por exemplo, os investimentos em capacidade de negócios dependem das expectativas quanto às perspectivas futuras para a empresa, que dependem da sua vantagem competitiva e dos seus investimentos

[90] A vontade de pagar não é observada diretamente, mas pode ser inferida de pesquisas com consumidores e pelo comportamento de preferência revelado no mercado (ou seja, a função de demanda estimada da indústria).

[91] Os consumidores normalmente fazem suas escolhas de compra entre várias empresas, cada uma das quais oferece vários níveis de produtos (por exemplo, prêmio, desconto) e escolhem o produto que oferece a melhor relação preço-qualidade. Pelo mesmo bem de qualidade, os consumidores sempre preferem preços mais baixos. No entanto, uma vez que a demanda dos consumidores por qualidade e outras características do produto varia, ter várias escolhas aumenta a probabilidade de que os consumidores possam encontrar produtos que correspondam mais de perto aos seus gostos idiossincráticos. Além disso, quanto mais empresas para escolher, mais concorrência, o que pode (ou não) resultar em uma seleção mais ampla de níveis de qualidade dependendo da natureza do produto e da dinâmica competitiva, mas geralmente resultará em preços mais baixos. No entanto, mesmo com uma única empresa, a seleção de produtos oferecidos é projetada para maximizar o excedente do produtor, o que confronta as empresas com o desafio de definir a precificação de nível do produto para discriminar o preço de forma otimizada: isto é, precificar para que alguns consumidores considerem racional a compensação entre a qualidade agregada e um preço mais alto; caso contrário, os consumidores optam pelo produto de menor preço e qualidade inferior, e o nível de qualidade superior não é viável no mercado.

em P&D e diversos investimentos estratégicos (por exemplo, em imagem da marca, segurança cibernética, propriedade intelectual , etc.). Conforme explicamos mais à frente, uma das possíveis respostas comportamentais a serem esperadas é que as empresas reduzam seus investimentos em P&D e no lançamentos de novos produtos na Austrália, que deverão sofrer impactos adversos da LATO, seja direta ou indiretamente. Nesse caso, estimar o impacto econômico dependerá de calcular os benefícios líquidos futuros esperados dos investimentos dissuadidos ou das melhorias na escolha de produto e preços, que de outra forma teriam ocorrido. Isso é inerentemente mais desafiador do que medir o que realmente aconteceu.

Logo, os impactos comportamentais e relacionados aos resultados dependem das posturas e expectativas sobre o negócio. Os impactos são potencialmente do tamanho da economia e até mesmo globais. Portanto, eles extrapolam os efeitos diretamente atribuíveis às empresas que receberam Requisições ou Notificações da LATO. De fato, espera-se que, no agregado, esses impactos indiretos sejam muito maiores que os efeitos diretos. No entanto, embora seja difícil avaliar os impactos econômicos diretos, é ainda mais desafiador estimar os impactos indiretos.

5.1.2. Foco nos impactos australianos ou globais?

Embora nosso foco esteja na economia australiana, também estamos interessados em identificar os prováveis efeitos colaterais de forma mais ampla. O mercado de tecnologia, produtos e serviços de TIC é global e a legislação da Austrália pode influenciar a probabilidade de leis semelhantes em outras nações, que fortaleçam ou enfraqueçam o impacto econômico da LATO no âmbito da Austrália ao longo do tempo.

Cada vez mais as informações estão em formato digital. Seja "em movimento" (chamadas telefônicas, mensagens, transferências de arquivos, trocas de identidade ou credenciais) ou "em repouso" (armazenadas como arquivos digitais, ou programas em dispositivos ou servidores de arquivos na nuvem), essas informações também cada vez mais estão protegidas por ferramentas de segurança cibernética, tais como tecnologias de criptografia ponta a ponta. A preocupação em conferir às Autoridades a capacidade de acessar essas informações é considerada uma séria ameaça internacional à efetividade da aplicação da lei e dos serviços de segurança.

Os legisladores em vários países propuseram e debateram iniciativas legislativas que concederiam às agências de aplicação da lei e de inteligência poderes adicionais para obter acesso excepcional a dados digitais.[92] Conforme explicado anteriormente, embora a LATO siga

[92] Por exemplo, o Reino Unido tem legislação em vigor que permite aos serviços de segurança pública e de inteligência de segurança nacional obter acesso legal a informações criptografadas desde o início de 2000, a qual foi ampliada por meio da Lei de Poderes Investigativos ("Investigatory Powers Act") de 2016, ver Nota 27 *supra*. Mais recentemente, nos EUA, a senadora republicana Lindsay Graham apresentou o Projeto de Lei do Senado 4051 - Lei de Acesso Legal a Dados Criptografados (LAEDA, de "*Lawful Access to Encrypted Data Act*") em junho de 2020 (ver CONGRESS.GOV. "S.4051 - 116th Congress (2019-2020): Lawful Access to Encrypted Data Act", 23 de junho de 2020 https://www.congress.gov/bill/116th-congress/senate-bill/4051); e em outubro de 2020, a aliança de inteligência entre os "Cinco Olhos" ("*Five Eyes*"), formada por Australia, Canadá, Nova Zelândia, Reino Unido, EUA (os países originais da aliança), Índia e Japão, apresentou um pronunciamento conjunto pedindo por ferramentas mais fortes para permitir o acesso legal a dados criptografados (ver

a adoção anterior pelo Reino Unido de poderes governamentais adicionais para obter a ajuda da indústria para contornar a criptografia, as lições aprendidas na Austrália provavelmente terão impacto se outras nações seguirem o exemplo. Isso preocupa, pois a falta de evidência empírica sobre danos econômicos significativos pode ser confundida com a evidência da ausência de tais danos, podendo encorajar outros países a adotarem legislação semelhante à LATO, ampliando assim os seus custos.

5.1.3. Como equilibrar o foco nos custos e benefícios da LATO?

A avaliação do impacto monetário agregado líquido da LATO requer a consideração dos custos que ela provavelmente vai impor, bem como os benefícios que pode oferecer. Embora seja relativamente fácil identificar vários mecanismos pelos quais a LATO pode impactar diretamente o comportamento das empresas e, portanto, dos consumidores, de maneiras que resultarão em aumento de custos, acaba sendo mais difícil rastrear o mecanismo pelo qual ela levará a maiores benefícios.

Nas seções subsequentes, identificamos os vários mecanismos pelos quais a LATO pode resultar em aumento de custos. No restante deste capítulo, explicamos por que estimar os benefícios é mais desafiador.

Em ambos os lados do custo e do benefício, as restrições à divulgação prevista na LATO interferem na coleta detalhada de dados sobre como o uso da Lei muda o comportamento. As lacunas de dados são ainda mais graves e o rastro de causalidade é ainda mais difícil de estabelecer no lado do benefício do que no lado do custo. O principal benefício verificado para a aprovação da LATO foi o enfrentamento à percepção do desafio que o aumento do uso de criptografia representa para as Autoridades em suas missões de aplicação da lei e segurança nacional. Presume-se que a ampliação das ferramentas legitimadas pela LATO devem melhorar a eficácia e a eficiência das Autoridades. Mas a falta de transparência torna mais difícil determinar como a LATO mudou ou pode mudar o comportamento das Autoridades (em relação ao mundo controle relevante).

No entanto, antes mesmo de alguém se aprofundar na resolução dessas deficiências de dados, é possível considerar qualitativamente como a LATO pode impactar a eficácia das Autoridades. Existem várias razões plausíveis que sugerem que os benefícios para as Autoridades são provavelmente pequenos. Isso inclui o fato de que (a) as tecnologias estão amplamente disponíveis para qualquer pessoa (incluindo criminosos) sobrepor camadas adicionais de segurança de dados, incluindo criptografia; e (b) já existe legislação extensa em muitos países que prevê o acesso legal aos dados.

O primeiro ponto sugere que alvos devidamente motivados que desejem proteger seus dados podem fazê-lo mesmo se a LATO for adotada, empregando criptografia forte para dados em trânsito (p. ex., mensagens de ponta a ponta) e em repouso (p. ex., armazenamento em um

UNITED KINGDOM, Home Office. “Declaração internacional: criptografia de ponta a ponta e segurança pública” (“*International statement: End-to-end encryption and public safety*”), Gov.UK, 11 de outubro de 2020, disponível em https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety).

dispositivo), e fazendo uso de outras técnicas (p. ex., várias formas de diversionismo, como o roteamento-cebola, [NdT. 5: sistema característico da rede ToR]) para tornar ineficazes quaisquer esforços de prestação de auxílio por Provedores. Os criminosos sabem que estão sempre brincando de gato e rato com as Autoridades. Portanto, eles têm um incentivo adicional para se aproveitarem das técnicas que utilizam camadas adicionais de segurança.

Mesmo que se rejeite o primeiro ponto, o segundo ponto destaca que os benefícios incrementais da LATO dependem da extensão em que ela cria novas ferramentas de ampliação dos recursos das agências para acessarem dados de alvos legais. Entretanto, havendo incerteza sobre como a LATO pode ser usada, fica incerto quão grandes podem ser esses benefícios incrementais.

Em qualquer caso, a análise de política baseada em evidências necessárias para estimar com mais precisão os custos e benefícios da LATO só se torna necessária caso haja expectativa de as estimativas serem relativamente próximas em magnitude. Se houver suporte (ou evidência) convincente de que os custos totais são mínimos, mas os benefícios totais são substanciais (ou vice-versa), ter estimativas precisas do impacto econômico é menos importante.[93]

Uma vez que até agora nenhuma análise de impacto econômico detalhada real foi conduzida (ou disponibilizada publicamente), seria razoável concluir que os benefícios são maiores que os custos, se fosse concluído que ou (1) os custos potenciais são mínimos, ao passo que os benefícios são grandes, ou (2) os custos e os benefícios potenciais são ambos mínimos, mas os benefícios potenciais são maiores.[94] Os argumentos qualitativos citados acima sugerem que o primeiro caso seja improvável, mas o segundo caso ainda precisa ser analisado. Assim, é um ponto de partida razoável focar na dimensão dos custos potenciais.

5.1.4. A análise dos impactos é de longo ou curto prazo?

Obviamente, é de interesse ver se é viável medir quaisquer impactos de curto prazo causados pela LATO desde sua aprovação, há apenas dois anos. No entanto, é provável que o efeito total dela seja experimentado com o tempo, e o futuro tem muito mais tempo para provocar quaisquer custos que a LATO possa trazer. Assim, espera-se que provavelmente os impactos econômicos mais significativos da LATO estejam no futuro. Por exemplo, os impactos esperados seriam maiores se toda a amplitude da LATO permanecesse em vigor, o número de Requisições e Notificações da LATO ultrapassasse a baixa escala vista durante seus dois primeiros anos, e se expandisse mais para incluir o uso de Notificações de Capacidade Técnica que exigem dos provedores de serviço mudanças em seus sistemas ou tecnologia.[95]

[93] Há quatro casos possíveis para a razão entre custos e benefícios, quais sejam: grande/grande, grande/pequeno, pequeno/grande, e pequeno/pequeno.

[94] Neste estudo, ignoramos os casos em que os custos são considerados grandes, pois isso tornaria menos provável que a passagem da LATO fosse apoiada por uma avaliação de impacto econômico.

[95] Até o momento, a LATO foi utilizada ao mínimo: foram emitidos menos de 50 TARs (e nenhum TAN ou TCN). (Ver Nota 32 *supra*).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

5.1.5. Como se caracteriza o mundo "controle"?

Tomamos a situação pré-LATO como nosso padrão "controle", mas reconhecemos que em um mundo sem ela, outras coisas teriam acontecido que poderiam ser passíveis de previsão (p. ex., uma versão diferente de LATO ou uma taxa de adoção diferente de tecnologia de criptografia). A identificação de um cenário apropriado representa um problema especial no caso de avaliação do impacto econômico dos investimentos em segurança da informação (ou seja, "InfoSec", como em firewalls, monitoramento aprimorado de segurança e tecnologias de criptografia). O retorno do investimento se baseia no custo dos danos evitados, e qualquer estimativa desse tipo depende da probabilidade de esses danos se concretizarem na ausência do investimento em InfoSec – o que é inerentemente probabilístico e incerto.[96] A elaboração adicional do cenário de controle faria parte de uma avaliação de equilíbrio mais geral dos impactos econômicos da LATO.

5.1.6. Como coletar dados sobre os impactos da LATO?

Os desafios para estimar o impacto econômico se tornam significativamente mais difíceis devido às condições de não divulgação previstas na Lei. Isso impede que os destinatários relatem os detalhes sobre quaisquer avisos da LATO que receberam, ou sobre o que aconteceu como consequência. Elas também evitam que as LEIAs divulguem como podem estar usando a LATO. Isso torna muito difícil isolar os impactos relacionados à LATO de muitos outros impactos que podem afetar o comportamento economicamente relevante da empresa ou os seus resultados (como receitas, investimento em segurança cibernética, etc.). Por exemplo, se as empresas modificam suas práticas de divulgação da marca, publicidade de produto ou suporte ao cliente, não fica claro se estão fazendo isso como resultado de terem recebido um aviso da LATO, em antecipação de como ela poderia impactar seus mercados, ou devido a alguma causa totalmente não relacionada.

Os relatórios sobre as notificações da LATO são atrasados e fornecidos apenas de modo agregado. O número total de emissões é relatado, mas não os tipos de empresas que as receberam. Os Provedores são autorizados a fazerem divulgações estatísticas sobre o número total de notificações recebidas durante os seis meses anteriores e se eram voluntários (TARs) ou obrigatórios (TANs ou TCNs), mas as empresas não podem detalhar qual Autoridade fez emissão ou mais detalhes.

[96] Para a maioria dos investimentos, um usuário observará os benefícios decorrentes do uso das ferramentas permitidas pelo investimento (por exemplo, um carro e a viagem por ele permitida podem autorizar que o investimento seja amortizado ao longo da distância percorrida). Com os investimentos em segurança cibernética, o benefício deriva dos danos não ocorridos (p. ex., a redução da incidência de fraude ou custos sentidos no caso de uma violação de dados). Como no seguro contra incêndio, um consumidor gostaria de poder recuperar todos os pagamentos feitos nos anos anteriores em que não sofreu um incêndio.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Os Provedores podem solicitar autorização para divulgar informações sobre o auxílio.[97] Mas é incerto se buscarão essa autorização e se ela será concedida. Por exemplo, qualquer Provedor induzido a fornecer auxílio que realmente ameace ou possa ser percebido como uma ameaça à segurança digital de seus produtos ou serviços pode estar inclinado a não divulgar nada, por medo do potencial impacto adverso sobre a marca.

A transparência total sobre como a LATO está sendo usada pelas Autoridades provavelmente prejudicasse a eficácia das atividades auxiliadas pela Lei e pudesse representar riscos adicionais à segurança cibernética.[98] Todavia, o bloqueio quase total de quaisquer dados sobre como ela está sendo usada torna quase impossível qualquer avaliação precisa de seus impactos econômicos.[99]

Além disso, as lacunas nos dados relacionados à LATO, juntamente com as regras de porto seguro (disposições de reembolso que permitem aos Provedores solicitar a recuperação de custos relacionados à assistência e a ambiguidade no que os Autoridades podem solicitar ou exigir), têm o resultado perverso de poderem aumentar os danos econômicos esperados da LATO. É mais provável que esses danos se associem a efeitos indiretos, uma vez que, juntos, esses recursos da LATO reduzem os incentivos para os Provedores resistirem em atender às requisições das LEIAs, ainda que possam representar uma ameaça à segurança digital.

Um Provedor que coopera tem menos chance de ser penalizado por sua cooperação por parte de seus clientes ou outras entidades com as quais faz negócios. Essas outras entidades ou clientes só podem supor se o Provedor recebeu um aviso e como respondeu. O sigilo em torno do uso da LATO aumenta para os negócios uma incerteza que confronta todas as entidades que

[97] Ver a sessão 186 (2) da Lei TIA, Nota 14 *supra* e a sessão 317ZF (13) a (17) da LATO, Nota 2 *supra*. Também, ver "Assistência e acesso: mitos comuns e equívocos" ("*Assistance & Access: Common myths and misconception*"), Nota 146 *infra*.

[98] Por exemplo, a transparência total incluiria informações sobre quais Provedores receberam notificações, o que foi solicitado ou exigido que eles fizessem, o que foi feito em resposta, quais Autoridades emitiram as notificações e o que fizeram como consequência do auxílio prestado pelos Provedores. Obviamente, esse nível de divulgação pública serviria de aviso para os alvos de interesse das Autoridades (p. ex., criminosos em potencial), o que lhes permitiria tomar ações evasivas para conter os esforços investigativos das Autoridades. A divulgação completa também poderia revelar detalhes sobre as ferramentas de segurança das Autoridades ou dos Provedores que seriam exploráveis por terceiros, gerando riscos adicionais de segurança cibernética.

[99] Para estimar o impacto econômico da LATO, a divulgação não precisa ser completa nem pública. Dados mais granulares e detalhados podem facilitar melhores estimativas, mas mesmo dados relativamente grosseiros sobre os tipos de assistência que foram solicitados, exigidos e/ou fornecidos superariam em grande parte as lacunas de dados. Além disso, esses dados podem ser divulgados sob ordens de proteção que restringem o relato de dados detalhados usados para estimar os impactos econômicos agregados por analistas ou pesquisadores encarregados de derivar as estimativas. Está além do escopo deste relatório especificar qual divulgação mínima pode facilitar estimativas razoáveis de impactos econômicos Entretanto, acreditamos que um acesso mais protegido a dados relevantes poderia ser autorizado para facilitar a estimativa de impactos econômicos, preservando a eficácia do auxílio da LATO às Autoridades.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

podem ser afetadas pela LATO. Esses impactos se ampliam à medida que as partes interessadas têm que adivinhar se qualquer um dos Provedores, ou a totalidade deles, pode ter tido que cumprir notificações ou requisições da LATO.

Finalmente, a mesma falta de acesso aos dados relacionados à LATO que inibe a estimativa de seus impactos econômicos também torna mais difícil sua supervisão.[100] Uma maior percepção de que essa supervisão esteja inadequada pode contribuir para a percepção do risco sobre abusos das Autoridades que ameacem a segurança digital e, portanto, a confiança digital. Agrava, assim, qualquer impacto econômico adverso que a LATO possa ter.

5.2. Discussão qualitativa dos impactos econômicos

Conforme observado acima, os impactos econômicos da LATO provavelmente serão diretos e indiretos, aumentarão e mudarão ao longo do tempo e terão efeitos colaterais além da Austrália. Alguns desses impactos podem ser mais facilmente observáveis e quantificáveis do que outros. Por exemplo, avaliar os efeitos diretos da LATO, concentrar-se primeiro nas empresas que são obrigadas pelo escopo da legislação a responder aos Requisições e Notificações da LATO, e nos produtos e serviços oferecidos por essas empresas que fazem uso de dados criptografados, seja em trânsito ou em repouso, provavelmente oferecerá a melhor oportunidade para detectar os impactos econômicos comportamentais ou relacionados a resultados da LATO que podem ser medidos.

Em primeiro lugar, as Requisições e Notificações da LATO só podem ser direcionadas aos Provedores, termo interpretado amplamente para incluir qualquer empresa que ofereçam serviços ou produtos de Tecnologia da Informação e Comunicação (ICT) que possibilitem o uso de dados criptografados na Austrália (tenham ou não essas empresas sede no país).[101] Mesmo este escopo apresenta uma complexa "cadeia de suprimentos"[102] de empresas

[100] Na verdade, estimar o impacto econômico da LATO faz parte da supervisão necessária para proteger a Austrália e outros países dos efeitos de uma legislação equivocada.

[101] Este escopo exclui a consideração de empresas ou usuários finais que possam ser os compradores de serviços de TIC que façam uso de dados criptografados (p. ex., hospitais, bancos e outros). No entanto, uma vez que os usuários finais constituem a última demanda para o uso dos serviços de dados criptografados, o impacto da LATO em seu comportamento e os resultados que experimentam (p. ex., nos preços que pagam e na seleção dos produtos que podem escolher, ou de forma equivalente, a qualidade desses produtos) também é relevante para a avaliação do impacto econômico total da Lei.

[102] Os termos cadeia de suprimentos, cadeia de valor ou cadeia de produção podem ser usados aqui de forma intercambiável. Elas refletem o conceito de que a produção da maioria dos bens e serviços pode ser organizada em uma cadeia de tarefas ou estágios que vão desde os recursos brutos, passando pelos estágios intermediários de produção, até as últimas vendas aos usuários finais. Em sua forma mais simples, isso é visto como um fluxo linear de estágios que podem ser organizados em uma série de empresas fornecedoras e distribuidoras, com algumas empresas sendo verticalmente integradas em vários estágios sequenciais. As empresas que operam no mesmo estágio são concorrentes horizontais, enquanto as empresas que operam em diferentes estágios são concorrentes verticais. Nesse sentido, a competição é, em última instância, pela demanda final que fornece os fluxos de receita que sustentam a atividade da cadeia de suprimentos. No entanto, a maioria dos processos de produção, especialmente

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

fornecedoras e distribuidoras. Elas são coletivamente responsáveis por entregarem serviços e produtos de dados criptografados para uso (consumo) por usuários finais, inclusive outras empresas que fazem uso de dados criptografados em suas operações diárias (p. ex., bancos, hospitais e, de fato, a maioria das empresas hoje, mas com variados graus de importância para suas operações) e consumidores do mercado de massa (p. ex., usuários domésticos de serviços de banda larga móvel e fixa).

A cadeia de suprimento inclui os fornecedores que produzem tecnologias de criptografia, equipamentos e serviços, tais como as empresas que fabricam o equipamento de rede, contribuem para o desenvolvimento de padrões internacionais, possuem patentes ou marcas registradas para tecnologias de segurança, etc. Essas empresas, vagamente caracterizadas como "InfoSec", vendem produtos de software e hardware usados para autenticar credenciais digitais, filtrar e bloquear seletivamente o tráfego digital (p. ex., firewalls) e diversos outros serviços (p. ex., atualizações sobre monitoramento de tráfego em segurança cibernética) que são adquiridos e usados por Provedores distribuidores, a exemplo de Provedores de Serviços de Internet (ISPs, de "*Internet Service Providers*"), tais como Telstra e TPG, ou provedores de serviços em nuvem ou nas pontas, que fornecem aplicativos e serviços de conteúdo, tais como Facebook, Google ou Netflix. Incluem-se fabricantes de dispositivos para usuários finais, e desenvolvedores e fornecedores de programas e serviços de aplicativos que fazem uso desses dispositivos, desde smartphones a tablets e aparelhos de Internet das Coisas (IoT).

Rastrear as relações comerciais entre empresas de TIC é complicado. Elas vendem entre si e diretamente para usuários finais (p. ex., redes de dados privadas internas atuando com empresas e consumidores do mercado de massa). Além disso, muitas empresas de TIC operam em diferentes níveis dentro da cadeia de suprimento e podem vender simultaneamente componentes e tecnologia para empresas como fornecedores para as mesmas empresas com as quais competem simultaneamente nos mercados de distribuição (p. ex., a Apple compra componentes da Samsung, elas cruzam licenças de tecnologia e ambas vendem smartphones).

Para analisar o impacto econômico da LATO, pode-se observar toda a cadeia de valor de TIC que fornece produtos e serviços que fazem uso de criptografia ou dados criptografados; enxergar toda essa cadeia de valor como uma "caixa preta" que fornece uma gama de produtos e serviços, os quais usam dados criptografados; e focar em como a Lei pode impactar a oferta e a demanda agregadas por esses produtos e serviços. Em nível abstrato e em uma economia cada vez mais digital, isso pode ser observado para incluir todos os bens e serviços, uma vez que praticamente tudo em uma economia moderna faz uso direta ou indiretamente das TIC. Cada vez mais, a criptografia de dados é vista como uma "melhor prática" chave para garantir que produtos e serviços de TIC sejam "confiáveis" ou protegidos de forma equivalente contra riscos cibernéticos. Esses incluem violações de dados que possam ameaçar a privacidade, e outras formas de perda econômica (p. ex., fraudes, ataques de *ransomware*, destruição de valor, perda de segurança pessoal, etc.).

quando se trata de produtos e serviços de TIC, não se encaixa perfeitamente neste modelo. Existem vários processos paralelos e complexos ciclos de retroalimentação. As empresas podem ser concorrentes verticais e horizontais simultaneamente.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Nessa perspectiva, pode-se ver a LATO impondo custos à proteção de dados e, com isso, ameaçando a "confiança" de produtos e serviços digitais. Isso inclui a confiança no uso da Internet e de outras redes de dados para comércio eletrônico, o que, como já foi observado, incluirá cada vez mais toda a economia. Na análise econômica mais simples, o aumento do custo do fornecimento de serviços de TIC "confiáveis" aumentará os custos de suprimento e reduzirá a disposição dos usuários finais em pagar. Isso sugeriria uma mudança ascendente na oferta agregada e uma mudança descendente na demanda agregada, resultando em um novo preço de equilíbrio pós-LATO mais alto, em um nível mais baixo de demanda agregada. Os preços seriam mais altos e a demanda agregada mais baixa, produzindo o que os economistas chamam de "perda de peso morto", associada à aplicação da LATO.

Se essa análise simples dos efeitos fosse a história completa, então, claramente, seria irracional ter adotado tal política. Os fatores complicadores incluem o fato já observado de que estamos ignorando as formas potenciais em que a LATO pode aumentar a confiança: permitindo que a polícia seja melhor em prevenir crime, gerando uma mudança líquida ascendente na demanda agregada que pode mais do que compensar qualquer ameaça para a qual a Lei possa ser considerada a causa, em decorrência de um aumento na percepção do risco de perder privacidade; ou em razão de custos mais altos que as empresas sentirem, dadas as restrições que a LATO impõe ao uso de tecnologias de criptografia.

Uma complicação adicional na análise da LATO é que os efeitos provavelmente não serão uniformes em todos os setores da economia; nos diferentes estágios da cadeia de suprimentos de TIC; ou em produtos e serviços que usam criptografia e, portanto, em sua demanda final. Uma maneira de enfrentar esse desafio é aplicar conceitualmente a estrutura acima separadamente a diferentes setores, estágios de produção de TIC, ou "mercados" para produtos e serviços e, em seguida, modelar as interações entre essas diferentes análises de economia parcial e equilíbrio parcial para calcular os efeitos totais. Essas análises podem ser realizadas construindo um modelo de entrada-saída adequadamente detalhado da economia ou da cadeia de suprimento de TIC, que rastreie as compras e vendas que as empresas ou agregados de empresas (ou "indústrias" ou "setores da indústria") fazem uns dos outros, e o impacto da LATO nos preços e quantidades dessas transações. Em princípio, quanto mais detalhado o modelo e quanto melhores os dados, as ferramentas de modelagem e previsão forem para a implementação do modelo, melhor será a imagem que se poderá obter dos efeitos agregados e distributivos da LATO.

Tal modelo econômico ideal permitiria considerar como as empresas de TIC, empresas de usuários finais, e consumidores individuais mudariam seu comportamento em resposta à LATO e seu impacto, primeiro nas empresas diretamente impactadas e, em seguida, como consequência das reações das outras e assim por diante. As respostas comportamentais diretas e indiretas dos negócios se propagariam através do modelo, produzindo um novo resultado de equilíbrio. Este poderia ser comparado ao equilíbrio pré-LATO (ou seja, o mundo "controle"), para ver se os benefícios líquidos agregados totais para a economia australiana, ou mesmo global, foram maiores ou menores com a LATO, e para mostrar como os benefícios agregados totais estão distribuídos.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Infelizmente, esse modelo ideal não é viável porque nenhum dos elementos necessários para o seu desenvolvimento existe. Antes de considerar as ferramentas e métodos econômicos disponíveis para a construção de tal modelo idealizado, é suficiente observar que a quase completa falta de dados relevantes, por si só, é um impedimento suficiente para a estimativa do impacto econômico de LATO, independentemente da perspectiva de escopo adotada. Não existem dados nem mesmo para identificar de forma inequívoca, muito menos para medir os impactos comportamentais e de resultados, no subconjunto de empresas da cadeia de suprimento de TIC que serão impactadas pela LATO.

Os defensores do LATO assumiram a perspectiva de que quaisquer impactos econômicos adversos da LATO provavelmente seriam mínimos porque:

- Apenas os Provedores que recebem avisos da LATO seriam afetados,
- A LATO prevê a recuperação de custos razoáveis sentidos na resposta a notificações, e
- A LATO impede as LEIAs de solicitar aos Provedores que façam qualquer coisa que gere dano sistêmico à segurança de seus produtos e serviços.[103]

Ou seja, o argumento deles é que poucas empresas serão afetadas e as implicações sobre a confiabilidade ("qualidade") e o preço ("custo") dos produtos e serviços dessas empresas serão insignificantes e, portanto, a LATO não gerará nem um efeito adverso significativo, nem impactos econômicos adversos, distributivos ou agregados.

Os oponentes à previsão legal de acessos excepcionais como a LATO, incluindo a maior parte da comunidade técnica global e da indústria de TIC, contestam ambas as reivindicações. Tomamos como evidência desta visão consensual o Relatório Carnegie (2019) que ecoou as conclusões alcançadas anteriormente por um artigo prévio da autoria de alguns dos mesmos especialistas. Concluiu-se não haver maneira conhecida de permitir o tipo de acesso direcionado a dados criptografados previsto pela LATO que não gere a criação de vulnerabilidade sistêmica.[104]

Ao enquadrar a análise dos potenciais impactos adversos da LATO, a criação de uma vulnerabilidade sistêmica - e, portanto, a permissão do acesso direcionado a dados

[103] O dano sistêmico à segurança digital se diferencia de uma redução seletiva na segurança digital para o(s) indivíduo(s) estritamente definido(s) como alvo(s), que é(são) o foco de uma notificação da LATO.

[104] See ENCRYPTION WORKING GROUP, "Movendo a conversa sobre política de criptografia para frente" ("*Moving the Encryption Policy Conversation Forward*"), Carnegie Endowment for International Peace, 10 de setembro de 2019, disponível em https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573. O relatório resumiu a conclusão de um Grupo de Trabalho de Criptografia ("*Encryption Working Group*") convocado pela Fundação Carnegie para prover a orientação de pesquisadores seniores da comunidade de segurança cibernética sobre como lidar com leis que prevêem acesso legal. A conclusão geral foi que eles não viam (ainda) nenhuma maneira de permitir amplamente esse acesso legal sem a introdução de vulnerabilidades sistêmicas.

criptografados que a LATO oferece - terá um impacto adverso sobre a "confiança" na segurança cibernética.[105] Esse impacto adverso pode advir de múltiplos efeitos.

Em primeiro lugar, o potencial de a LATO levar ao acesso de uma Autoridade a dados que anteriormente o alvo via como seguros significa que o alvo experimenta uma redução na segurança cibernética. Em segundo lugar, uma vez que a LATO deixa inerentemente incerto quais dados serão alvo de investigação, isso significa um aumento no risco cibernético para todos.[106] Terceiro, se aceitarmos a visão do Relatório Carnegie de que não há maneira conhecida de habilitar o acesso direcionado sem inserir uma vulnerabilidade sistêmica, a aplicação da LATO reduziria a segurança cibernética diretamente para quaisquer sistemas ou serviços que sofressem essa inserção. Juntos, esses efeitos sugerem que a LATO resulta em maior risco de segurança cibernética.

Além disso, mesmo que fosse viável limitar a vulnerabilidade sistêmica, os comentários apresentados durante a consulta pública sobre a LATO antes de sua promulgação em dezembro de 2018 destacaram as múltiplas maneiras pelas quais sua aprovação aumentou a incerteza, em relação aos poderes do governo para potencialmente impactar de modo adverso a segurança cibernética.[107] Portanto, mesmo que se determinasse como sendo trivial a ameaça real à cibersegurança, ou equivalentemente, o aumento do risco cibernético, a percepção do potencial de impacto adverso poderia prejudicar a confiança e resultar em significativos efeitos econômicos potencialmente adversos, que não seriam limitado apenas a empresas de TIC ou Provedores que possam ser destinatários de notificações da LATO.

Portanto, uma maneira de pensar sobre a LATO é considerar qual pode ser o impacto econômico agregado de uma queda da confiança na segurança cibernética. Essa queda reduziria a demanda e a atividade na economia digital, o que reduziria ou atrasaria (o que reduz o valor

[105] Usamos "confiança" aqui abstratamente para nos referirmos às percepções que as partes interessadas (clientes, empresas, formuladores de políticas, etc.) têm na segurança cibernética, o que apenas aponta de forma imperfeita para qualquer que seja o estado real da segurança cibernética.

[106] Pode-se argumentar que, devendo apenas os criminosos serem alvo de requisições de acesso autorizado, a probabilidade de cidadãos honestos serem alvo algum dia é suficientemente pequena e pode ser ignorada. Mas isso depende de se aceitar a suposição de que os poderes da LATO não seriam abusados por acidente, nem de propósito, e ambas são preocupações legítimas.

[107] O Ministério do Interior australiano (DHA) publicou 343 dos comentários recebidos durante a consulta pública [ver DEPARTMENT OF HOME AFFAIRS (2018). "Submissões recebidas de consulta pública" ("*Submissions received from public consultation*"), Projeto de Lei de Assistência e Acesso de 2018 (*The Assistance and Access Bill 2018*). Consultas (*Consultations*), disponível em https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/the-assistance-and-access-bill-2018]. As preocupações comuns expressadas por muitos comentadores incluíram a falta de clareza em relação ao escopo dos poderes da LATO, a eficácia das proteções e supervisão, a falta de transparência e a falta de qualquer análise empírica sobre o impacto econômico da Lei. Todas essas, e os desafios subsequentes, contribuíram para aumentar a incerteza quanto ao provável impacto da LATO sobre a cibersegurança.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

econômico presente) o crescimento da produtividade e da inovação impulsionadas pelas TIC.[108]

Uma maneira de dimensionar o valor econômico de um aumento do risco cibernético percebido ou uma redução da confiança, em toda a economia, é desenvolver previsões baseadas em cenários do que acontece sob diferentes níveis de confiança. Um bom exemplo de tal análise foi preparado pelo Grupo de Seguros Zurich ("*Zurich Insurance Group*") em 2015.[109] O estudo do Zurich usou um modelo macroeconômico a fim de prever os benefícios potenciais para o crescimento econômico global sob uma variedade de cenários, que diferiam com relação ao nível de confiança em uma Internet segura.

Em um cenário de alta confiança, o comércio eletrônico não é ameaçado pelo crime cibernético e o crescimento econômico é mais rápido; ao passo que, no pior cenário, o crime cibernético prejudica tanto a confiança na atividade econômica online que o comércio eletrônico cresce muito mais lentamente. O caso-base está em algum lugar no meio. Este estudo apontou para uma lacuna potencial entre as previsões de melhores e piores casos até 2030 de 120 trilhões de dólares, representando uma variação de 6% no PIB global acumulado, demonstrando a grave ameaça que o crime cibernético representa para a economia global. O crescimento mais lento se deve aos efeitos conjuntos da redução na demanda para se engajar no comércio online, e da redução resultante nos incentivos para as empresas do lado da oferta investirem no fornecimento de capacidade para suportar um crescimento mais lento da demanda.

Para trazer esse contexto mais perto da Austrália, um relatório da AustCyber (julho de 2020) estimou que a atividade digital "contribui com AU$ 426 bilhões para a economia australiana e gera AU$ 1 trilhão em produção econômica bruta, gerando 1 em cada 6 empregos".[110] Esse

---

[108] Há uma significativa literatura econômica demonstrando que o investimento em TICs tem o potencial de gerar significativos retornos excedentes e contribuir para o crescimento da produtividade econômica. Para um resumo, ver LEHR, W.; SHARAFAT, A. (2017), "Mecanismos de TIC para o desenvolvimento sustentável" ("*ICT Engines for Sustainable Development*"), em SHARAFAT, A.; LEHR, W. (eds.). "Crescimento econômico, inovação e criação de empregos centrados em TIC" ("*ICT-centric economic growth, innovation and job creation*"), Genebra, Suíça: União Internacional de Telecomunicações (UIT), 2017, disponível em https://www.itu.int/dms_pub/itu-d/opb/gen/D-GEN-ICT_SDGS.01-2017-PDF-E.pdf; ou BANCO MUNDIAL (2016), "Relatório de Desenvolvimento Mundial 2016: Dividendos Digitais" ("*World Development Report 2016: Digital Dividends*"), 17 de maio de 2016, disponível em http://www.worldbank.org/en/publication/wdr2016.

[109] Ver ZURICH (2015), "Nexo de risco: Superado por riscos cibernéticos? Benefícios econômicos e custos de futuros cibernéticos alternativos" ("*Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures*"), relatório preparado por Conselho Atlântico ("*Atlantic Council*") e Grupo de Seguros Zurich ("*Zurich Insurance Group*"), setembro de 2015, disponível em http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf.

[110] Ver AUSTCYBER (2020), "Relatório de confiança digital da Austrália" ("*Australia's Digital Trust Report*"), Rede Australiana de Crescimento da Segurança Cibernética (*Australian Cyber Security Growth Network*), 13 de julho de 2020, 52 páginas, disponível em https://www.austcyber.com/resource/digitaltrustreport2020. O relatório estima que 22% da economia

relatório estimou que uma interrupção digital de quatro semanas devido a um ciberataque generalizado custaria 1,5% do PIB anual da Austrália.[111] Essa é uma estimativa dos efeitos diretos de um ataque bem-sucedido, e um aumento no risco cibernético significa ser mais provável que tal resultado ocorra.

O que esses dois estudos destacam é o potencial de grandes impactos adversos se a segurança digital for comprometida e, portanto, a importância de se aumentar a confiança na segurança digital. Infelizmente, eles não fornecem orientação útil sobre como quantificar o modo pelo qual a LATO pode aumentar o risco cibernético, a não ser para sugerir que os efeitos podem ser muito grandes e impactar toda a economia.[112]

Também é possível considerar que pode haver efeitos adversos regionais ou específicos do setor, resultantes de ameaças assimétricas à confiança. Por exemplo, pode-se esperar que os setores de TIC australianos sofram um choque adverso maior associado à LATO no curto prazo, associado a menos confiança em seus produtos e serviços, do que os setores de TIC em outras nações que não sejam diretamente afetadas. Isso poderia impactar negativamente a competitividade internacional do setor de TIC da Austrália. Pode-se também investigar abaixo do âmbito nacional, para observar subsegmentos dos setores de TIC e outros setores que são heterogeneamente dependentes em maior ou menor extensão do uso de dados criptografados, que seriam vulneráveis devido à LATO.

No âmbito da empresa, pode-se antecipar que a LATO pode resultar em uma variedade de efeitos diretos ou indiretos. Por exemplo, a redução na demanda agregada pelos produtos de uma empresa, devido à redução na confiança do mercado, encolheria o bolo para todas as empresas. Além disso, a extensão em que uma empresa sofreu uma perda ainda maior de confiança pode reduzir a sua participação de mercado na menor demanda agregada. Os efeitos da reduzida segurança de dados podem variar de pequenos (p. ex., a perda de algumas vendas de alguns produtos) a grandes (p. ex., a ameaça existencial para os negócios futuros de uma empresa se a LATO levar os participantes do mercado a desconfiarem do seu compromisso com a transparência e proteção dos dados de clientes).

Este último resultado é uma preocupação relevante para empresas cujos modelos de negócios são baseados em programas de código aberto e em serviços e produtos prontos para o uso ou

---

australiana é sustentada pela atividade digital, respondendo diretamente por 6% do PIB. Os 317 bilhões os setor de atividade digital incluem 16 bilhões de cibersegurança, 35 bilhões de varejo online, 2,7 bilhões de saúde digital, 0,7 bilhões de energia solar, 3,9 bilhões de indústria espacial etc. (página 11).

[111] *Ibidem*, página 5. O relatório estima que AU$ 30 bilhões e 163.000 empregos seriam perdidos como resultado do ataque generalizado.

[112] O impacto pode ser grande se resultar em uma única violação de dados com um impacto grande e generalizado; se resultar em muito mais violações bem-sucedidas, cada uma pequena, mas grande em impacto agregado; ou alguma combinação de ambos. A questão é que as vulnerabilidades de segurança cibernética podem resultar em vários tipos de danos que diferem em gravidade e escopo. Na ausência de um modelo do cenário de ameaças e da probabilidade de ameaças específicas serem bem-sucedidas, não é possível prever com segurança o esperado dano resultante.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

de mercado de massa (ou seja, não personalizados para um cliente individual). Ao se comprometer com o código aberto como um componente-chave do modelo e da plataforma de negócios, a empresa assume um nível de transparência fundamentalmente incompatível com as restrições da LATO, que limitam a capacidade de divulgar mudanças em suas ofertas, e códigos que podem ser necessários para responder a um aviso da LATO.

Ao avaliar o impacto econômico da LATO, uma empresa individual precisa avaliar a probabilidade de receber uma Requisição ou Notificação da LATO que afetará suas operações, como isso afetaria suas operações, e quais são suas opções de resposta. Isso é semelhante à maneira como as empresas devem avaliar seu risco cibernético e determinar suas estratégias ideais para investir em produtos e serviços de segurança da informação (InfoSec), como firewalls; serviços de monitoramento de tráfego; e outros recursos internos de segurança cibernética, incluindo seguro cibernético (CyberIns) para lidar com qualquer risco cibernético residual que não possa ser tratado de forma adequada por processos aprimorados de segurança cibernética.[113] Algumas das maneiras pelas quais uma empresa individual pode sentir os impactos adversos da LATO são abordadas nas subseções a seguir.

[113] Tomar decisões de investimento sobre InfoSec e CyberIns requer muita informação e, portanto, é caro por si só. ARORA et al. (2004), HUBBARD; SEIERSEN (2016), JONES (2005), GORDON; LOEB (2002) e outros propuseram ferramentas e métodos teóricos de decisão para auxiliar na estimativa de custos cibernéticos, e os benefícios de estratégias alternativas de segurança cibernética para auxiliar na tomada de decisão sobre investimento. Ver ARORA, A.; HALL, D.; PIATO, C.; RAMSEY, D.; TELANG, R. (2004) "Medição do valor baseado em risco de soluções de segurança de TI" ("*Measuring the Risk-Based Value of IT Security Solutions*"), Profissional de TI ("*IT Professional*"), Volume 6, Número 6, Novembro.Dezembro de 2004, DOI: 10.1109/MITP.2004.89, pp. 35-42, disponível em https://ieeexplore.ieee.org/abstract/document/1390871; HUBBARD, Douglas W.; SEIERSEN, Richard (2016) "Como medir qualquer risco de segurança cibernética" ("*How to measure anything in cybersecurity risk*"), John Wiley & Sons: Nova Iorque, 1º de agosto de 2016, DOI: 10.1002/9781119162315, disponível em https://onlinelibrary.wiley.com/doi/book/10.1002/9781119162315; e GORDON, Lawrence A.; LOEB, Martin P. (2002), "A economia do investimento em segurança da informação" ("*The economics of information security investment*") "Transações ACM sobre Segurança da Informação e do Sistema" ("*ACM Transactions on Information and System Security*"), *(TISSEC)*, Volume 5, Número 4, pp. 438-457, DOI: 1145/581271.581274, disponível em https://dl.acm.org/doi/abs/10.1145/581271.581274. Para entender alguns dos desafios associados à avaliação do impacto econômico do crime cibernético, ver WOLFF, Josephine; LEHR, William (2017), "Graus de ignorância sobre os custos das violações de dados: o que os formuladores de políticas podem e não podem fazer sobre a falta de dados empíricos confiáveis" ("*Degrees of Ignorance About the Costs of Data Breaches: What Policymakers Can and Can't Do About the Lack of Good Empirical Data*"), 45ª Conferência de Pesquisa sobre Comunicações, Informação e Política de Internet ("*45th Research Conference on Communications, Information and Internet Policy*") (TPRC45), setembro de 2017, Alexandria, Vancouver, disponível em SSRN: https://ssrn.com/abstract=2943867.

5.3. Aumento da incerteza nos negócios

A LATO eleva a incerteza regulatória, como já observado. A incerteza técnica, mercadológica ou regulatória elevada aumenta o risco de investimentos irreversíveis, o que pode atrasar ou impedi-los. Medir o impacto da incerteza nos negócios é difícil em geral, e não é prático para o efeito de uma lei em particular, como a LATO.

Um indicativo da potencial importância de leis que impactam a incerteza regulatória associada ao uso da tecnologia de criptografia, entretanto, está disponível nos dois únicos estudos conduzidos até o momento que buscaram estimar o impacto econômico da tecnologia de criptografia. Esses estudos foram conduzidos nos EUA pelo Instituto Nacional de Padrões e Tecnologia (NIST, de "*National Institute of Standards and Technology*"), em 2001 e 2018.

No estudo de impacto da criptografia do NIST (2001),[114] os pesquisadores tentaram estimar a contribuição econômica que a promoção, pelo Instituto, do padrão de criptografia de dados denominado DES (de "*Data Encryption Standard*") acrescentou à economia dos EUA. Eles concluíram que os esforços do NIST aceleraram a adoção do DES em vários anos, resultando em benefícios líquidos de US$ 345 milhões a US$ 1.190 milhões, associados a custos mais baixos para o gerenciamento de dados bancários de terceiros.[115]

Um estudo sucessor de 2018 analisou o impacto econômico do Padrão de Criptografia Avançada (AES), em cuja promoção o NIST também desempenhou um papel.[116] Adotou uma

---

[114] Ver LEECH, D.; CHINWORTH, M. (2001), "O Impacto Econômico do Programa do NIST para Padrão de Criptografia de Dados (DES)" ("*The Economic Impacts of NIST's Data Encryption Standard (DES) Program*", estudo preparado pelo Grupo de Planejamento Estratégico e Análise Econômica do Escritório do Programa (*Program Office Strategic Planning and Economic Analysis Group*) do Instituto Nacional de Padrões e Tecnologia dos EUA (*U.S. National Institute of Standards and Technology*) (NIST), outubro de 2001, disponível em https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=918355 (daqui em diante, Estudo de Impacto da Criptografia do NIST de 2001).

[115] O objetivo do estudo era demonstrar como o NIST contribuiu para o crescimento econômico. O estudo de caso documentou o papel do NIST em promover a adoção antecipada de um padrão de criptografia da indústria, em relação ao que teria acontecido de outra forma. O padrão DES foi adotado em 1977 e o estudo analisou o comportamento de adoção de 1977-1982. Os pesquisadores inicialmente tentaram coletar dados de pesquisa para medir diretamente os impactos e não tiveram sucesso. A alternativa que eles usaram foi calcular o impacto com base nos resultados específicos da indústria, fundados nos custos evitados pelos bancos de varejo nos Estados Unidos, que foram capazes de mudar para transações eletrônicas (custo mais baixo) mais rapidamente do que teria sido de outra forma. Eles estimaram os benefícios de redução de custos das transações eletrônicas conforme foram produzidos ao longo do tempo (mundo real) e os compararam a dois cenários de mundo controle (os benefícios teriam sido atrasados em 3 a 6 anos) e calcularam o Valor Presente Líquido (VPL) dos cenários para estimar o efeito líquido dos esforços do NIST.

[116] Ver LEECH, David P.; SCOTT, John (2018), "Os impactos econômicos do padrão de criptografia avançado, de 1996 a 2017" ("*The Economic Impacts of the Advanced Encryption Standard, 1996-2017*"), preparado para o Instituto Nacional de Padrões e Tecnologia (*National Institute of Standards*

abordagem baseada em entrevistas para obter estimativas de como o AES ajudou a reduzir os custos das empresas ativas na implantação de tecnologias de criptografia devido à existência de um padrão federal. No estudo de 2018 do NIST, eles novamente postularam um mundo contrafactual no qual teria sido mais lenta a evolução para o padrão mais eficiente do AES.

Nesse caso, os pesquisadores se beneficiaram por poderem modelar diretamente as melhorias de desempenho que o AES oferecia em relação ao padrão que estava substituindo. O estudo de 2018 estimou que a taxa interna de retorno sobre o investimento do NIST na promoção de AES foi de 81%, significativamente mais do que o custo de capital de 7% do Instituto (de acordo com os regulamentos governamentais), e os benefícios líquidos agregados para a economia ultrapassaram US $ 250 bilhões, uma vez calculados todos os efeitos colaterais diretos e indiretos.

Ambos os estudos concluíram que um pequeno investimento na aceleração da implantação de recursos de criptografia resultou em ganhos muito grandes para a economia. Isso sugere que pode ter um grande impacto negativo ver a LATO como uma intervenção com potencial para atrasar a adoção de técnicas aprimoradas de criptografia (retardando ou inclinando para uma menos segura). Além disso, em ambos os casos, podem-se entender os esforços do NIST em promover a aceitação de um padrão da indústria, como uma ação para reduzir a incerteza dos negócios.

5.4. Danos à Marca da Empresa

As empresas estabelecem sua marca por meio da publicidade e da reputação que constroem a partir da comparação de seus produtos no mercado com as ofertas concorrentes de outras empresas. Quanto melhor a marca, mais fácil é para a empresa vender seus produtos e obter receita com as vendas, defender-se contra concorrentes ou responder às mudanças adversas do mercado, e mais atraente para os investidores se torna a empresa . Todas as outras coisas permanecendo inalteradas ou constantes, uma imagem de marca melhor está associada a vendas mais altas ao longo do tempo e, portanto, a um valor de mercado mais alto (que reflete a avaliação do mercado sobre o valor descontado dos esperados lucros futuros da empresa). É um ativo intangível que não pode ser medido diretamente, mas é avaliado por referência a mudanças em outros indícios mensuráveis, como vendas, lucros, valor de mercado ou pesquisas de investidores ou percepções do cliente.

Qualquer coisa que ameace a percepção relativa da confiança em uma empresa pode prejudicar sua marca e, portanto, suas perspectivas de vendas e valor comercial. Embora clientes, parceiros de negócios, investidores e conhecedores da empresa possam avaliar qualitativamente se a LATO teve um impacto significativo na marca da empresa ou não, esse efeito não pode ser quantificado diretamente.

De acordo com algumas interpretações da LATO, o seu potencial impacto adverso pode ser visto como uma ameaça existencial para algumas empresas cuja marca é altamente dependente

and Technology) dos EUA, NIST GCR 18-017, disponível em https://doi.org/10.6028/NIST.GCR.18-017.

do compromisso com a segurança cibernética e/ou modelos de negócios que dependem de programas de código aberto. Por exemplo, um fornecedor de tecnologia de criptografia de segurança cibernética pode descobrir que seu produto principal está prejudicado pela criação de uma ferramenta na Austrália que ameaça sua oferta de serviço. Em outro caso, ela poderia desfazer o modelo de negócios de uma empresa construído com o compromisso de um programa de computador de código transparente e aberto que não discrimina os usuários finais. Ser obrigado a alterar o código de um alvo e, em seguida, não ser capaz de divulgar essas modificações para o resto de seus clientes (devido aos requisitos de não divulgação da LATO) seria inconsistente com um componente fundamental de seu modelo de negócios. E, em outro caso, uma empresa que constrói seu modelo de negócios com base em código proprietário pode ver um ativo essencial prejudicado se a LATO forçar a empresa a divulgar o código-fonte, que pode vazar para o domínio público.

5.5. Vendas Perdidas

Embora o impacto direto na imagem da marca de uma empresa não possa ser quantificado diretamente em dólares, o impacto nas vendas muitas vezes pode ser. Uma empresa pode ser capaz de rastrear um evento específico como tendo um impacto adverso no comportamento de compra de clientes específicos ou em relação a produtos específicos. Uma empresa pode observar que os clientes compram menos de suas ofertas porque os clientes indicam que estão preocupados com a ameaça da LATO à segurança dos dados.

Essas vendas perdidas podem refletir um menor consumo pelos compradores (p. ex., pela redução na demanda agregada em um mundo menos confiável) ou vendas que mudam para um concorrente. O concorrente pode ser outra empresa no mesmo mercado (Austrália) ou no exterior. As mudanças no comportamento de compra do cliente e, portanto, nas vendas da empresa podem ser rastreadas até subconjuntos específicos de produtos em maior ou menor grau. As empresas costumam entrar em contato direto com clientes reais e potenciais para identificar o que lhes interessa e por que compram o que compram. As empresas também podem inferir isso a partir do que os clientes compram e da inteligência de mercado de terceiros, que busca estimar o valor para os clientes de diferentes recursos relacionados à segurança.

Embora, em princípio, os dados de vendas sejam uma das fontes de efeitos de resultados diretos que podem ser mais facilmente observáveis, atribuir mudanças nas vendas devido uma lei específica como a LATO é sempre um desafio. Primeiro, existem muitos fatores que podem impactar o comportamento dos clientes, e separar os efeitos desses fatores pode não ser viável. Em segundo lugar, quando os efeitos são antecipados no futuro, devem-se considerar os desafios adicionais de prever eventos incertos. Terceiro, os clientes nem sempre são honestos ao explicar por que compram o que compram. Eles podem não querer compartilhar informações porque não querem ofender seu fornecedor, ou por se preocuparem em revelar informações demais e colocar em risco sua posição de barganha. Independentemente da causa, a redução nas vendas normalmente se traduz em lucros reduzidos (sob a suposição razoável de que as empresas evitariam vendas incrementais que não trazem receita suficiente para cobrir seus

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

custos incrementais),[117] e um fluxo futuro reduzido de lucros se traduz em um valor econômico mais baixo para a empresa.

Embora seja desafiador considerar como se podem avaliar as vendas perdidas, há uma série de razões para antecipar porque o risco de um potencial impacto adverso significativo nas vendas pode ser substancial. Por exemplo, em julho de 2020, o Tribunal de Justiça Europeu emitiu uma decisão amplamente prevista que invalidou o emprego de uma solução alternativa que permitia às empresas dos EUA e da Europa trocarem dados de seus clientes, sem violar regulamentos de privacidade europeus vigentes, aumentando o risco de que fossem exigidos dessas empresas ou o aumento da proteção de dados ou o encerramento das trocas.[118]

A LATO pode ser vista como uma ameaça à capacidade de atender aos padrões de proteção de dados mais rigorosos adotados pela União Europeia e, portanto, representar uma ameaça à capacidade das empresas de trocar dados entre a Austrália e a União Europeia. Além disso, na medida em que o LATO é indicativa de novas ampliações dos poderes do governo na Austrália, ou em outro lugar, para obrigar o acesso a dados confidenciais, isso poderia levar a mais interrupções nos fluxos de dados.[119] Uma vez que as trocas internacionais de dados são críticas para o funcionamento saudável da economia digital global, o colapso dessas trocas tem um potencial impacto desastroso no comércio digital global.

5.6. O custo operacional aumenta devido à LATO

Os custos da empresa podem aumentar como resultado da LATO. Em primeiro lugar, pode haver custos diretos sentidos por uma empresa que recebe uma Requisição ou Notificação da LATO. Os custos ocasionados dependeriam do cumprimento voluntário (Requisições da LATO) ou obrigatória (Notificações da LATO) e dos requisitos específicos de qualquer Aviso da LATO.

---

[117] Aqui, estamos ignorando estratégias de curto prazo, como vendas de líderes de perdas ou operações de negócios durante uma recessão temporária.

[118] Ver FENNESSY, Caitlin (2020). "A decisão 'Schrems II': transferências de dados UE-EUA em questão" ("*The 'Schrems II' decision: EU-US data transfers in question*") Privacy Tracker, Associação Internacional de Profissional de Privacidade (*International Association of Privacy Professionals*) - IAPP, 16 de julho de 2020, disponível em https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

[119] Por exemplo, a Nova Zelândia tem uma decisão de adequação da UE, e a LATO pode afetar adversamente as decisões de entidades da Nova Zelândia em usar hospedagem ou outros serviços fornecidos por empresas australianas sujeitas a ela [ver "Decisões de Adequação" ("*Adequacy Decisions*"), União Europeia https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_pt e Decisão de Execução da Comissão de 19 de dezembro de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela Nova Zelândia [notificada com o número C(2012) 9557] (Texto relevante para efeitos do EEE) (2013/65/UE), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02013D0065-20161217].

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

A LATO tem previsões destinadas a mitigar os custos diretos de responder aos avisos da LATO (a) permitindo que os destinatários recuperem os custos incrementais de resposta; e (b) limitando o escopo das requisições da LATO àquelas que não resultariam na inserção de vulnerabilidades sistêmicas. Dada a dificuldade em estimar os custos totais de resposta a requisições ou notificações da LATO, incluindo efeitos diretos e indiretos, é razoável esperar que os Provedores sejam céticos quanto ao compromisso de reembolsar os custos totais do impacto da LATO, ou mesmo a totalidade dos custos diretos de responder a um aviso da LATO.

Adicionalmente, observamos o histórico de como a supervisão tem ficado aquém da eficácia total ao limitar o escopo das agências governamentais que atuam sob novas concessões de autorização.[120] Como resultado, é razoável esperar que os Provedores e outras empresas impactadas pela LATO permaneçam incertas quanto à eficácia das disposições de supervisão, à luz da ausência de transparência, da imprecisão em partes da lei e outros problemas potenciais. Depois de estimar os custos diretos de responder a qualquer Requisição ou Notificação da LATO, a empresa precisaria pesar isso em relação à probabilidade de receber tal Requisição ou Notificação. Quanto menor a probabilidade de a empresa receber um aviso da LATO, menor será o custo direto esperado sentido como resultado.

Além disso, embora o cumprimento das Requisições da LATO seja voluntário, é razoável antecipar que alguns destinatários podem percebê-los como um prenúncio de futuras Notificações da LATO. Portanto, é discutível a visão de que as Requisições da LATO têm um impacto econômico significativamente menor do que as Notificações LATO.

Em segundo lugar, mesmo as empresas que talvez nunca recebam uma Requisição ou Notificação da LATO podem sofrer problemas de imagem de marca ou relacionamento com o cliente, que podem induzi-las a terem que arcar com custos adicionais. Elas podem se sentir compelidas a aumentarem a publicidade da imagem da marca e o marketing direto para compensarem os riscos percebidos em sua imagem de marca, ou perspectivas de venda. Elas

[120] Veja a extensa literatura de economia sobre a escolha do público, e a economia regulatória sobre o deslizamento regulatório, que têm uma longa história, remontando, pelo menos, ao "Riqueza das Nações" de Adam Smith, mas inclui mais notavelmente o trabalho de George J. Stigler, "A Teoria da Regulação Econômica", The Bell Journal of Economics and Management Science vol. 2, No. 1 (Spring, 1971), pp. 3-21; e Peltzman, S. (1976), "Rumo a uma Teoria Mais Geral da Regulação", Journal of Law and Economics, 19, 211-48. Veja também a teoria econômica das burocracias, incluindo agências reguladoras, na tese de maximização do orçamento de William Niskanen, "Burocracia e Economia Pública" (Cheltenham, Reino Unido: Edward Elgar, 1994) que pode impulsionar o deslizamento regulatório. Veja também Helm, Dieter. (2006) "Reforma Regulatória, Captura e Carga Regulatória", Oxford Review of Economic Policy, 22 (2), 169; e Dal Bó, E. (2006), "Captura regulatória: uma revisão", Oxford Review of Economic Policy, 22 (2), 203-25. Para o reconhecimento do problema pelo governo, consulte o Relatório do Gabinete do Reino Unido - Força-Tarefa de Melhoria Regulatória e Subgrupo de Deslizamento Regulatório - 2004: "Evitar o deslizamento regulatório", que definiu o deslizamento regulatório como o processo pelo qual a regulamentação é desenvolvida ou aplicada de forma abaixo da transparência e em desacordo com seus cinco princípios de boa regulamentação: proporcionalidade, responsabilidade, consistência, transparência e direcionamento.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

podem precisar gastar recursos adicionais para lidar com as preocupações reais ou percebidas dos clientes sobre o impacto da LATO na segurança de seus dados e na confiança online.

Terceiro, as empresas podem estar preocupadas com a ameaça da LATO para a segurança dos serviços ou produtos fornecidos por seus fornecedores, ou a segurança das suas próprias operações internas na Austrália. As empresas podem reavaliar suas relações com fornecedores e opções de terceirização (p. ex., para serviços em nuvem de gerenciamento de dados de clientes ou dados confidenciais da empresa) à luz de preocupações elevadas de que esses dados possam estar vulneráveis por causa de respostas comportamentais de fornecedores parceiros, induzidas pela LATO.

Isso poderia levar empresas a mudarem os relacionamentos de terceirização e vendas para o exterior, a fim de evitarem a LATO. Ajustar as relações com os vendedores ou mudar as operações empresariais interna da Austrália gerará custos de ajuste que devem ser diretamente atribuíveis à LATO, ao mesmo tempo que implicará efeitos colaterais adversos sobre outros participantes do setor digital australiano, aumentando assim os efeitos indiretos da LATO.

Quarto, as empresas podem abandonar sua estratégia ideal de segurança cibernética devido às restrições impostas pela LATO. Isso provavelmente se manifestaria como um aumento nos custos de InfoSec e CyberIns para compensar ou lidar com o aumento do risco cibernético associado à LATO. Uma maneira de as empresas estimarem o risco cibernético é estimar a ameaça de diferentes tipos de ataques. Uma das ameaças mais difíceis de enfrentar são as ameaças internas ou crimes cibernéticos perpetrados por funcionários que seriam confiáveis.

Por exemplo, uma fonte comum de violações de dados são funcionários descontentes ou corrompidos motivados pelo desejo de vingança ou ganhos ilícitos contornando as defesas de segurança interna para extrair dados.[121] O melhor firewall do mundo não impede um funcionário que leva para casa arquivos de dados confidenciais em uma unidade USB ou em papel.

A LATO pode ser vista como um aumento das ameaças internas, pois tem o potencial de fazer com que a autoridade do Estado induza um funcionário que seria confiável a contornar os protocolos de segurança da empresa. Pode exacerbar ainda mais esse risco de ameaça interna a falta de transparência e restrições sobre quais informações os destinatários de um aviso da

[121] Embora não haja estatísticas confiáveis sobre a porcentagem de violações de dados causados por ameaças internas, é amplamente aceito na comunidade de segurança que os funcionários que não seguem os procedimentos de segurança propositalmente ou por acidente são geralmente considerados uma das principais fontes de violações de dados. Mas como a maioria não é relatada, e as estatísticas das relatados são incompletas, não se sabe qual porcentagem é interna. Uma pesquisa relatou que "*66% das organizações consideram mais prováveis ataques internos maliciosos ou violações acidentais, do que ataques externos*" [ver GEO, Deyan. "20 estatísticas de ameaças internas a serem observadas em 2020" ("*20 Insider Threat Statistics to Look Out For in 2020*"), Table of Contents, Techjury, 17 de agosto de 2020, cópia arquivada disponível em https://web.archive.org/web/20201022025736/https://techjury.net/blog/insider-threat-statistics/].

LATO podem compartilhar, seja com terceiros (tal como um advogado) ou com outros funcionários dentro da empresa.

Para avaliar os impactos potenciais da LATO nos custos operacionais e de capital de InfoSec e CyberIns de uma empresa, é necessário saber como a empresa usa criptografia para seus dados em trânsito e em repouso; e, conforme observado anteriormente, as opções para modificar as estratégias de InfoSec e CyberIns para lidar com a LATO. Além de dividir os desafios de segurança de dados em aqueles relacionados aos dados em trânsito (p. ex. serviços de comunicação eletrônica como telefonia, e-mail, chat, mensagens, acesso a terminal remoto, etc.) versus dados em repouso (p. ex., arquivos de dados confidenciais, credenciais de segurança etc.), será importante saber como a criptografia é usada internamente pela empresa, em seus relacionamentos com parceiros da cadeia de suprimentos, como fornecedores, e com seus clientes. Em cada um dos seis casos, diferentes considerações e opções econômicas podem ser relevantes (e casos adicionais podem ser necessários para atender a diferentes segmentos de produto, mercado ou cliente).[122]

Quinto, em resposta ao aumento dos esforços nacionais para proteger os dados de seus cidadãos da vigilância estrangeira, as empresas digitais podem ser compelidas a investir em maiores esforços de localização de dados. Por exemplo, após a quebra do acordo anterior que fornecia porto seguro para as trocas internacionais de dados dentro da União Europeia após a decisão Schrems I em 2015, a Microsoft investiu no fornecimento de uma solução de localização de dados na Alemanha, que foi posteriormente abandonada em 2016, uma vez que um novo acordo de compartilhamento com porto seguro foi adotado pela indústria.[123]

---

[122] Os seis casos são para (usos de dados em repouso / em trânsito) x (Interno / Relações com fornecedores / Clientes).

[123] Ver HERNANDEZ, Pedro (2016), "Nuvem da Microsoft na Alemanha é aberta usando um modelo de fidúcia de dados" ("*Microsoft Cloud Germany opens using a Data Trustee Model*"), eWeek, 22 de setembro de 2016, disponível em https://www.eweek.com/cloud/microsoft-cloud-germany-opens-using-data-trustee-model para artigo de imprensa comercial de 2016, quando a Microsoft anunciou o novo acordo; e PRADEEP (2018), "A Microsoft está descontinuando o modelo alemão de fidúcia de dados" ("*Microsoft is discontinuing the German data trustee model*"), Microsoft Power User, 5 de setembro de 2018, disponível em https://mspoweruser.com/microsoft-is-discontinuing-the-german-data-trustee-model/ de quando a Microsoft anunciou que estava interrompendo seu esforço de localização de dados. Embora a Microsoft não identifique as implicações do custo de implementar e abandonar seu modelo de fidúcia de dados, é razoável prever que o projeto custará milhões de dólares. Seguindo a decisão mais recente do Schrems II, ao derrubar o porto seguro que havia sido estabelecido alguns anos após o Schrems I, a Microsoft reafirmou seu compromisso em proteger a confidencialidade dos dados de seus clientes [ver "Novas etapas para defender seus dados" ("*New steps to defend your data*"), Blog da Microsoft, 19 de novembro de 2019, disponível em https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/]. Ver GAUDINO, Francesca; SEINEN, Wouter; SMALL, Harry; DEHARENG, Elisabeth; HENGESBAUGH, Brian; WALTER, Andre (2019). "Schrems I", Proteção de Dados (*Data Protection*), Baker Makenzie, dezembro de 2019, disponível em https://www.bakermckenzie.com/en/-/media/files/insight/publications/2019/12/schrems-ibackgroundv6.pdf para mais informações sobre a decisão Schrems, e para a decisão mesma, ver "Acórdão do Tribunal de Justiça (Grande Secção) de 6

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Ao abandonar a solução provisória, a Microsoft sinalizou os custos mais altos e a reduzida eficiência para o cliente resultante da adoção de uma solução de localização de dados. Essas soluções aumentam os custos e diminuem a eficiência, limitando a capacidade de empresas multinacionais realizarem economias de escala e escopo. Aumenta o custo da atualização de programas de computador [incluindo a distribuição de remendos (*patches*) de software para resolver novos problemas de segurança] porque são assumidos custos de criação de respostas diferenciadas por mercado, junto com os custos indiretos adicionais associados ao gerenciamento de um processo de atualização mais complexo.

5.7. Redução nas oportunidades de crescimento futuro devido à LATO

Finalmente, a LATO pode fazer com que as empresas repensem seus planos de investimento estratégico em relação ao desenvolvimento e lançamento de novos produtos e recursos. Isso pode levar as empresas a alterarem seus planos de lançamento ou os preços de novos produtos e conjuntos de recursos que agreguem valor. Isso pode levar as empresas a decidirem não oferecer certos produtos na Austrália, a fim de protegê-los do impacto da LATO. Além de reduzir as vendas futuras da empresa e o potencial de crescimento (ou o excedente do produtor), isso também nega aos consumidores os benefícios da escolha adicional e, assim, reduz o excedente do consumidor.

Menos investimento em produtos novos e mais seguros pode se traduzir em menos investimento em capacidade empresarial, incluindo investimento em P&D e inovação de produtos. Eles podem ser adiados, abandonados ou transferidos para fora da Austrália. Em qualquer caso, há uma perda direta e indireta para a economia australiana.

5.8. Impactos globais e de longo prazo

Embora a LATO tenha sido aprovada em 2018, dois anos depois, ela continua sujeita a desafios que tornam incerto seu futuro de longo prazo. Se a Lei realmente representa uma ameaça para adoção e segurança mais amplas dos serviços de criptografia e, portanto, à segurança digital e, logo, à confiança no comércio digital, a adoção mais ampla de normas jurídicas semelhantes em todo o mundo ampliará o impacto adverso. Por outro lado, os impactos adversos descritos acima serão temporários e evitados se a probabilidade de serem utilizadas as ferramentas autorizadas pela LATO for suficientemente reduzida pelos desafios contínuos para a Lei, e pelas preocupações sobre a ameaça que ela representa para a segurança digital.

---

de outubro de 2015. Maximillian Schrems contra Data Protection Commissioner. Pedido de decisão prejudicial apresentado pela High Court (Irlanda). Identificador Europeu da Jurisprudência (ECLI): ECLI:EU:C:2015:650". Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62014CJ0362. Para a decisão Schrems II, de julho de 2020, ver "Acórdão do Tribunal de Justiça (Grande Secção) de 16 de julho de 2020. Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems. Pedido de decisão prejudicial apresentado pela High Court (Irlanda). Processo C-311/18. Identificador Europeu da Jurisprudência (ECLI): ECLI:EU:C:2020:559", disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62018CJ0311&qid=1622956815449.

No atual estágio, é impossível prever qual desses cenários seja mais provável.

5.7. Resumindo

Os impactos econômicos diretos e indiretos da LATO podem ser atribuídos aos efeitos da Lei na redução da confiança na segurança cibernética. Os custos diretos associados à resposta a Requerimentos e Notificações da LATO são provavelmente a menor e menos importante fonte dos custos totais, uma vez que o número de destinatários reais da LATO provavelmente permanecerá pequeno.

Os efeitos indiretos, no entanto, incluirão o impacto que a LATO tem em todos os setores da economia como potenciais destinatários diretos, o que inclui todos os Provedores. E as empresas e clientes com os quais eles interagem respondem ao aumento do risco cibernético representado pela Lei. Espera-se que esses custos totais se acumulem ao longo do tempo, à medida que efeitos indiretos se propaguem em ondas no setor de TIC da Austrália, dele para outros setores da economia australiana, para as economias globais e, em seguida, de volta, através dos ciclos de retroalimentação que compõem nosso ecossistema econômico global interconectado.

O estudo do Zurich (2015)[124] e o relatório da AustCyber (2020)[125] indicam que os potenciais danos indiretos resultantes de uma ameaça à confiança digital seriam medidos em bilhões de dólares. Embora isso não forneça nem mesmo uma estimativa da ordem de magnitude dos custos agregados da LATO, é suficiente para demonstrar ser grande o potencial para danos causados nacional e internacionalmente.

Há evidências empíricas anedóticas e parciais que sugerem que o impacto da LATO pode gerar significativos efeitos indiretos. Argumentos qualitativos sólidos também sugerem que os potenciais impactos adversos (custos líquidos) da LATO podem ser realmente grandes. No entanto, não há evidências empíricas diretas para quantificar esses efeitos.

Nós vasculhamos pesquisas publicamente disponíveis e não encontramos estudos empíricos relevantes, ou dados adequados para se desenvolverem estimativas materiais. Para enfrentar este desafio, como parte deste projeto, empreendemos uma nova pesquisa partindo do zero, coletando as opiniões de grandes empresas estrangeiras multinacionais de tecnologia, e um grande número e uma ampla gama de empresas australianas, sobre os prováveis efeitos da LATO em seus negócios: se eles acreditam que qualquer um dos impactos observados acima teria ocorrido e, em caso afirmativo, quaisquer estimativas que eles tenham dos impactos em dólar.

Esta pesquisa envolveu dois elementos. Primeiro, entrevistas em profundidade por videoconferência com os principais provedores de comunicações multinacionais regulamentados pela LATO. Em segundo lugar, uma enquete anônima com um grande número de provedores de comunicações regulados pela LATO e empresas relacionadas, afetadas na

[124] Ver Nota 109 *supra*.

[125] Ver Nota 110 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Austrália pela Lei. Os resultados deste trabalho são apresentados no próximo capítulo. Em resumo, os resultados suportam a conclusão de que o impacto econômico líquido da LATO foi negativo e que ela representa um risco de futuros danos substanciais.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

6. Resultados da pesquisa empírica

Como parte de nossa análise do impacto econômico da LATO, nós (1) conduzimos entrevistas confidenciais detalhadas por videoconferência com nove grandes empresas com operações na Austrália que são diretamente afetadas pela Lei (ou seja, podem ser consideradas Provedores cuja equipe pode ser destinatária de avisos da LATO); e (2) fizemos uma enquete anônima com empresas operando na Austrália que podem ser direta ou indiretamente impactadas pela LATO.

Conforme explicamos mais detalhadamente no resumo deste capítulo, os resultados das entrevistas e da enquete anônima fornecem suporte empírico (limitado) e são totalmente consistentes com nossa avaliação sobre o impacto econômico da LATO. As percepções gerais alcançadas incluem:

1. A expectativa de que a LATO terá um impacto adverso generalizado sobre as empresas e seus clientes (ou seja, não limitado apenas aos setores de TIC).
2. A maioria dos danos esperados serão indiretos e associados à ameaça que a LATO representa para as percepções, de clientes e parceiros da indústria, sobre a confiança digital.
3. A incerteza significativa sobre a LATO (e seus efeitos) continua.
4. A evidência empírica direta de custos (ou benefícios) econômicos é bastante limitada, mas atribuímos isso a (a) a opacidade que envolve as atividades da LATO devido às previsões de não divulgação; (b) o tempo limitado desde a aprovação da LATO, e a persistente controvérsia que reprime o uso da autorização da LATO pelas Autoridades; e (c) a expectativa de que os impactos mais provavelmente sejam indiretos e futuros.
5. A evidência direta limitada que observamos justifica a conclusão de que os benefícios específicos para uma empresa são provavelmente pequenos, enquanto os custos específicos podem ser muito grandes.[126]
6. Os dados empíricos disponíveis não fornecem uma amostra grande o suficiente a fim de serem base confiável para estimar o impacto econômico agregado da LATO.

As nove empresas de tecnologia da informação (TI) selecionadas para entrevistas em profundidade incluíram seis grandes multinacionais de tecnologia com receitas totais de pouco mais de US$ 1 trilhão.[127] As três outras incluíam uma operadora australiana de telecomunicações e dois provedores australianos de serviços eletrônicos. Desses, uma era exportadora de propriedade australiana, e a outra uma investidora e importadora estrangeira de serviços inovadores para a Austrália.

A enquete anônima foi elaborada e lançada, sob direção do LECA, pela *Clarity Strategic Research* (Sydney).[128] A pesquisa foi lançada em dezembro de 2020 e resultou em respostas de

[126] Nossas entrevistas e enquetes focaram nos impactos de que os entrevistados tinham conhecimento em primeira mão.

[127] Para fornecer alguma perspectiva, esta estimativa de receita total é equivalente a quase três quartos do PIB australiano.

[128] Ver site da Clareza Pesquisa Estratégica em https://claritystrategicresearch.com.au/.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

79 empresas. Embora, como explicado anteriormente, o impacto econômico potencial da LATO ocorra em toda a economia e seja razoável antecipar que os impactos econômicos mais significativos possam ser indiretos, direcionamos a enquete para profissionais com experiência em TI. Fez-se isso por ser razoável esperar que profissionais de TI provavelmente estejam mais informados sobre a LATO e as implicações das políticas que afetam o uso de tecnologias de criptografia. Dado o pouco tempo e os recursos limitados disponíveis para realizar a enquete, fomos auxiliados na definição dos respondentes por várias associações comerciais australianas que concordaram em nos ajudar a alcançar seus membros combinados de 16.000 profissionais de TI. Entre eles estão a *Australian Cyber Security Growth Network* (AustCyber),[129] a *Australian Information Industry Association* (AIIA),[130] a *Communications Alliance*,[131] e a *Information Technology Professionals Association* (ITPA).[132]

Nossa enquete se baseou em duas pesquisas anteriores. A primeira foi lançada pela AustCyber em 2018, na véspera da passagem da LATO; enquanto a segunda foi lançada pela Communications Alliance e a ITPA em 2019, após um ano de vigência da Lei. Os resultados das enquetes relatados aqui oferecem outro retrato das percepções e experiências da indústria dois anos após a aprovação do LATO. Um resultado importante que emerge dessa análise é a notável semelhança em termos do que os participantes da indústria anteciparam que seriam os efeitos da LATO, e o que eles relatam ter sido suas experiências e expectativas dali pra frente. Como explicaremos mais adiante, a maioria dos respondentes da enquete esperava impactos econômicos adversos da LATO antes de sua aprovação e essas expectativas se concretizaram, com mais impactos adversos futuros esperados.

Antes de discutir os resultados de nossas entrevistas e pesquisas em profundidade, resumimos brevemente os resultados das duas pesquisas anteriores.

6.1. AustCyber (2018)

Antes da aprovação da LATO em 2018, a AustCyber contratou o Centro de Política Cibernética Internacional (*International Cyber Policy Centre*) do Instituto Australiano de Estratégia Política (ASPI, de *Australian Strategic Policy Institute*) para conduzir uma enquete online sobre a indústria australiana. A pesquisa foi lançada em novembro de 2018 e os resultados publicados em dezembro de 2018.[133] A enquete foi enviada a 512 empresas de TI com

[129] Ver site da Rede Australiana de Crescimento da Segurança Cibernética em https://www.austcyber.com/.

[130] Ver site da Associação da Indústria de Informação da Austrália em https://www.aiia.com.au/.

[131] Ver site da Aliança de Comunicações em https://www.commsalliance.com.au/.

[132] Ver site da Associação de Profissionais de Tecnologia da Informação https://www.itpa.org.au/.

[133] Ver a enquete financiada pela Rede Australiana de Crescimento da Segurança Cibernética e executada pelo Instituto Australiano de Estratégia Política, ASPI (2018), "Enquete de percepções: As Visões da Indústria sobre as Implicações Econômicas do Projeto de Lei de Assistência e Acesso de 2018" ("*Perceptions survey: Industry Views on the Economic Implications of the Assistance and*

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

operações na Austrália e foram recebidas 63 respostas. 76% das empresas "relataram preocupação com o projeto de lei" e "algumas das questões levantadas como principais preocupações pelos entrevistados eram sobre percepções e falta de clareza" com relação ao que a LATO pode exigir das empresas.[134] Por exemplo, 57% dos entrevistados esperavam que a Lei tivesse um impacto negativo em seus negócios na Austrália e, desses, 69% esperavam que o impacto durasse mais de dois anos;[135] e 65% dos entrevistados que se identificaram como exportadores esperavam que a LATO tivesse um impacto negativo nas exportações das empresas.[136]

Os 76% dos entrevistados que relataram ter preocupações sobre a LATO antes de sua aprovação identificaram as seguintes preocupações principais:[137]

Tabela 6.1: Preocupações da Enquete AustCyber	%
Falta de clareza em torno das definições	81%
Potencial conflito entre as leis australianas e países estrangeiros	73%
Percepção de que o produto da sua empresa está menos seguro	71%
O custo de cumprir as notificações	52%
Erosão da capacidade da empresa	50%
O Impacto na receita da empresa	46%
Redução da atratividade de sua empresa para potenciais investidores	46%
Perda potencial de toda a propriedade intelectual	44%
Incapacidade de aplicar sanções para empresas estabelecidas em outros países que fornecem serviços para a Austrália	40%
Danos para a marca da sua empresa	40%
Impacto sobre a cadeia de suprimentos	38%
Redução da atratividade de sua empresa para potenciais compradores	33%

Access Bill 2018"), AustCyber, 22 de dezembro de 2018, disponível em https://www.austcyber.com/resources/perceptions-survey.

[134] *Ibidem*, página 3.

[135] *Ibidem*, página 8. Apenas 7% esperavam um impacto positivo, 22% não esperavam nenhum impacto e 14% não tinham certeza.

[136] *Ibidem*, página 7. 51% dos entrevistados relataram ser exportadores e, desses, apenas 4% esperavam que a LATO tivesse um impacto positivo, 17% esperavam que o LATO não tivesse nenhum impacto e 13% estavam incertos sobre o impacto nas exportações das empresas.

[137] *Ibidem*, página 23. As porcentagens são calculadas com base nas respostas das 48 empresas que indicaram ter preocupações sobre a LATO.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Redução da transparência entre participantes da indústria	33%
Risco de perder clientes atuais	31%
Outras preocupações	23%

Além disso, embora o projeto de lei indicasse que o governo reembolsaria as empresas pelos custos assumidos no cumprimento da legislação, apenas 5% das empresas esperavam ser totalmente reembolsadas pelos custos de conformidade relacionados à LATO.[138]

6.2. Enquete da Innovation Australia

A segunda pesquisa foi realizada em 2019 pela *Innovation Australia* (InnovationAus), uma publicação independente com foco em políticas públicas australianas e questões de inovação empresarial;[139] pela *StartupAus*, um grupo sem fins lucrativos que atua na defesa de direitos de *startups* da comunidade de tecnologia na Austrália,[140] pela Communications Alliance e pela ITPA. Os resultados foram publicados em dezembro de 2019, um ano após começar a vigência da LATO.[141]

A enquete da InnovationAus foi realizada de 5 a 12 de dezembro de 2019, para coincidir com o aniversário da aprovação parlamentar da LATO. A pesquisa recebeu 70 respostas de integrantes da Communications Alliance e da ITPA. Destes, 40% relataram que a LATO gerou perda nos negócios de sua empresa e 51% relataram um impacto muito negativo na reputação das empresas de tecnologia australianas nos mercados globais.[142] Além disso, após a aprovação da LATO, 57% dos entrevistados pensavam que sua organização tinha menos probabilidade de realizar operações de desenvolvimento na Austrália.[143]

---

[138] *Ibidem*, página 27.

[139] Ver site da Autrália Inovação em https://www.innovationaus.com/.

[140] Ver site da StartupAus em https://startupaus.org/.

[141] INNOVATIONAUS (2019), "O Pulso da Indústria | Leis de Criptografia | Resultados da Enquete" ("*Industry Pulse - Encryption Laws - Survey Results*"), publicado por InnovationAus, StartupAus, Communications Alliance e ITPA, 18 de dezembro de 2019, disponível em https://www.innovationaus.com/wp-content/uploads/2019/12/Encryption_Law_Survey_Results.pdf.

[142] *Ibidem*, página 3. Além dos 51% que consideraram o impacto na reputação muito negativo, 44% acharam que seria um pouco negativo e apenas 3% não esperavam nenhum impacto (0% foram positivos). Ainda, 61% dos entrevistados indicaram que clientes internacionais ou domésticos expressaram preocupação sobre a LATO.

[143] *Ibidem*, página 4. Apenas 30% não esperavam nenhum impacto sobre os planos de desenvolvimento e 7% que a LATO aprimoraria seus planos de desenvolvimento na Austrália. Além disso, 51% dos entrevistados que relataram ter operações de desenvolvimento na Austrália esperavam que a LATO tornasse menos provável o aumento do emprego associado a essas operações.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

6.3. Resumo das entrevistas qualitativa por videoconferência

Conforme descrito, conduzimos entrevistas em profundidade com nove Provedores que têm operações na Austrália e tiveram experiência significativa em como seus negócios enfrentaram a LATO e o que eles achavam que isso significava para as perspectivas de seus negócios na Austrália e no exterior.

Em todos os casos, os entrevistados deixaram claro que se oporiam a qualquer solicitação do governo que visasse induzi-los a criar "*portas dos fundos*" em seus processos de segurança. Atender a tal solicitação enfraqueceria a segurança que eles já oferecem e seria contrário aos compromissos públicos com seus clientes e outras pessoas, de proteger os direitos legais e a confidencialidade dos dados sob seu controle. Isso inclui requerimentos que incorporariam uma ferramenta para quebrar ou contornar a criptografia em quaisquer produtos que atualmente contenham esse recurso ou que seriam divulgados no mercado como tendo esse recurso.

Todos os entrevistados também deixaram claro que já cumprem as solicitações legais do governo de acesso a dados sob as leis e regulamentos australianos existentes. Dito isto, apenas um dos entrevistados indicou que considerava a LATO uma melhoria da situação legal quanto ao acesso do governo a dados. Esse entrevistado viu o porto seguro que a LATO concede a quem atende às solicitações de acesso legais como uma melhoria em relação à situação pré-LATO. Isso porque sentiu que a LATO fornece clareza adicional em relação à proteção de processo e responsabilidade em relação à estrutura preexistente, que era mais fragmentada e, portanto, burocraticamente confusa e onerosa, ou pelo menos, essa tinha sido sua experiência até então. Além disso, as disposições sobre reembolso de custos diretos associados à resposta às solicitações do LATO funcionaram bem para tal entrevistado até o momento. Esta única empresa entrevistada que apoiou a LATO não via a Lei como um potencial risco de se exigir que eles quebrassem a criptografia, divulgassem código-fonte confidencial, ou uma ameaça significativa às mensagens de sua marca para clientes corporativos ou consumidores na Austrália ou no exterior.

As outras oito empresas entrevistadas, no entanto, tiveram impressões negativas sobre a LATO. Elas a viram como uma ameaça potencial à segurança e ao crescimento da demanda pela variedade de serviços de informação que elas oferecem, e que a Lei poderia impor custos mais elevados ao lidar com esses riscos de segurança ampliados. Um dos principais motivos para essa percepção foi a conclusão consensual de que a amplitude da LATO, a inadequação nas previsões de supervisão e a ambigüidade nos termos do que poderia ser necessário, assim como a falta de transparência, representavam uma ameaça à segurança dos dados digitais em repouso ou em trânsito. Os comentários oferecidos ecoaram muitas das mesmas preocupações levantadas como parte da consulta anterior à aprovação da LATO[144] e refletidas nas revisões subsequentes, incluindo a revisão do Monitor Independente da Legislação de Segurança

[144] Ver PARLIAMENT OF AUSTRALIA (2018). Submissões (*Submissions*). *Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*. 5 de dezembro de 2018. Disponível em https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Submissions.

Nacional (INSLM, de *Independent National Security Legislation Monitor*), publicada em julho de 2020.[145] Embora o Governo australiano tenha procurado tratar muitas dessas preocupações como "mitos" infundados,[146] a revisão do INSLM recomendou uma série de mudanças para fortalecer a supervisão da LATO, e esclarecimento adicional de alguns dos termos da Lei.

Apesar das contínuas garantias do governo de que a LATO não seria abusada, e de que sua aplicação seria estritamente limitada apenas a um conjunto restrito de contextos graves, tais como acusação de crimes notórios como terrorismo internacional, material de abuso sexual infantil, ou tráfico de pessoas, muitos entrevistados não ficaram totalmente convencidos, tendo testemunhado o fracasso de previsões análogas de supervisão aplicadas em outros contextos na Austrália e no exterior. Havia uma preocupação de que a capacidade de ampliar a autorização do governo para acessar dados confidenciais por meios ambíguos exigiria contínua vigilância (e aumento do custo para os Provedores) a fim de proteger contra o deslizamento da missão e abusos que as previsões de supervisão deveriam prevenir.

Durante o período que antecedeu a aprovação da LATO, e no primeiro período posterior, vários entrevistados destacaram a preocupação de que ela pudesse sujeitá-los a uma posição insustentável (por causa das disposições confusas e restritivas quanto a quais informações sobre os avisos da LATO poderiam ser compartilhados por seus destinatários). Por exemplo, havia a preocupação de que um funcionário pudesse ser incapaz de compartilhar tais informações com a alta administração sem enfrentar sanções legais. Esse cenário exporia os funcionários e sua empresa a responsabilidades legais inaceitáveis.

Discussões subsequentes com as autoridades regulatórias responsáveis pela LATO, de acordo com os entrevistados, levaram-nos a descontar esse risco; no entanto, o fato de ter surgido é um indicativo da confusão e da incerteza jurídica (e, portanto, comercial) que a LATO gerou desde que foi proposta pela primeira vez, e que segue até hoje. Adicionalmente, essa perspectiva pode mudar à medida que a liderança e o pessoal dessas autoridades reguladoras mudem e adotem pontos de vista diferentes, já que isso não está explícito na redação da lei.

Vários entrevistados indicaram que um requisito para quebrar ou burlar a criptografia de um de seus produtos seria inviável de uma forma direcionada a um indivíduo e, portanto, inseriria uma vulnerabilidade sistêmica que se propagaria, impactando adversamente a segurança do produto ou serviço para outros usuários. Isso é especialmente verdadeiro para os Provedores dependentes e fornecedores de serviços baseados em código aberto, ou dependentes de criptografia e proteções de segurança que não são personalizáveis por usuário individual. Alguns Provedores também podem contar com serviços desse tipo, mesmo que eles próprios não os forneçam.

---

[145] Ver INSLM (2020a), Nota 50 *supra*.

[146] Ver DEPARTMENT OF HOME AFFAIRS (2019). "Assistência e acesso: mitos comuns e equívocos" ("*Assistance & Access: Common myths and misconception*"), Governo da Austrália (*Australian Government*), 16 de setembro de 2009, disponível em https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-agir.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Obrigar-se um fornecedor a quebrar a segurança de um produto via LATO poderia constituir uma ameaça existencial, e exigir da empresa retirar da Austrália suas operações e vendas de produtos ou serviços. Alguns entrevistados admitiram esse risco e disseram que se oporiam ao cumprimento de qualquer solicitação desse tipo, até o limite total de suas prerrogativas legais para apelar e contestá-la, escalando esses esforços até qualquer nível necessário.

Independentemente da realidade de certos cenários extremos de como a LATO pode ser abusada, a mera percepção de que ela enfraquece a segurança era uma preocupação para os Provedores: por estarem sujeitos à Lei, seus produtos e serviços seriam considerados menos seguros pelas partes interessadas, e essa segurança reduzida poderia levar a vazamentos de dados e violações de segurança, não apenas na Austrália, mas em outros lugares. A percepção de que a LATO representa uma política ruim de segurança foi tratada por todos, exceto um de nossos entrevistados, como uma ameaça potencial para suas marcas, a qual eles precisariam monitorar cuidadosamente e considerar em seus planos estratégicos futuros, a fim de desenvolverem e fornecerem produtos dotados de segurança para venda na Austrália.

Vários entrevistados observaram que a LATO, e o que ela sinalizou sobre um potencial clima de piora em termos de interferência do governo e de regulamentação de produtos de segurança, seriam um fator em seus planos futuros para arquitetarem suas operações de desenvolvimento e vendas na Austrália. Por exemplo, seria um fator na seleção de fornecedores de serviços, tais como centros de dados (*data centers*) localizados na Austrália, sujeitos à LATO. Além disso, estando os destinatários legalmente impedidos de compartilhar informações sobre os avisos da LATO que receberem, seus clientes podem não saber quais Provedores receberam esses avisos, nem quais podem ter sido suas respostas.

Um entrevistado é um Provedor com sede na Austrália que estava crescendo rapidamente e procurando se expandir para mercados internacionais, o que considerava uma oportunidade de bilhões de dólares. Depois da LATO, o impacto adverso da marca em seus produtos os levou a abandonar os planos de expansão das vendas de exportação, fechando uma importante oportunidade de crescimento para aquela empresa. O entrevistado observou que perderam negócios com clientes existentes, que decidiram transferir seus negócios para outros fornecedores cujas ofertas estavam fora do alcance da LATO.

Vários entrevistados observaram que a preocupação com a segurança dos dados dos clientes havia sido levantada por seus consumidores e era um fator que eles deveriam considerar ao pensar em planos futuros. Eles tiveram que reassegurar os clientes de seus compromissos em proteger a confidencialidade dos dados.

Com exceção do caso observado acima, a maioria dos entrevistados indicou que os custos impostos pela LATO até então não tinham sido excessivos, embora a maioria expressasse ceticismo de que as previsões de reembolso das despesas relacionadas os iriam imunizar contra impactos adversos de custos. Os entrevistados esperavam que os custos mais significativos relacionados à LATO provavelmente seriam indiretos (p. ex., danos à imagem da marca ou redução da demanda por serviços ou produtos de Provedores australianos) em vez de diretos (p. ex., gasto de recursos humanos com funcionários dedicados ao cumprimento de uma solicitação específica).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

A maioria dos entrevistados adotou proteções procedimentais adicionais relacionadas à LATO (com custos associados),[147] mas a maioria não indicou que a LATO já tivesse resultado na mudança do design de suas ofertas de produtos ou em suas decisões de equipe com relação à localização das pessoas na Austrália ou no exterior. Todavia, as proteções procedimentais adicionais indicam que esses tipos de decisões podem se tornar fatores no futuro. Vários entrevistados comentaram que a falta de evidências sobre custos diretos significativos da Lei não era surpreendente, à luz do exercício limitado da autoridade da LATO desde sua aprovação. Eles atribuíram isso ao fato de levar tempo para que os efeitos da nova legislação sejam sentidos, juntamente com a persistente controvérsia e os pedidos de emendas à Lei.

Além disso, vários viram a LATO como um passo infeliz em uma direção que amplificaria ainda mais a ameaça global à maior segurança de dados, do que ela já representa, caso se tornasse mais difundida, com a adoção mais ampla de leis que a copiassem.

Finalmente, à luz da decisão de julho de 2020 na União Europeia (Schrems II, que derrubou a solução de proteção de privacidade que havia sido adotada para proteger os acordos internacionais de compartilhamento de dados de entrarem em conflito com as leis de proteção de dados da UE)[148], uma série de entrevistados indicaram estarem preocupados que a LATO pudesse representar um risco para os fluxos de dados internacionais pra dentro e pra fora da Austrália. Qualquer ameaça, se efetivamente comprovada, poderia impor significativos custos ao bom funcionamento dos mercados globais de dados e comunicação.

6.4. Resultados da enquete do LECA

6.4.1. Participantes da enquete online

Conforme observado acima, houve 79 entrevistados na pesquisa conduzida pelo LECA com o auxílio da Clarity Strategic Research. Semelhante à composição das duas pesquisas anteriores observadas acima, os entrevistados representaram empresas com operações na Austrália em vários setores da economia e uma gama de tamanhos (medidos com base em funcionários ou receitas):

- 54 das empresas tinha sede na Austrália (68%);
- As empresas entrevistadas variaram em tamanho de menos de 10 (34% ou 27 de 79) a mais de 500 funcionários (28% ou 22 de 79);
- Uma proporção considerável relatou que todos os seus funcionários estavam localizados na Austrália (46% ou 36 de 79), enquanto outra proporção menor, mas ainda considerável (27% ou 21 de 79) relatou que menos da metade ficavam na Austrália.

[147] Por exemplo, vários entrevistados mencionaram que essas proteções procedimentais incluíam a adição de outra camada de revisão de processo para planos de investimento e desenvolvimento de produto para lidar com o impacto potencial da LATO.

[148] Ver Nota 118, *supra*.

- Classificadas com base nas receitas totais, 43% (ou 34 de 79) são pequenas (menos de AU$ 5 milhões), enquanto 13% (ou 10 de 79) são grandes empresas (mais que AU$ 5 milhões).
- Como esperado, a maioria dos entrevistados identificou que suas empresas operavam em negócios relacionados a TI (54% ou 43 de 79), com muitos deles ativos em várias linhas.
- Das que não estavam em negócios relacionados a TI (43% ou 34 de 79), os entrevistados identificaram que suas empresas operavam em Serviços (44% ou 15 de 34), Administração Pública e Segurança (18% ou 6 de 34) ou outros setores (38% ou 13 de 34), desde Indústria até Educação.[149]
- Os cargos dos entrevistados indicaram estarem quase todos, senão todos, envolvidos em trabalhos relacionados a TI, o que não surpreende, dado para quem foi enviada a enquete.

Esses resultados estão resumidos nas tabelas a seguir:

Tabela 6.2: QA1i: Onde está sediada a empresa?		
	Quantidade	%
Austrália	54	68%
Em outro lugar	23	29%
Sem resposta	2	3%
Total	79	100%

Tabela 6.3: QA3i: Quantos empregados globalmente (quantidade aproximada)?		
Número de empregados globais	Quantidade	%
Sem resposta	10	13%
0-10	27	34%
11-499	20	25%
500+	22	28%
Total	79	100%

[149] Dois (3% dos 79) entrevistados não responderam.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Tabela 6.4: Proporção de empregados na Austrália	Quantidade	%
Sem resposta	12	15%
10% ou menos	16	20%
10 <% <100	15	19%
100%	36	46%
Total	79	100%
0%	4	5%
<50%	21	27%

Tabela 6.5: A empresa é um negócio de TI?		
Setor	Quantidade	%
Sem resposta	2	3%
TI	43	54%
Não-TI	34	43%
Total	79	100%

Tabela 6.5B: Localização da sede e linha de negócios				
Localização da sede	Linha de negócios			Total
	TIC	Não TIC	Sem resposta	
Austrália	31 (39%)	23 (29%)	0 (0%)	54 (68%)
Em outro lugar	12 (15%)	10 (13%)	1 (1%)	23 (29%)
Sem resposta	0 (0%)	1 (1%)	1 (1%)	2 (3%)

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Total	43 (54%)	34 (43%)	2 (3%)	79 (100%)

Tabela 6.6: Linhas de negócios de TI

	código	Quantidade
Operações, equipamentos e serviços de redes de telecomunicações	1-3 , 10, 13	18
Provedor de serviços de Internet, portais web de pesquisa, outros serviços de Internet	4-5	7
Serviços de armazenamento eletrônico	6	6
Desenvolvedor ou fornecedor de software	7-8	25
Fabricação e vendas de equipamentos de informática	9-12, 13-14	17
Outras TI (especifique)	97	13
Não sei, não direi	98-99	3
Total		89

Tabela 6.7: Linhas de negócios das empresas que não são de TI

setor	códigos	Quantidade	%
Serviços	10, 12, 18	12	46%
Administração pública e segurança	14	6	23%
Outros (Fabricação, Construção, Educação)	3, 5, 7, 15	8	31%
Total		26	100%

6.4.2. A importância dos serviços de criptografia para empresas

Os respondentes da enquete indicaram de forma esmagadora que os serviços e recursos de criptografia eram muito ou bastante importantes para seus negócios de várias maneiras: tanto para comunicações (dados em trânsito) quanto para dados armazenados (dados em repouso), bem como para uso interno e em negociações comerciais com vendedores ou fornecedores e com clientes. 96% (ou 76 de 79) dos entrevistados indicaram que os serviços de criptografia

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

eram muito ou bastante importantes para pelo menos uma categoria de uso.[150] Além disso, a Tabela 6.8 demonstra que bem mais de 85% (ou 67 de 79) dos entrevistados consideraram os serviços e recursos de criptografia muito ou bastante importantes para a maioria dos contextos de uso considerados separadamente e, desses, bem mais de 53% (ou 42 de 79) respondeu que os serviços e recursos de criptografia eram muito importantes.

Os entrevistados também indicaram que adquiriram de várias formas os recursos de criptografia necessários: às vezes desenvolvendo-os internamente e às vezes contando com fornecedores terceirizados de produtos e serviços de uso geral (ou seja, as ferramentas de criptografia podem ser um recurso integrado de um produto ou serviço de TI) ou com prestadores especializados de serviços de criptografia. Os métodos de aquisição de recursos variam conforme o uso (ou seja, dados em trânsito ou em repouso, usados internamente, com vendedores e fornecedores ou com clientes). Muitos usaram abordagens diferentes em contextos diferentes e, às vezes, abordagens múltiplas em contextos específicos. Embora os resultados de nossa enquete anônima não nos permitam rastrear co-dependências entre as empresas (ou seja, alguns entrevistados podem ser consumidores e/ou fornecedores dos serviços de criptografia de outros), fica claro que o uso de recursos e serviços de criptografia está difundido entre diferentes empresas que são e as que não são de TI.

Esses resultados indicam ampla dependência de serviços de criptografia por todos os tipos de negócios em toda a economia e da rede potencialmente emaranhada de repercussões que pode ser transmitida entre as empresas na Austrália e internacionalmente, se estiverem ameaçadas as ferramentas de criptografia de pelo menos um subconjunto de empresas. A propagação de tais efeitos adversos pela economia poderia amplificar e aumentar o impacto direto adverso. Infelizmente, o pequeno número de respostas à pesquisa e a falta de melhores dados sobre o comércio de bens e serviços dependentes de recursos criptografados não permitem estimar ou modelar as maneiras pelas quais os efeitos diretos e indiretos podem repercutir na economia.

Tabela 6.8: Qual a importância dos serviços e recursos de criptografia para sua empresa?

	Muito ou bastante importante	Pouco (nada) importante ou não usado	Não sabe ou não respondeu	Total	% da coluna (a) que responderam Muito importante
	(a)	(b)	(c)	(a)+(b)+(c)	
Comunicações (dados em trânsito) internas da empresa	85%	14%	1%	100%	53%

[150] Apenas um entrevistado indicou que não usa serviços de criptografia, apenas um outro entrevistado indicou que os serviços de criptografia não eram muito ou muito importantes para pelo menos uma das categorias de uso, e apenas um outro entrevistado preferiu não responder em todas as categorias de uso, representando apenas 4% do total (ou 3 de 76).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Acervos de dados internos (em repouso) da empresa	92%	6%	1%	100%	73%
Comunicações (dados em trânsito) com vendedores e fornecedores	90%	9%	1%	100%	59%
Acervos de dados (em repouso) mantidos por vendedores e fornecedores	91%	6%	3%	100%	70%
Comunicações (dados em trânsito) com clientes	91%	8%	1%	100%	65%
Acervos de dados (em repouso) em produtos ou serviços que sua empresa fornece para clientes	87%	11%	1%	100%	71%

6.4.3. Conhecimento e familiaridade em relação à LATO

Dos 79 entrevistados, 58 indicaram já ter ouvido falar da LATO. Esses 58 entrevistados são principalmente de empresas com sede na Austrália (68%), cujo principal negócio é baseado em TI (60% ou 35 de 58); e 40% (ou 23 de 58) dos entrevistados indicaram que estavam muito ou bastante familiarizados com a Lei.

Tabela 6.9: Conhecimento dos entrevistados sobre a LATO por localização da sede

	Conhece	Não conhece / Sem resposta	Total
Austrália	42 (53%)	12 (15%)	54 (68%)
Outro lugar	16 (20%)	9 (11%)	25 (32%)
Total	**58 (73%)**	21 (27%)	79 (100%)

Tabela 6.10: Conhecimento dos entrevistados em relação à LATO por tipo de empresa

	Conhece	Não conhece / Sem resposta	Total
TI	35 (44%)	8 (10%)	43 (54%)
Não TI	23 (29%)	13 (16%)	36 (46%)
Total	**58 (73%)**	21 (27%)	79 (100%)

Tabela 6.11: Nível de familiaridade em relação à LATO

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Muito / Bastante familiarizado	23	40%
Não muito familiarizado	29	50%
Não familiarizado	4	7%
Sem resposta	2	3%
Total	58	100%

6.4.4. Postura dos entrevistados em relação à LATO

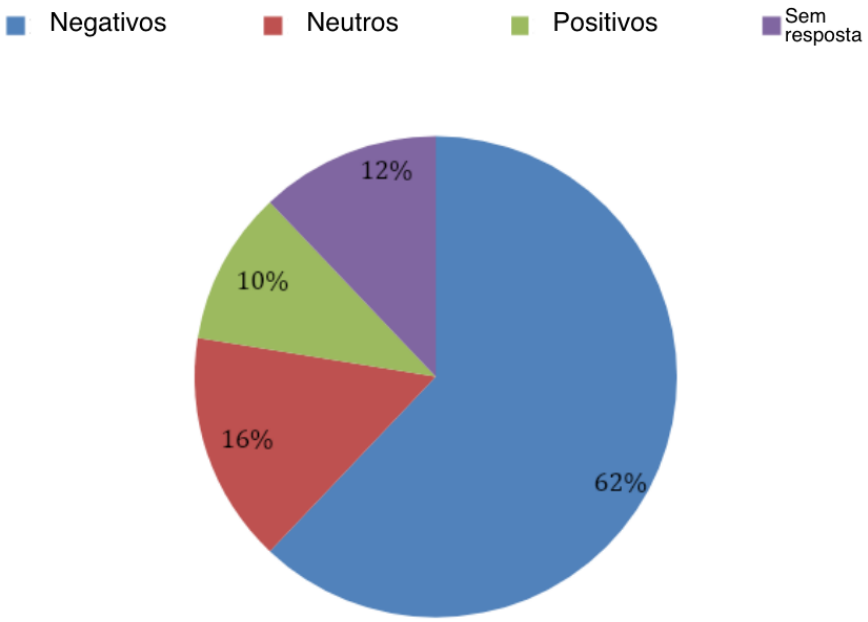
Entre aqueles que conhecem a LATO, uma grande proporção (62% ou 36 de 58) se sente muito ou bastante negativa em relação às mudanças que ela fez na Lei de Telecomunicações de 1997. Apenas 10% (ou 6 de 58) disseram ter postura positiva. O gráfico abaixo resume as posturas em relação à LATO, dentre os 58 entrevistados que a conheciam.

Tabela 6.12: Postura dos entrevistados em relação à LATO	
Muito Positivo	0%
Bastante Positivo	10%
Neutro	16%
Bastante Negativo	26%
Muito Negativo	36%
Sem Resposta	12%
Total	100%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Imagem 6.1 Para os 58 entrevistados cientes da TOLA



Questionados sobre como achavam que a LATO impactou várias questões políticas, a maioria dos entrevistados acredita que ela teve impacto adverso nas relações exteriores da Austrália e na segurança e integridade dos dados digitais; e, o mais importante, um impacto adverso na economia da Austrália. Eles tiveram sentimentos mistos em relação ao impacto na segurança nacional da Austrália. O impacto positivo mais significativo da Lei (mas ainda bem menos do que a maioria) foi na aplicação da lei criminal na Austrália (ver Tabela 6.13).

Tabela 6.13: Expectativas dos entrevistados sobre o impacto da LATO nas questões

	Negativo	Sem Impacto	Positivo	Sem Resposta	Total
Segurança nacional da Austrália	33%	22%	24%	21%	100%
Relações exteriores da Austrália	53%	7%	9%	31%	100%
Bem-estar econômico nacional da Austrália	52%	10%	16%	22%	100%
A segurança e integridade das informações processadas, armazenadas ou comunicadas por meios eletrônicos ou semelhantes	59%	12%	10%	19%	100%
Aplicação da lei criminal na Austrália	12%	29%	34%	24%	100%
Aplicação da lei criminal em outros países	10%	50%	7%	33%	100%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

6.4.5 LATO impacta nos negócios dos entrevistados

Quando questionados sobre se a LATO impactou seus negócios de várias maneiras, 41% dos entrevistados responderam que ela impactou seus negócios de uma ou mais maneiras (Tabela 6.14A) e, em média, 18% dos entrevistados que conhecia a TOLA (58 de 79) respondeu ter a Lei impactado seus negócios em todas as categorias (Tabela 6.14B).

Tabela 6.14A: Empresas que relatam impactos de várias categorias

Sem impacto	59%
Uma categoria de impacto	5%
Duas ou mais categorias de impacto	36%

Tabela 6.14B: A LATO teve impacto nos negócios?

	Sim	Não	Não sei	Sem Resposta	Totais
Vendas	16%	47%	31%	7%	100%
Reputação do Negócio	14%	45%	36%	5%	100%
Relações com fornecedores	16%	52%	28%	5%	100%
Relações com clientes	16%	48%	31%	5%	100%
Desenvolvimento do Produto, Decisões de Marketing	31%	43%	22%	3%	100%
OPEX / CAPEX	21%	45%	33%	2%	100%
Outras áreas Negócios	21%	40%	36%	3%	100%
Média	19%	46%	31%	4%	

Questionados se os impactos foram positivos ou negativos até o momento, e se esperavam futuros efeitos sobre várias questões de negócios, mais uma vez, os entrevistados que tinham visto um impacto destacaram a ampla gama de impactos (ver Tabela 6.15A, 6.15B e 6.15C). Embora a maioria das empresas não tenha relatado nenhum impacto (Tabela 6.14), das que disseram ter sentido em pelo menos em uma categoria, o número que apontou um efeito negativo é maior do que o das que viram efeitos positivos em todas as categorias. Além disso, elas preveem a continuidade futura dos efeitos negativos em todas as 15 áreas de impacto; e, para a grande maioria dos efeitos negativos (11 das 15 áreas de impacto, ou 73%), mais empresas esperam por eles no futuro do que os sentiram até o momento (Tabela 6.15C) – aumentando de 18% para 20%. Essas respostas correspondem à visão de que, no futuro, os impactos econômicos irão continuar, ou talvez até piorar. Finalmente, no geral, 36% (ou 21 de 58) das empresas experimentaram um impacto negativo em uma ou mais áreas de seus negócios até então e os esperam no futuro (Tabela 6.15D).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Tabela 6.15A: Empresas que sentiram um impacto até então (desde 2018)					
Porção das empresas que tiveram impacto	Negativo	Sem impacto	Positivo	Sem resposta	Total
Sua receita global total	10%	12%	3%	74%	100%
Sua receita global de serviços criptografados	9%	16 %	2%	74%	100%
Seus custos operacionais globais de negócio, incluindo conformidade e remediação	16%	14%	2%	69%	100%
Seu investimento global em serviços criptografados	21%	9%	3%	67%	100%
Seu nível global de investimento e financiamento	17%	9%	3%	71%	100%
Seu gasto global em estratégia de inovação em relação a serviços criptografados	21%	7%	5%	67%	100%
Seu investimento global em desenvolvimento de novos produtos	22%	7%	2%	69%	100 %
Suas despesas globais de P&D	19%	9%	3%	69%	100%
Seu valor global de marca ou reputação	19%	10%	3%	67%	100%
Seu valor global de outra propriedade intelectual (patentes, direitos autorais, etc.)	14%	14%	2%	71%	100%
Sua capacidade global de atrair bons funcionários para trabalhar para seu negócio	12%	17%	2%	69%	100%
Sua capacidade global de comprar produtos e serviços criptografados necessários	10%	17%	3%	69%	100%
Sua confidencialidade, segurança ou privacidade global de serviços criptografados	28%	9%	2%	62%	100%
Seu ambiente de risco global para a empresa	36%	2%	2%	60%	100%
Níveis globais de emprego em serviços criptografados	14%	9%	3%	74%	100%

Tabela 6.15B: Empresas que esperam sentir impactos futuros					
Porção das empresas que tiveram impacto	Negativo	Sem impacto	Positivo	Sem resposta	Total

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Sua receita global total	14%	7%	7%	72%	100%
Sua receita global de serviços criptografados	14%	9%	2%	76%	100%
Seus custos operacionais globais de negócio, incluindo conformidade e remediação	21%	10%	2%	67%	100%
Seu investimento global em serviços criptografados	28%	9%	0%	64%	100%
Seu nível global de investimento e financiamento	19%	9%	3%	69%	100%
Seu gasto global em estratégia de inovação em relação a serviços criptografados	24 %	9%	0%	67%	100%
Seu investimento global em desenvolvimento de novos produtos	21%	7%	3%	69%	100%
Suas despesas globais de P&D	19%	12%	2%	67%	100%
Seu valor global de marca ou reputação	19%	9%	5%	67%	100%
Seu valor global de outra propriedade intelectual (patentes, direitos autorais, etc.)	16%	14%	0%	71%	100%
Sua capacidade global de atrair bons funcionários para trabalhar para seu negócio	14%	16%	5%	66%	100%
Sua capacidade global aliado para comprar produtos e serviços criptografados que sua empresa precisa	19%	12%	2%	67 %	100%
Sua capacidade global de comprar produtos e serviços criptografados necessários	29%	5%	3%	62%	100%
Seu ambiente de risco global para a empresa	33%	2%	2%	64%	100%
Níveis globais de emprego em serviços criptografados	16 %	7%	3%	74%	100%

Tabela 6.15C: Empresas que sentiram até então ou que esperavam sentir no futuro impactos negativos da LATO em seus negócios

Porção das empresas que tiveram impacto	até então	Futuro
Sua receita global total	10%	14%
Sua receita global de serviços criptografados	9%	14%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Seus custos operacionais globais de negócio, incluindo conformidade e remediação	16%	21 %
Seu investimento global em serviços criptografados	21%	28%
Seu nível global de investimento e financiamento	17%	19%
Seu gasto global em estratégia de inovação em relação a serviços criptografados	21%	24%
Seu investimento global em desenvolvimento de novos produtos	22%	21%
Suas despesas globais de P&D	19%	19%
Seu valor global de marca ou reputação	19%	19%
Seu valor global de outra propriedade intelectual (patentes, direitos autorais, etc.)	14%	16%
Sua capacidade global de atrair bons funcionários para trabalhar para seu negócio	12%	14%
Sua capacidade global de comprar produtos e serviços criptografados necessários	10%	19%
Sua confidencialidade, segurança ou privacidade global de serviços criptografados	28%	29%
Seu ambiente de risco global para a empresa	36%	33 %
Níveis globais de emprego em serviços criptografados	14%	16%
Média (das linhas)	18%	20%

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Figura 6.2 Impacto Negativo Passado e Futuro % das Empresas Australianas e Estrangeiras

Tabela 6.15D: Número de categorias de impactos negativos sentidos ou esperados		
Número de impactos negativos (globalmente e na Austrália) Total de casos que conhecem a TOLA = 58	Número de casos até então	Número de casos no futuro
0 (inclui nenhuma resposta) em todas as categorias	37 (64%)	37 (64%)
1 de 15 categorias	0 (0%)	0 (3%)
2 de 15 categorias	2 (3%)	0 (0%)
3 de 15 categorias	2 (3%)	2 (2%)
4 ou mais de 15 categorias	17 (29%)	18 (31%)
Total	58 (100%)	58 (100 %)
Impacto negativo em pelo menos 1 das 15 categorias	21 (36%)	21 (36%)

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

6.5. Conclusões da pesquisa empírica

Em resumo, os riscos econômicos hipotéticos descritos no Capítulo 5 foram ecoados pelas empresas de TIC que entrevistamos e nas respostas à nossa enquete. Em ambos os casos, houve justificativa empírica para a visão de que a LATO representa uma ameaça econômica para as perspectivas de negócios das empresas de TIC e para a economia australiana e global.

A pesquisa também indicou a ausência de evidência empírica até o momento sobre custos econômicos significativos (e ainda mais, de benefícios) que podem ser diretamente atribuídos à LATO. Essa ausência de evidência empírica, entretanto, não é evidência da ausência de efeito. Embora valesse a pena procurar evidências empíricas de custos assumidos desde 2018, teríamos ficado surpresos se as encontrássemos à luz da atividade muito limitada da LATO relatada, e dos desafios e da controvérsia persistentes que tornam incerto o futuro da Lei. Além disso, as regras de não divulgação e sigilo que envolvem a atividade da LATO geram uma barreira significativa para a coleta de evidências em relação a seus impactos econômicos. Todavia, a limitação nas evidências coletadas é reveladora. O fato de o único entrevistado que viu o impacto do LATO de maneira mais favorável ter visto como seu efeito principal a racionalização da legislação existente sobre o acesso legal do governo a dados digitais é consistente com a perspectiva de que provavelmente são pequenos os benefícios diretos da Lei. Por outro lado, o único entrevistado capaz de quantificar o dano econômico por ele sofrido em decorrência da LATO, estimou um valor da ordem de um bilhão de dólares de receita de exportação perdida, o que é consistente com a expectativa de que podem ser bem grandes os potenciais danos econômicos diretos.

O tamanho da enquete anônima e os desafios que a confiança nos dados da pesquisa impõe à inferência de impactos econômicos limitam nossa capacidade de quantificar a magnitude dos efeitos econômicos. No entanto, os resultados são consistentes com o que foi observado nas enquetes anteriores, e demonstram que as preocupações que existiam antes da aprovação da LATO continuam existindo hoje; e, se essas preocupações forem confirmadas, os impactos econômicos adversos podem ser extensos.

As respostas à enquete destacam o fato de os impactos adversos serem amplamente compartilhados entre empresas que são e que não são de TIC, bem como que ainda muitas empresas não entendem a ameaça que a LATO representa para seus negócios.

7. Apêndices, acrônimos, abreviações e definições

7.1. Siglas, abreviações e definições

- **Lei ASIO** (*ASIO Act*): Lei da Organização Australiana de Inteligência de Segurança (*The Australian Security Intelligence Organisation Act*) de 1979 (ver Nota 18).
- **ASIO**: Organização Australiana de Inteligência de Segurança (*Australian Security Intelligence Organization*), uma das agências governamentais australianas que podem emitir avisos da LATO.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

- **Cth**: significa Comunidade (*Commonwealth*) e é usado para distinguir a legislação federal da Austrália da legislação estadual. [NdT. 6: A Comunidade da Austrália, nome oficial do país, é composta de seis estados: Nova Gales do Sul, Queensland, Austrália Meridional, Tasmânia, Vitória, Austrália Ocidental; e dois territórios: o Território do Norte e Território da Capital Australiana]

- **Provedor**: refere-se ao termo legal Provedor de Comunicações Designado (*Designated Communications Provider*) [ver NdT. 3, ao final da Nota 3, *supra*], uma categoria interpretada de forma ampla sob a LATO, abarcando as empresas às quais ela se aplica, conforme a lista constante da sessão 317C, reproduzida a seguir.

- **INSLM**: Monitor Independente de Legislação de Segurança Nacional (*Independent National Security Legislation Monitor*), apresentou um relatório de revisão da TOLA em 20 de julho de 2020 (ver Nota 50).

- **PJCIS**: Comissão Parlamentar Mista de Inteligência e Segurança (*Parliamentary Joint Committee on Intelligence and Security*), conduziu um inquérito sobre a LATO antes de sua promulgação e, desde então, tem realizado revisões (Ver Nota 40).

- **LATO** (*TOLA*): Lei de Alteração das Telecomunicações e de Outras Legislações (de Assistência e Acesso) de 2018 [*Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*], também conhecida como Lei de Criptografia ou Lei de Assistência e Acesso (ver Nota 2, *supra*), é composta por 5 capítulos, sendo o foco deste estudo o Capítulo 1, sobre remoção e evasão de criptografia ou acesso excepcional.

- **TAR, TAN, TCN**: três tipos de avisos que podem ser emitidos de acordo com a LATO, oralmente ou por escrito (sessão 317H):

    - TAR: Requisição de Assistência Técnica (*Technical Assistance Request*), pode solicitar que um Provedor realize ações voluntárias (sessão 317L)

    - TAN: Notificação de Assistência Técnica (*Technical Assistance Notice*), exige que um Provedor forneça ajuda técnica (317M)

    - TCN: Notificação de Ferramenta Técnica (*Technical Capability Notice*), exige que um Provedor realiza ações específicas, incluindo o desenvolvimento de uma ferramenta (317T)

- **Lei TIA**: Lei de (Interceptação e Acesso a) Telecomunicações [*The Telecommunications (Interception and Access) Act*] de 1979 (ver Nota 14).

- **TA1997**: A Lei de Telecomunicações (*The Telecommunications Act*) de 1997 (ver Nota 13).

- **SD Act**: Lei de Vigilância de Dispositivos (*The Surveillance Devices Act*) de 2004 (ver Nota 15).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

- **MACMA**: A Lei de Assistência Mútua em Matérias Criminais (*The Mutual Assistance in Criminal Matters Act*) de 1987 (ver Nota 17).

7.2. Definições constantes da LATO

317B Definições

Neste Capítulo:

……

proteção eletrônica inclui:

(a) autenticação; e

(b) criptografia.

……

tecnologia alvo:

(a) para os fins deste Capítulo, um determinado serviço de conexão, na medida em que o serviço seja usado, ou tenha probabilidade de ser usado, (seja direta ou indiretamente) por uma determinada pessoa, é uma **tecnologia alvo** que é conectada com essa pessoa; e

(b) para os fins deste Capítulo, um determinado serviço eletrônico, na medida em que o serviço seja usado, ou tenha probabilidade de ser usado, (seja direta ou indiretamente) por uma determinada pessoa, é uma **tecnologia alvo** que está conectada com essa pessoa; e

(c) para os fins deste Capítulo, determinado programa de computador instalado ou a ser instalado em:

(i) um determinado computador; ou

(ii) um determinado item de equipamento;

usado, ou com probabilidade de ser usado, (seja direta ou indiretamente) por uma determinada pessoa é uma **tecnologia alvo** que está conectada a essa pessoa; e

(d) para os fins deste Capítulo, uma determinada atualização de programa de computador que foi instalada em:

(i) um determinado computador; ou

(ii) um determinado item de equipamento;

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

usado, ou com probabilidade de ser usado, (seja direta ou indiretamente) por uma determinada pessoa é uma **tecnologia alvo** que está conectada a essa pessoa; e

(e) para os fins deste Capítulo, um determinado item de equipamento de consumo usado, ou com probabilidade de ser usado, (seja direta ou indiretamente) por uma determinada pessoa, é uma **tecnologia alvo** que está conectada a essa pessoa; e

(f) para os fins deste Capítulo, um determinado dispositivo de processamento de dados usado, ou com probabilidade de ser usado, (seja direta ou indiretamente) por uma determinada pessoa, é uma **tecnologia alvo** que está conectada a essa pessoa.

Para os fins dos parágrafos (a), (b), (c), (d), (e) e (f), é irrelevante se a pessoa possa ser identificada.

……

317 Provedor de Comunicações Designado, etc.

Para os fins deste Capítulo, a tabela a seguir define:

(a) **provedor de comunicações designado**; e

(b) as **atividades elegíveis** de um provedor de comunicações designado.

Provedor de comunicações designado e atividades elegíveis		
Item	**Uma pessoa é um provedor de comunicações designado se ...**	**... e as atividades elegíveis da pessoa são ...**
1	a pessoa é uma conectora ou prestadora de serviços de conexão	(a) a operação, pela pessoa, de redes ou instalações de telecomunicações na Austrália; ou (b) o fornecimento, pela pessoa, de serviços de conexão listados
2	a pessoa é um serviço intermediário de conexão que organiza o fornecimento, por um prestador de serviços de conexão, dos serviços de conexão listados	(a) a organização, pela pessoa, do fornecimento, pelo fornecedor de serviços de conexão, de serviços de transporte listados; ou (b) a operação, pelo provedor de serviços de conexão, de redes ou instalações de telecomunicações na Austrália; ou (c) o fornecimento, pelo provedor de serviços de conexão, de serviços de conexão listados

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

3	a pessoa fornece um serviço que facilita, ou é auxiliar ou incidental a, o fornecimento de um serviço de conexão listado	a prestação, pela pessoa, de um serviço que facilita, ou é acessório ou incidental a, o fornecimento de um serviço de conexão listado
4	a pessoa fornece um serviço eletrônico que tem um ou mais usuários finais na Austrália	o fornecimento, pela pessoa, de um serviço eletrônico que tem um ou mais usuários finais na Austrália
5	a pessoa fornece um serviço que facilita, ou é auxiliar ou incidental a, o fornecimento de um serviço eletrônico que tem um ou mais usuários finais na Austrália	o fornecimento, pela pessoa, de um serviço que facilita, ou é acessório ou incidental a, o fornecimento de um serviço eletrônico que tem um ou mais usuários finais na Austrália
6	a pessoa desenvolve, fornece ou atualiza o programa de computador usado, para uso, ou com probabilidade de ser usado, em conexão com: (a) um serviço de conexão listado; ou (b) um serviço eletrônico que tem um ou mais usuários finais na Austrália	(a) o desenvolvimento, pela pessoa, de qualquer programa de computador desse tipo; ou (b) o fornecimento, pela pessoa, de qualquer programa de computador desse tipo; ou (c) a atualização, pela pessoa, de qualquer programa de computador desse tipo;

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Provedor de comunicações designado e atividades elegíveis		
Item	**Uma pessoa é um provedor de comunicações designado se ...**	**... e as atividades elegíveis da pessoa são ...**
7	a pessoa produz, fornece, instala, mantém ou opera um recurso	(a) a produção, pela pessoa, de um recurso para uso, ou com probabilidade de ser usado, na Austrália; ou (b) o fornecimento, pela pessoa, de um recurso para uso, ou com probabilidade de ser usada, na Austrália; ou (c) a instalação, pela pessoa, de um recurso na Austrália; ou (d) a manutenção, pela pessoa, de um recurso na Austrália; ou (e) a operação, pela pessoa, de um recurso na Austrália
8	a pessoa fabrica ou fornece componentes para uso, ou com probabilidade de serem usados, na produção de um recurso para uso, ou com probabilidade de uso, na Austrália	(a) a produção pela pessoa de qualquer um desses componentes; ou (b) o fornecimento pela pessoa de quaisquer desses componentes
9	a pessoa conecta um recurso a uma rede de telecomunicações na Austrália	a conexão, pela pessoa, de um recurso a uma rede de telecomunicações na Austrália
10	a pessoa produz ou fornece equipamento de consumo para uso, ou com probabilidade de ser usado, na Austrália	(a) a produção, pela pessoa, de qualquer equipamento de consumo desse tipo; ou (b) o fornecimento pela pessoa de qualquer equipamento de consumo desse tipo

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Provedor de comunicações designado e atividades elegíveis		
Item	**Uma pessoa é um provedor de comunicações designado se ...**	**... e as atividades elegíveis da pessoa são ...**
11	a pessoa produz ou fornece componentes para uso, ou com probabilidade de serem usados, na fabricação de equipamento de consumo para uso, ou com probabilidade de serem usados, na Austrália	(a) a produção, pela pessoa, de quaisquer componentes desse tipo; ou (b) o fornecimento, pela pessoa, de quaisquer componentes desse tipo
12	a pessoa: (a) instala ou mantém equipamento de consumo na Austrália; e (b) o faz de outra forma que não na capacidade de usuário final do equipamento de consumo	(a) qualquer instalação desse tipo, pela pessoa, de equipamento de consumo; ou (b) qualquer manutenção desse tipo, pela pessoa, de equipamento de consumo
13	a pessoa: (a) conecte o equipamento de consumo a uma rede de telecomunicações na Austrália; e (b) o faça de outra forma que não seja na capacidade de usuário final do equipamento,	qualquer conexão desse tipo, pela pessoa, de equipamento de consumo a uma rede de telecomunicações na Austrália
14	a pessoa é uma empresa constitucional que: (a) produz; ou (b) fornece; ou (c) instala; ou (d) mantém; dispositivos de processamento de dados	(a) produção, pela pessoa, de dispositivos de processamento de dados para uso, ou com probabilidade de serem usados, na Austrália; ou (b) o fornecimento, pela pessoa, de dispositivos de processamento de dados para uso, ou com probabilidade de serem usados, na Austrália; ou (c) a instalação, pela pessoa, de dispositivos de processamento de dados na Austrália; ou (d) a manutenção, pela pessoa, de dispositivos de processamento de dados na Austrália

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

Provedor de comunicações designado e atividades elegíveis		
Item	**Uma pessoa é um provedor de comunicações designado se ...**	**... e as atividades elegíveis da pessoa são ...**
15	a pessoa é uma empresa constitucional que: (a) desenvolve; ou (b) fornece; ou (c) atualiza; programa de computador que seja capaz de ser instalado em um computador, ou outro equipamento, que esteja, ou com probabilidade de estar, conectado a uma rede de telecomunicações na Austrália	(a) o desenvolvimento, pela pessoa, de qualquer programa de computador desse tipo; ou (b) o fornecimento, pela pessoa, de qualquer programa de computador desse tipo; ou (c) a atualização, pela pessoa, de qualquer programa de computador desse tipo.

Nota 1: Ver também as seções 317HAA, 317MAA e 317TAA (fornecimento de parecer aos provedores de comunicações designados).

Nota 2: Ver também a seção 317ZT (base constitucional alternativa).

……

317E Ações ou coisas listada

(1) Para os fins da aplicação deste Capítulo a um provedor de comunicações designado, ***ação ou coisa listada*** significa:

(a) remover uma ou mais formas de proteção eletrônica que são ou foram aplicadas pelo provedor, ou em seu nome; ou

(b) fornecer informações técnicas; ou

(c) instalar, manter, testar ou usar programa de computador ou equipamento; ou

(d) garantir que as informações obtidas em conexão com a execução de um mandado ou autorização sejam fornecidas em um determinado formato; ou

(da) um ato ou coisa feita para auxiliar, ou facilitar:

(i) a efetividade de um mandado ou autorização sob uma lei da Comunidade, de um Estado ou de um Território; ou

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

(ii) o efetivo recebimento de informações em conexão com um mandado ou autorização sob uma lei da Comunidade, de um Estado ou de um Território; ou

(e) facilitar ou auxiliar o acesso a qualquer um dos itens a seguir que sejam objeto de atividades elegíveis do provedor:

(i) um recurso;

(ii) equipamento de consumo;

(iii) um dispositivo de processamento de dados;

(iv) um serviço de conexão listado;

(v) um serviço que facilita, ou é acessório ou incidental a, o fornecimento de um serviço de conexão listado;

(vi) um serviço eletrônico;

(vii) um serviço que facilita, ou é acessório ou incidental a, a prestação de um serviço eletrônico;

(viii) programa de computador usado, para uso, ou com probabilidade de ser usado, em conexão com um serviço de conexão listado;

(ix) programa de computador usado, para uso, ou com probabilidade de ser usado, em conexão com um serviço eletrônico;

(x) programa de computador que seja capaz de ser instalado em um computador, ou outro equipamento, que esteja, ou com probabilidade de estar, conectado a uma rede de telecomunicações; ou

(f) auxiliar no teste, modificação, desenvolvimento ou manutenção de uma tecnologia ou ferramenta; ou

(g) notificar determinados tipos de mudanças ou desenvolvimentos que afetem as atividades elegíveis do provedor de comunicações designado, se as mudanças forem relevantes para a execução de um mandado ou autorização; ou

(h) modificar, ou facilitar a modificação, de qualquer uma das características de um serviço fornecido pelo provedor de comunicações designado; ou

(i) substituir, ou facilitar a substituição de, um serviço fornecido pelo provedor de comunicações designado por:

(i) outro serviço fornecido pelo provedor; ou

(ii) um serviço fornecido por outro provedor de comunicações designado; ou

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

(j) uma ação ou coisa feita para ocultar o fato de que algo foi feito secretamente no desempenho de uma função, ou o exercício de um poder, conferido por uma lei da Comunidade, de um Estado ou de um Território, na medida em que a função ou poder se relacione a:

(i) aplicação da lei criminal, na medida em que se relacione a infrações australianas graves; ou

(ii) auxiliar na aplicação das leis criminais vigentes em um país estrangeiro, na medida em que essas leis se relacionem com infrações estrangeiras graves; ou

(iii) os interesses de segurança nacional da Austrália, os interesses de relações exteriores da Austrália ou os interesses de bem-estar econômico nacional da Austrália.

(2) O parágrafo (1) (j) não se aplica a:

(a) fazer uma declaração falsa ou enganosa; ou

(b) envolver-se em conduta desonesta.

……

Termos de conformidade

317ZK Termos e condições nas quais a ajuda deve ser prestada etc.

Âmbito

(1) Esta seção se aplica se um fornecedor de comunicações designado estiver sujeito a um requisito sob:

(a) uma notificação de assistência técnica; ou

(b) uma notificação de ferramenta técnica;

……

Termos e condições

(4) O fornecedor de comunicações designado deve estar em conformidade com os requisitos dos termos e condições que são:

(a) acordadas entre as seguintes partes:

(i) o fornecedor;

(ii) o negociador de custos aplicáveis; ou na

(b) na falta de acordo, determinadas por árbitro indicado pelas partes.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

……

317V Critérios de tomada de decisão

O Procurador-Geral não deve fornecer uma notificação de ferramenta técnica a um provedor de comunicações designado, a menos que:

(a) o Procurador-Geral esteja convencido de que os requisitos impostos pela notificação são razoáveis e proporcionais; e

(b) o Procurador-Geral esteja convencido de que o cumprimento da notificação é:

(i) praticável; e

(ii) tecnicamente viável.

……

317WA Avaliação e relatório

O provedor de comunicações designado pode solicitar a realização da avaliação

……

(7) Ao realizarem uma avaliação nos termos do parágrafo (6) (a), em relação a uma notificação de ferramenta técnica proposta a ser entregue a um provedor de comunicações designado, os avaliadores devem:

(a) considerar:

(i) se o aviso de capacidade técnica proposto infringiria a seção 317ZG; e

(ii) se os requisitos impostos pela notificação de ferramenta técnica proposta são razoáveis e proporcionais; e

(iii) se o cumprimento da notificação de ferramenta técnica proposta é praticável; e

(iv) se o cumprimento da notificação de ferramenta técnica proposta é tecnicamente viável; e

(v) se a notificação de ferramenta técnica proposta é a medida menos intrusiva que seria eficaz para atingir o objetivo legítimo da notificação de ferramenta técnica proposta; e

(b) dar maior peso ao assunto mencionado no subparágrafo (a) (i).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

8. Sobre os autores

8.1. George Barker

George Barker é diretor do LECA e especialista em análise econômica de leis e regulamentos. Atualmente é Professor Associado Honorário na *Australian National University* (ANU) e membro do *Wolfson College*, *University of Oxford*. Ele ensinou economia regulatória para equipes de agências reguladoras e empresas reguladas da Austrália, conduziu pesquisas de interesse público e forneceu consultoria econômica especializada e pareceres sobre uma ampla gama de assuntos relacionados à regulamentação da indústria de tecnologia da informação e comunicação (por exemplo, regulamentação da Internet, alocação e uso de espectro, provedoras e serviços de conexão, e acesso à rede) e indústrias de serviços públicos (por exemplo, energia e transporte), bem como direito de concorrência, propriedade intelectual, contratos e legislação tributária que afetam uma ampla variedade de outras indústrias na Austrália, Ásia-Pacífico, América do Norte e Europa. O Dr. Barker contribuiu para várias análises de políticas regulatórias e de concorrência na Austrália, Ásia-Pacífico, América do Norte e Europa. O Dr. Barker deu parecer técnico como especialista em todo o mundo, perante agências reguladoras e tribunais que revisam decisões regulatórias em fase de apelação - bem como em casos de arbitragem em Haia - e perante ministros e parlamentos envolvidos em investigações e processos de reforma na Austrália, Reino Unido, UE, Novo Zelândia, China, Coréia, Japão e Filipinas. Ele deu, por exemplo, parecer técnico aos tribunais federais dos EUA, ao Tribunal Federal da Austrália, ao Tribunal Superior da Nova Zelândia e sua análise foi citada na Câmara dos Lordes do Reino Unido, pelo Tribunal Superior da Inglaterra e País de Gales e pela Comissão Europeia. Ele foi Diretor do *Centre for Law and Economics* na *Australian National University* de 1997-2017 e recebeu o *Olin Fellowship* em *Law and Economics* na *Cornell University USA* em 2000, e foi *Visiting Fellow* na *London School of Economics* (LSE) (2015-2018), no *Centre for Law and Economics* da *University College London* (2010-2015), na *Oxford University* 2008, e no *British Institute of International and Comparative Law* (BIICL) (2009-presente). Ele foi *Chief Analyst and Economic Advisor* do Ministério do Tesouro da Nova Zelândia 1984-1997. É membro do Conselho Editorial do *European Journal of Law and Economics*. Ele obteve um Doutorado em Economia pela *Oxford University* em 1992, e possui Mestrado em Economia (Hons) e é Bacharel em Direito.

8.2. William Lehr

William Lehr é um Economista e consultor do setor de telecomunicações e Internet com mais de 25 anos de experiência. Ele regularmente assessora executivos seniores da indústria e formuladores de políticas nos Estados Unidos e no exterior sobre o mercado, a indústria e as implicações políticas de eventos relevantes para o ecossistema da Internet. Ele é um cientista pesquisador no *Computer Science and Artificial Intelligence Laboratory* (CSAIL) no *Massachusetts Institute of Technology*, atualmente envolvido

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

em uma série de projetos de pesquisa multidisciplinares dentro do *Advanced Networking Architecture Group* do CSAIL. A pesquisa do Dr. Lehr concentra-se na economia e na política regulatória das indústrias de infraestrutura da Internet. Ele está envolvido em vários projetos de pesquisa multidisciplinares com foco em questões como acesso à Internet em banda larga, segurança cibernética, arquiteturas de rede de última geração e gerenciamento de espectro. Além de seu trabalho acadêmico, o Dr. Lehr assessora clientes do setor público e privado nos Estados Unidos e no exterior em questões de estratégia e política de TIC. O Dr. Lehr possui PhD em Economia por Stanford, MBA em Finanças pela *Wharton School*, e MSE, BA e BS pela *University of Pennsylvania*. Para obter mais informações, consulte http://people.csail.mit.edu/wlehr/. Para este compromisso, o Dr. Lehr foi nomeado Diretor de Consultoria no LECA.

8.3. Mark Loney

Mark Loney é Diretor de Consultoria no LECA e especialista em sistemas e tecnologias de comunicações avançadas, políticas públicas e gestão do setor público. Mark foi um Executivo Sênior no Serviço Público Australiano por quinze anos e tem prestado consultoria independente sobre gerenciamento de espectro e questões regulatórias de telecomunicações para clientes internacionais desde 2019. Gerente Executivo da *Australian Communications and Media Authority* (ACMA) de 2005-2018, Mark desempenhou um papel fundamental no estabelecimento do regulador de comunicações convergentes da Austrália de 2004 a 2005. Mark liderou o desenvolvimento, implementação e entrega de acordos regulatórios para serviços de radiodifusão, radiocomunicações e telecomunicações por mais de vinte anos na Spectrum Management Agency, Australian Communications Authority e a ACMA. Mark foi Vice-Chefe da Delegação Australiana para a Conferência Mundial de Radiocomunicações de 2003.

Mark ingressou no Serviço Público Australiano em 1988 no Departamento de Defesa, onde esteve envolvido em pesquisas de comunicações complexas por quase 9 anos. Desde 2010, Mark é co-autor de artigos para séries de conferências do IEEE, como DySPAN e também para o *Journal of Telecommunications Policy* (TelPol). Em 2014, Mark aconselhou o Governo da Mongólia sobre a rápida transição para redes móveis de próxima geração (LTE/LTE Advanced) e questões associadas, como *backhaul* e requisitos de segurança. Mark possui BA pela *Curtin University* e fez estudos de pós-graduação na *Australian National University*.

8.4. Doug Sicker

Douglas Sicker é um proeminente especialista global dos EUA em tecnologias de rede e suas aplicações e implicações em outras indústrias, como sistemas sem fio e segurança cibernética, tanto hoje quanto no futuro. Doug é atualmente o *Senior Associate Dean of Computing* e Professor de Ciência da Computação e de Engenharia Elétrica na *University of Colorado*, Denver | Campus de Anschutz. Anteriormente, Doug atuou como *Lord Endowed Chair* na *School of Computer Science* e na Faculdade de

Engenharia da *Carnegie Mellon University* (CMU) e como *Department Head in Engineering*. Ele também foi recentemente o Diretor interino do CyLab na CMU, que reúne especialistas de uma variedade de disciplinas em toda a universidade para colaborar na pesquisa e educação de ponta, projetada para ajudar a criar um mundo no qual a tecnologia possa ser confiável. Doug também atua como Diretor Executivo do *Broadband Internet Technical Advisory Group* (BITAG). Doug atuou como CTO da *National Telecommunications and Information Administration* (NTIA e da *Federal Communications Commission* (FCC), e como consultor sênior do *Department of Justice National Institute of Justice* e foi Presidente da Comissão Diretora do *Network Reliability and Interoperability Council*. Antes disso, ele foi Diretor de Arquitetura Global na *Level 3 Communications, Inc*. Doug publicou amplamente nas áreas de rede, sistemas sem fio, segurança de rede e política de rede. Para os fins deste compromisso, o Dr. Sicker foi nomeado um Diretor de Consultoria no LECA.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060

16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718