Law & Economics Consulting Associates

El impacto económico de las leyes que debilitan el cifrado

Autores:

George Barker, William Lehr, Mark Loney y Douglas Sicker

5 de abril de 2021

Personal de contacto: Dr. George Barker (LECA)
C. e.: George.Barker@cleconsult.com

Encargado por

Internet Society

LECA

Índice

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +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, Reino Unido +44 7554 065 718

1. Resumen ejecutivo[1]

En diciembre de 2018, el Parlamento de Australia aprobó la *Ley de Modificación de la Legislación sobre Telecomunicaciones y otras Leyes (Asistencia y Acceso) (Telecommunications and Other Legislation Amendment (Assistance and Access) Act) de 2018* (más conocida como TOLA)[2], que amplió la autoridad y las capacidades del Gobierno para eludir las protecciones de los datos digitales. La ley TOLA creó un marco de conformidad con el cual los organismos de inteligencia y aplicación de la ley (LEIA)[3] podrían solicitar o exigir a los proveedores de tecnología de la información o, en la terminología de la ley TOLA, a los Proveedores de Comunicaciones Designados (DCP), que proporcionaran asistencia para acceder al contenido de los datos cifrados, lo que puede implicar el intercambio de información empresarial confidencial o el diseño de nuevas capacidades.

El objetivo de este informe es evaluar las pruebas disponibles sobre el impacto de la ley TOLA en la economía australiana y la del mundo. Nuestro análisis nos lleva a la conclusión de que la ley *TOLA tiene el potencial de provocar un daño económico considerable a la economía australiana y producir efectos indirectos negativos que amplificarán ese daño a nivel mundial*. Cuando decimos "considerable" nos referimos a un daño económico que asciende a varios *miles de millones de dólares*, que son de base amplia y que probablemente se materializará (sobre todo) en los próximos años.

Hay numerosos mecanismos por los que la ley TOLA puede causar daños económicos. Por ejemplo, esta ley aumenta la incertidumbre empresarial. En los estudios realizados por el Instituto Nacional de Normas y Tecnología (NIST) de los EE. UU. en 2001 y 2018 se concluyó que las intervenciones patrocinadas por el Gobierno que redujeron la incertidumbre sobre la seguridad digital dieron lugar a beneficios agregados por valor de muchos miles de millones de dólares.[4] Al aumentar la incertidumbre entre los participantes del mercado digital en cuanto a las mejores formas de asegurar la información digital, la ley TOLA puede impedir la materialización de beneficios análogos.

En segundo lugar, la ley TOLA puede perjudicar la imagen de marca de los proveedores DCP que operan en Australia y que son vulnerables a la amenaza que esta ley supone para la seguridad digital de los productos y servicios que ellos comercializan. Los clientes, entre los que se encuentran tanto empresas como usuarios de Internet del mercado masivo, preocupados por la posibilidad de que sus datos sean menos seguros

[1]Reconocimiento: agradecemos a Internet Society por el apoyo financiero prestado para llevar a cabo esta investigación. Los puntos de vista expresados en ella, no obstante, así como cualquier error que pudiera haber, son solo responsabilidad de los autores.

[2]También conocida como ley del cifrado o ley sobre asistencia y acceso, https://www.legislation.gov.au/Details/C2018A00148/Download

[3]LEIA significa organismos de inteligencia y aplicación de la ley, entre los que se encuentran los organismos gubernamentales legalmente facultados para solicitar acceso gubernamental a los datos.

[4]Véase NIST (2015, 2018), que se examina más adelante y al que se hace referencia en las notas 110, 112 *infra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

debido a la ley TOLA, pueden optar por llevar su negocio a otra parte. Estas respuestas pueden reducir los ingresos de los proveedores DCP y aumentar sus costos operativos, ya que estos adoptan estrategias para contrarrestar las amenazas relacionadas con la ley TOLA. Estos efectos directos no tienen por qué limitarse a los proveedores DCP que reciban notificaciones de la ley TOLA: ellos pueden incidir en los DCP que tomen medidas previendo que han de recibir una notificación de la ley TOLA o en otras entidades preocupadas por el impacto de dicha ley. Estas entidades no tienen por qué limitarse a los proveedores DCP, sino que pueden incluir a sus clientes. En conjunto, es probable que estos efectos directos e indirectos tengan una amplia base y se acumulen con el tiempo a medida que las repercusiones se propaguen por la economía.

En tercer lugar, quizá la mayor fuente de efectos económicos adversos sea la amenaza indirecta que la ley TOLA supone para la confianza en los servicios digitales, incluida Internet. Estamos en medio de una transición mundial hacia una economía digital en la que el comercio electrónico y la información digital en las redes desempeñan un papel cada vez más importante, que afecta a todos los países, todos los sectores y todas las empresas. Si los servicios y las redes que apoyan esta actividad son de confianza (por ejemplo, los proveedores DCP), las perspectivas de crecimiento económico son buenas. Se espera que la reducción de la confianza en la seguridad de los datos deprima la demanda agregada en toda la economía digital e induzca a las empresas a incurrir en mayores costos para tratar de compensar los perjuicios derivados de la reducción de la confianza.[5] Además, dado que la tecnología digital se utiliza en toda la economía, estos efectos abarcan la totalidad de esta última e impactan en todos los aspectos del funcionamiento de las empresas modernas. En consecuencia, incluso las pequeñas amenazas a la ciberseguridad, o lo que es lo mismo, a la confianza digital, tienen el potencial de provocar grandes efectos adversos. Un estudio muestra cómo las amenazas a la confianza digital pueden traducirse en daños mundiales del orden de un billón de dólares o más.[6] Medir, atribuir y cuantificar el impacto adverso que la ley TOLA tendrá en la confianza digital no es factible con los datos disponibles. Además, dado que estos efectos se producirán sobre todo en los próximos años, la estimación del impacto depende de que se formulen previsiones adecuadas sobre lo que ocurriría con esta ley y sin ella. Tales previsiones dependerán de una amplia gama de supuestos de modelización que probablemente serán controvertidos.

Aunque podemos identificar múltiples vectores a través de los cuales los daños de la ley TOLA pueden propagarse, los datos no nos permiten ofrecer una cuantificación más precisa de los probables daños económicos que esta ley supone. Esto se debe a múltiples motivos que se analizan con más detalle en el informe, pero entre ellos se encuentran los siguientes:

- La estimación del impacto económico de la ley TOLA es intrínsecamente compleja y difícil. Esta ley puede tener impactos económicos adversos tanto directa como indirectamente de múltiples maneras. Algunas son más fáciles

[5]En 2019, el 18 % de los que desconfiaban de Internet respondieron que hacían menos compras en línea (véase https://www.internetsociety.org/wp-content/uploads/2019/06/CIGI-Ipsos-Trust-User-Privacy_Report_2019_EN.pdf).

[6]Por ejemplo, véase el estudio del Zurich Insurance Group (2015), nota 105 *infra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

de rastrear y estimar que otras, pero para captar todos los efectos es importante no centrarse solo en lo que es fácilmente observable.

- Hasta la fecha, la aplicación de la ley TOLA ha sido limitada. Desde su aprobación, múltiples revisiones y diversos actores han expresado su preocupación por la posibilidad de que ella provoque importantes daños económicos y han pedido que se modifique para reducir esa amenaza. El poco tiempo transcurrido desde la aprobación de la ley TOLA y las preocupaciones sobre la mejor manera de responder a la oposición que ella ha generado pueden explicar los escasos datos empíricos sobre los costos que se puedan atribuir a ella.
- El acceso a datos relacionados con la ley TOLA para utilizarlos en el cálculo de los impactos económicos está muy limitado por la falta de transparencia y las disposiciones de no divulgación que forman parte de esta ley. Esta falta de datos supone una amenaza para la supervisión eficaz, en particular para la capacidad de los analistas que intentan hacer cálculos sólidos desde el punto de vista teórico y empírico sobre los impactos de la ley TOLA.

Además, aunque la atención se centra aquí en los posibles costos de la ley TOLA, el examen de los posibles beneficios sugiere que estos últimos serían aún más difíciles de estimar. No está claro si esta ley ha mejorado o mejorará el acceso de los organismos LEIA a los datos digitales o si aumentará la eficacia operativa de estos organismos. Además, en general se acepta que una de las formas más importantes de fomentar la ciberseguridad es promover una mayor adopción del cifrado de extremo a extremo.[7] La ley TOLA supone un desafío para la adopción más amplia de un cifrado eficaz de extremo a extremo, ya que, por su diseño, esta ley procura brindar una capacidad para acceder al contenido de los datos cifrados.

Nos ha sorprendido comprobar que ni en Australia ni en otros lugares se ha realizado ningún trabajo previo sustancial para estimar empíricamente los costos o beneficios económicos de la ley TOLA o de alguna ley análoga (con implicaciones económicas para la seguridad digital).

A falta de investigaciones de terceros en las que basar una estimación del impacto económico de la ley TOLA, llevamos a cabo una investigación primaria en forma de entrevistas detalladas realizadas por videoconferencia con los principales proveedores DCP multinacionales y por medio de una encuesta anónima realizada con proveedores DCP que tenían operaciones en Australia. Como explicamos con más detalle en el informe, los datos empíricos recogidos son totalmente coherentes y respaldan el análisis del resto del informe. La investigación de las experiencias y expectativas de los proveedores DCP con la ley TOLA proporciona un fundamento empírico para concluir que:

[7]El cifrado de extremo a extremo —en el que las claves necesarias para descifrar una comunicación cifrada residen solo en los dispositivos que se comunican— proporciona el nivel más fuerte de seguridad y confianza, porque por diseño, solo el destinatario tiene la clave para descifrar el mensaje (véase 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, Reino Unido +44 7554 065 718

1. Es de esperar que la ley TOLA tenga un impacto adverso en las empresas y sus clientes que sea de base amplia (*es decir*, que no se limite a las empresas de los sectores de las TIC).
2. La mayor parte de los daños previstos serán indirectos y estarán asociados a la amenaza que la ley TOLA supone para la percepción de los clientes y los socios del sector sobre la confianza digital.
3. Sigue habiendo una incertidumbre considerable sobre la ley TOLA y sus efectos.
4. Los datos empíricos directos sobre los costos (o beneficios) económicos son muy limitados, pero atribuimos ese hecho a lo siguiente: a) la falta de transparencia que caracteriza a las actividades relacionadas con la ley TOLA debido a las disposiciones de no divulgación; b) el escaso tiempo transcurrido desde la aprobación de esta ley y la controversia aún vigente que impide que los organismos LEIA apliquen la autoridad que esta ley les brinda, y c) la previsión de que los impactos sean probablemente indirectos y ocurran en el futuro.
5. Los limitados datos directos que observamos apoyan la conclusión de que los beneficios específicos de las empresas son probablemente pequeños, mientras que sus costos específicos pueden ser bastante grandes.
6. Los datos empíricos disponibles no proporcionan una base fiable para cuantificar el impacto económico agregado en dólares de la ley TOLA.

Los datos también fueron coherentes con nuestra expectativa de que las pruebas empíricas de los efectos directos de la ley TOLA serían escasas y difíciles de observar. Sin embargo, esta falta de datos empíricos *no* es prueba de que no haya ningún efecto. No obstante, los escasos datos recopilados son reveladores. Uno de los encuestados que había experimentado un impacto económico adverso directo estimaba que el efecto había sido del orden de los mil millones de dólares (australianos), [8]mientras que el único encuestado que opinaba que el impacto de la ley TOLA era mayoritariamente favorable consideraba que el principal efecto de esta ley era la racionalización de la legislación existente.[9]Ambas observaciones son coherentes con la conclusión de que los beneficios específicos para las empresas son probablemente pequeños, mientras que los costos específicos para ellas pueden ser bastante grandes. Aunque la investigación empírica apoya la conclusión general del informe, el tamaño de la muestra impide utilizarla como base para hacer una cuantificación más precisa de esos daños.

Conclusiones

En conjunto, este análisis nos lleva a concluir que la ley *TOLA supone un riesgo significativo de que en el futuro se produzcan daños económicos netos para la*

[8]El resultado adverso se atribuyó directamente al daño que la ley TOLA causó a la imagen de marca del proveedor DCP, lo que provocó pérdidas en las ventas actuales y futuras. Véase un análisis más completo de los resultados de las entrevistas y la encuesta en el capítulo 6.

[9]Antes de la ley TOLA, un subconjunto de los proveedores DCP estaba sujeto a la legislación vigente que permitía el acceso del Gobierno a los datos digitales. Uno de los encuestados opinaba que la ley TOLA reducía los costos al racionalizar la exposición de la empresa a la legislación vigente. El encuestado no proporcionó una estimación del ahorro en materia de costos, pero consideraba que este no era muy grande.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

economía de Australia, con probables efectos indirectos adversos en el extranjero. Las pruebas preliminares demuestran que algunas empresas ya han experimentado daños económicos significativos, aunque parece probable que la mayor parte del impacto agregado de los daños se produzca en el futuro y sea generalizado, si la amenaza que la ley TOLA supone para el cifrado, persiste. Además de eso, la confusión y la incertidumbre que la ley TOLA causa a los proveedores DCP siguen vigentes y todavía no han sido debidamente abordadas.

Si bien los desafíos que supone estimar el impacto económico son difíciles, no ha habido *ninguna* investigación pública que intente cuantificar los impactos económicos de la ley TOLA o de otras leyes similares en Australia o en otros lugares. Sin embargo, la falta de datos empíricos no implica que el impacto no sea considerable. Por el contrario, sugiere que la carga de la prueba debería trasladarse a la evaluación de los argumentos según los cuales es de esperar que la ley TOLA produzca beneficios considerables, ya que el riesgo de que produzca daños considerables es claro.

2. Introducción y descripción general

El presente informe se centra en proporcionar una evaluación de los datos disponibles sobre el impacto económico de la *Ley de Modificación de la Legislación sobre Telecomunicaciones y otras Leyes (Asistencia y Acceso) (Telecommunications and Other Legislation Amendment (Assistance and Access) Act) de 2018* (más conocida como "TOLA").[10]

La ley TOLA representa una legislación importante y compleja. Como explicaremos más adelante, modifica siete leyes importantes del Parlamento australiano relacionadas con la seguridad de la información, y se basa en y contribuye a la labor legislativa relacionada llevada a cabo en una serie de otros países, como el Reino Unido y los Estados Unidos. Por consiguiente, se espera que tenga consecuencias a nivel tanto nacional (para Australia) como internacional en lo que respecta a la labor destinada a asegurar los datos digitales.

Esta ley se centra en la creación de nuevas capacidades gubernamentales que permiten eludir el cifrado mediante la ampliación de la facultad del Gobierno para solicitar (o exigir) que los proveedores de comunicaciones digitales (DCP) lo asistan para acceder a los datos digitales, entre ellos los datos cifrados. La definición de los proveedores DCP en el marco de la ley TOLA es bastante amplia y abarca una gama mayor de empresas y actividades relacionadas con el suministro de productos y servicios de tecnología de la información y la computación (TIC).

En el capítulo 3 se ofrece un breve resumen de la historia y el impacto jurídico de la ley TOLA. Tras un proceso abreviado y rápido, esta ley se aprobó en diciembre de 2018. Posteriormente ha sido objeto de múltiples revisiones, en cada una de las cuales se han recomendado modificaciones de la ley y de su aplicación.

[10]Para consultar el texto de la ley TOLA, véase https://www.legislation.gov.au/Details/C2018A00148/Download. La ley TOLA también se denomina a veces "ley del cifrado", "ley australiana sobre la asistencia y el acceso" o "AAA".

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

En el capítulo 4 se explica el papel fundamental que desempeña el cifrado en la seguridad de los datos digitales y se destacan algunas de las consecuencias técnicas de ampliar las capacidades para eludirlo.

En el capítulo 5 se abordan los posibles impactos económicos de la ley TOLA. La conclusión que se desprende de este análisis es que la ley TOLA podría generar importantes costos económicos futuros que probablemente no se verán compensados por futuros beneficios económicos. Esta conclusión se justifica aunque no sea posible cuantificar de forma precisa del impacto económico neto sobre la base de los datos y las investigaciones disponibles hasta la fecha, en parte debido a la falta de transparencia que la ley TOLA crea.

En el capítulo 6 se presentan los resultados de la investigación primaria realizada en el marco de este proyecto. En ella se llevaron a cabo entrevistas detalladas con los principales proveedores DCP multinacionales y una encuesta anónima con DCP que tienen operaciones en Australia para evaluar sus experiencias y expectativas con respecto a la ley TOLA desde su aprobación en 2018. La encuesta fue similar a dos que se habían realizado anteriormente: la primera realizada en la víspera de la aprobación de la ley TOLA, y la segunda, un año después. Aunque los resultados de esta investigación son insuficientes para proporcionar una base empírica fiable que permita cuantificar el impacto esperado de la ley TOLA, los resultados fueron coherentes y apoyan la conclusión a la que se arriba en el capítulo 5.

En conjunto, este análisis nos lleva a concluir que la ley *TOLA supone un riesgo significativo de que en el futuro se produzcan daños económicos netos para la economía de Australia, con probables efectos indirectos adversos en el extranjero.* Las pruebas preliminares demuestran que algunas empresas ya han experimentado daños económicos significativos, aunque parece probable que la mayor parte del impacto agregado de los daños se produzca en el futuro y sea generalizado, si la amenaza que la ley TOLA supone para el cifrado, persiste.Además de eso, la confusión y la incertidumbre que la ley TOLA causa a los proveedores DCP siguen vigentes y todavía no han sido debidamente abordadas.

Si bien los desafíos que supone estimar el impacto económico son difíciles, no ha habido *ninguna* investigación pública que intente cuantificar los impactos económicos de la ley TOLA o de otras leyes similares en Australia o en otros lugares. Sin embargo, la falta de datos empíricos no implica que el impacto no sea considerable. Por el contrario, esto sugiere que la carga de la prueba debería trasladarse a la evaluación de los argumentos según los cuales es de esperar que la ley TOLA produzca beneficios considerables, ya que el riesgo de que produzca daños económicos generalizados y considerables es claro.

3. Estructura y antecedentes de la ley TOLA

En las siguientes dos subsecciones ofrecemos una descripción general de alto nivel de la estructura jurídica de la ley TOLA y de su historia hasta la fecha. En primer lugar, describimos cómo la ley TOLA amplía la autoridad gubernamental a los efectos de obtener la asistencia del sector para acceder a la información digital cifrada. En segundo

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

lugar, repasamos la historia de la ley TOLA desde sus orígenes recientes hasta las múltiples revisiones que se encuentran en curso.

3.1. Revisión estructural de la ley TOLA

Mediante la ley TOLA se introducen modificaciones amplias y considerables en siete leyes importantes del Parlamento australiano con el fin de "adoptar medidas que permitan afrontar mejor los desafíos que plantea la omnipresencia del cifrado" para los organismos de inteligencia y aplicación de la ley (LEIA).[11]Las leyes afectadas son las siguientes:[12]

1. La Ley de Telecomunicaciones de 1997 (*Telecommunications Act 1997*) (TA1997)[13]
2. La Ley de Telecomunicaciones (Interceptación y Acceso) de 1979 (*Telecommunications (Interception and Access) Act 1979*) (ley TIA)[14]
3. La Ley de Dispositivos de Vigilancia de 2004 (*Surveillance Devices Act 2004*) (ley SD)[15]
4. La Ley sobre Delitos de 1914 (*Crimes Act 1914*) (Ley sobre Delitos)[16]
5. La Ley de Asistencia Recíproca en Materia Penal de 1987 (*Mutual Assistance in Criminal Matters Act 1987*) (MACMA)[17]
6. La Ley de la Organización de Inteligencia de Seguridad Australiana de 1979 (*Australian Security Intelligence Organisation Act 1979*) (ley ASIO),[18] y
7. La Ley de Aduanas de 1901 (*Customs Act 1901*) (ley de Aduanas)[19]

3.1.1. Ampliación de la autoridad gubernamental para acceder a los datos cifrados

Con 228 páginas, la ley TOLA es una pieza legislativa sustancial compuesta por cinco anexos que abordan diferentes aspectos de las capacidades del Gobierno para obtener acceso legítimo a la información digital. Nuestro análisis se centra en el anexo 1, en el que se introducen nuevas capacidades para solicitar o exigir la asistencia de una "gama

[11]La cita es del párrafo inicial del Memorando Explicativo que acompañó a la introducción de la ley TOLA en el Parlamento australiano en septiembre de 2018.Véase "Explanatory Memorandum", distribuido a la Cámara de Representantes por el ministro de Asuntos Internos, el honorable Peter Dutton MP, sobre la introducción de la ley TOLA, 20 de septiembre de 2018, disponible en https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r6195%22 (en adelante, Memorando Explicativo 2018).

[12]Véase el apartado 1 del Memorando Explicativo de 2018, nota 11 *supra*.

[13]TA1997 disponible enhttps://www.legislation.gov.au/Series/C2004A05145.

[14]Ley TIA disponible en https://www.legislation.gov.au/Series/C2004A02124.

[15]Ley SD disponible en https://www.legislation.gov.au/Series/C2004A01387.

[16]Ley sobre Delitos disponible en https://www.legislation.gov.au/Series/C1914A00012.

[17]MACMA disponible en https://www.legislation.gov.au/Series/C2004A03494.

[18]Ley ASIO disponible en https://www.legislation.gov.au/Series/C2004A02123.

[19]Ley de Aduanas disponible en 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, Reino Unido +44 7554 065 718

más amplia de proveedores" del sector para acceder a la información digital cifrada.[20] Por lo tanto, el énfasis que ponemos aquí en el impacto económico de la ley TOLA y en la demanda de cifrado y el uso de este está justificado.

En resumen, la ley TOLA permite a un selecto pero amplio número de diferentes organismos LEIA solicitar o exigir a un Proveedor de Comunicaciones Designado (DCP) que proporcione asistencia tecnológica para eliminar o eludir el cifrado utilizando tres instrumentos jurídicos a los que aquí nos referiremos de forma colectiva como "notificaciones de la ley TOLA":[21]

1. Solicitud de Asistencia Técnica **(TAR)**: solicitud en la que se pide a un Proveedor de Comunicaciones Designado (DCP) que:
    1. ofrezca *voluntariamente* ayuda o asistencia a un organismo gubernamental, y/o
    2. cree *voluntariamente* capacidad para ayudar a un organismo gubernamental.
2. Notificación de Asistencia Técnica **(TAN)**: similar a una solicitud TAR, excepto que es obligatoria. Se trata de una orden en lugar de una solicitud emitida a un proveedor DCP, y debe estar limitada únicamente a exigir ayuda, sin que se exija crear capacidad para ayudar.
3. Notificación de Capacidad Técnica (**TCN**): una vez más se trata de una orden obligatoria que exige u ordena que un proveedor DCP cree una nueva capacidad que permita eludir el cifrado,[22] y también puede exigir que se ofrezca ayuda o asistencia.

Cada tipo de notificación de la ley TOLA está sujeta a diferentes requisitos legales en cuanto a quién puede emitir la notificación, las circunstancias y las normas del debido proceso que rigen el uso de la capacidad, lo que puede solicitarse u obligarse, y la supervisión y las opciones de apelación que los destinatarios de las notificaciones TOLA tienen a su alcance.

Las notificaciones de la ley TOLA crean nuevas capacidades gubernamentales para solicitar y exigir al sector lo siguiente: a) que preste asistencia; y/o b) que proporcione una capacidad para eludir el cifrado. Ambos tipos de facultades suscitan preocupación, pero es la amenaza de que el destinatario de una notificación de la ley TOLA pueda ser

[20]Véase 8 y 10 del Memorando Explicativo 2018, nota 3 *supra*.

[21]La ley TOLA aborda este tema en su anexo 1, que comprende más de la mitad de la ley, donde propone añadir una nueva "Parte 15-Asistencia del sector" a la ley TA1997 (véanse las páginas 4 a 109 de la ley TOLA, Nota 2, *supra*).

[22]Si bien la eliminación de una o varias formas de protección electrónica (es decir, la eliminación del cifrado) se incluye como uno de los actos o cosas enumeradas que se pueden solicitar en una TAR o que se pueden exigir en una TAN (véase el art. 317E (1)(a) de la ley TOLA, nota 2 *supra*), la ley TOLA no permite exigir en una TCN que un proveedor DCP habilite la capacidad para eliminar el cifrado (véase el art. 317T(4)(c)(i) de la ley TOLA, nota 2 *supra*).Dado que en las TCN se puede exigir a los proveedores DCP que proporcionen una capacidad para permitir otros actos enumerados en el art. 317E, las TCN pueden dar lugar a que se exija a los proveedores DCP que proporcionen capacidades que puedan ayudar a los organismos LEIA a eludir el cifrado.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

llamado a crear una capacidad para eludir el cifrado la que ha suscitado las mayores preocupaciones. Una vez creada, dicha capacidad podría servir de base para eludir el cifrado de cualquier información digital a la que se aplique, y no solo el de la información digital del objetivo designado que en un principio justificó la solicitud presentada en virtud de la ley TOLA.[23]

Sin conocer la naturaleza precisa de la capacidad que podría crearse, es imposible conocer la magnitud de la amenaza a la seguridad digital que dicha capacidad podría suponer. En la ley TOLA se trató de resolver esta obvia preocupación limitando las solicitudes de la ley a aquellas que no darían lugar a la creación de una "vulnerabilidad sistémica". Es decir que las solicitudes de asistencia o de creación de capacidad dirigidas al sector serían lo suficientemente acotadas como para abordar el objetivo o los objetivos particulares del interés de la orden legal de la autoridad gubernamental, y no crearían una vulnerabilidad de seguridad que afectaría a otros que no son el objetivo.[24] Como se expone más adelante, la eficacia de esta limitación sigue suscitando preocupación.

Los tipos de asistencia o capacidades que los organismos gubernamentales pueden solicitar en virtud de la ley TOLA son amplios y complejos. Entre ellos se encuentra "eliminar una o varias formas de protección electrónica", lo que incluye el cifrado, pero también "proporcionar información técnica", "facilitar... el acceso a... un centro, al equipo de un cliente, a un dispositivo de procesamiento de datos, a un servicio de telecomunicaciones listado, ..., a un software", etcétera.[25] Si bien en la legislación australiana ya había disposiciones que autorizaban a los organismos gubernamentales a solicitar la asistencia del sector en la ejecución de órdenes judiciales y en el acceso a datos digitales, la ley TOLA amplía considerablemente esa facultad.[26] Además, como

[23]Por ejemplo, una capacidad puede, una vez creada, servir de base para que terceros que no eran el objetivo original de la notificación de la ley TOLA eludan la seguridad digital. Las violaciones por parte de esos terceros pueden ser intencionales (por ejemplo, actores maliciosos que tengan la intención de adquirir acceso a información confidencial) o no intencionales (por ejemplo, actores que pongan en peligro la seguridad digital por ignorancia o descuido).La cuestión es que una vez que se ha creado una capacidad para eludir el cifrado, restringir su posterior uso supone un desafío adicional.

[24]La ley TOLA define una vulnerabilidad sistémica o debilidad sistémica como una vulnerabilidad o debilidad que afecta a toda una clase de tecnología (véanse las páginas 12, 84-81 de la ley TOLA, nota 2 *supra*).

[25]En el art. 317E de la ley TOLA figura una lista de los distintos tipos de ayuda que pueden solicitarse (páginas 18 a 20 de la ley TOLA, nota 2 *supra*).

[26]Por ejemplo, en la Parte 14 de la Ley TA1997 se impone a los operadores y proveedores de servicios de telecomunicaciones la obligación de prestar asistencia a los organismos LEIA en la medida en que sea razonablemente necesario para aplicar el derecho penal, ayudar en la investigación y el procesamiento de delitos y salvaguardar la seguridad nacional (véanse las páginas 322-328 de la Ley TA1997IA, nota 5 *supra*).Además, en el capítulo 5 de la Ley TIA se establece la obligación de que los operadores y proveedores de servicios de telecomunicaciones cooperen con los organismos LEIA y presten asistencia en la realización de actividades de interceptación legal (por ejemplo, intervenciones telefónicas) (véanse las páginas 360-410 de la Ley TIA, nota 6 *supra*).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

se ha señalado, la capacidad de solicitar y exigir asistencia para eludir el cifrado es, evidentemente, nueva en Australia.[27] Está claro que la ley TOLA amplía la facultad de los organismos LEIA para eludir el cifrado, pero los límites precisos de ese facultad, si es que los hay, no están claros.

Además de ampliar los tipos de asistencia que los organismos gubernamentales pueden solicitar o exigir al sector, la ley TOLA también amplió la gama de empresas de TIC a las que se aplican dichas obligaciones. Esto representa un cambio significativo. Antes de la ley TOLA, los proveedores de servicios de comunicaciones (CSP) ya solían cooperar con los organismos LEIA para proporcionar acceso legítimo a los datos digitales en una variedad de contextos (p. ej., proporcionando asistencia en la ejecución de intervenciones telefónicas legítimas). La ley TOLA amplía la gama de empresas que deben someterse a las exigencias de la ley para incluir las entidades clasificadas como Proveedores de Comunicaciones Designados (DCP).En la ley TOLA se define a los proveedores DCP como cualquier "persona" que corresponda a alguna de las quince categorías empresariales que se mencionan en el artículo 317C[28] y se enumeran en su totalidad en el Apéndice.

Aunque algunas entidades empresariales identificadas como DCP ya estaban sujetas a obligaciones legales para cooperar con los organismos LEIA en la obtención de acceso legal a la información digital, la ley TOLA amplió significativamente la gama de empresas de TIC que podrían ser objeto de solicitudes u órdenes de asistencia, así como las actividades afectadas. Dado que muchas empresas de TIC se dedican a múltiples actividades que abarcan varias categorías y que la clasificación adecuada de las actividades en categorías puede ser ambigua, está claro que el alcance de la ley TOLA es amplio. Lo que no está claro es qué tipos de empresas de TIC, si es que hay alguna, o qué actividades están exentas de ser destinatarias de las notificaciones de la ley TOLA. Este alcance amplio pero incierto de la ley TOLA significa que el impacto potencial de esta ley es también bastante amplio, ya que incluye esencialmente a todo el sector de las TIC. Además, la mayoría de las empresas de sectores no relacionados con las TIC utilizan en gran medida las TIC y tienen funciones empresariales que pueden ser destinatarias de las notificaciones de la ley TOLA. Podría decirse que

[27]Nuestra afirmación de que la autoridad que la ley TOLA otorga para eludir el cifrado es "nueva" debe tomarse con reservas por los siguientes motivos: a) la autoridad gubernamental para solicitar la asistencia del sector a fin de obtener acceso a la información cifrada existía en el Reino Unido desde antes de la ley TOLA y esta última tomó conceptos de la Ley de Facultades de Investigación del Reino Unido de 2016 (véase "Investigatory Powers Act 2016", Reino Unido, disponible en https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted); y b) se están estudiando numerosas recomendaciones para introducir nuevas modificaciones en la ley TOLA y, dada la complejidad de esta ley y de las leyes con las que se solapa y modifica, está fuera del alcance de este informe proporcionar un análisis jurídico completo de la ley TOLA y del grado en que sus capacidades son realmente novedosas.Los juristas pueden discrepar en cuanto a la interpretación tanto de las modificaciones de esta ley como de la medida en que la legislación anterior a ella que forma parte del marco jurídico relacionado con el acceso legal del Gobierno a la información podría interpretarse como la concesión de cierto nivel de facultades gubernamentales para eludir el cifrado.

[28]Páginas 14 a 18 de la ley TOLA, nota 2 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

cualquier empresa que interactúe con sus proveedores o clientes a través de un sitio web o una aplicación es un proveedor DCP.

El abanico de organismos LEIA que pueden emitir notificaciones de la ley TOLA también es amplio. Abarca organismos responsables de la aplicación de la ley en el ámbito nacional, de la seguridad nacional y de las actividades de seguridad y aplicación de la ley en el ámbito que excede lo nacional (incluida la recopilación de información de inteligencia).[29] La autoridad concedida a los diferentes organismos LEIA en el marco de la ley TOLA se detalla con distintos grados de especificidad. Por ejemplo, el número de organismos LEIA que puede emitir solicitudes TAR (voluntarias) es más amplio que el número que puede emitir notificaciones TAN o TCN (obligatorias).[30]Muchas de las modificaciones de la ley TOLA que se han propuesto y de las inquietudes que se han planteado sobre ella se refieren a la necesidad de mejorar la supervisión para contribuir a garantizar que no se abuse de las nuevas capacidades de acceso a los datos digitales y de elusión del cifrado. Varias de esas modificaciones consisten en revisar las restricciones sobre quién puede emitir notificaciones de la ley TOLA, las circunstancias en las que estas se pueden emitir, el proceso de revisión antes de que estas se aprueben y otras medidas diversas relacionadas con la supervisión. El análisis jurídico completo o la evaluación de la eficacia de estas disposiciones de supervisión y de los esfuerzos por limitar el alcance del impacto de la ley TOLA está más allá del alcance de este informe, pero basta con decir que se han hecho varias recomendaciones importantes dirigidas a que se introduzcan reformas.[31]

En resumen, la ley TOLA crea nuevas y considerables capacidades que permiten a una amplia gama de organismos LEIA solicitar o exigir a una gama más amplia de entidades de TIC que les brinden asistencia para obtener acceso a datos digitales confidenciales y eludir el cifrado. Además, hay gran incertidumbre en lo que se refiere a la naturaleza y los límites de estas facultades.

3.1.2. Información sobre las notificaciones de la ley TOLA y otras disposiciones importantes

Una distinción clave entre los diferentes tipos de notificaciones de la ley TOLA es que, en el caso de una solicitud TAR, el destinatario cumple de forma voluntaria, mientras que, en el caso de una notificación TAN o TCN, el cumplimiento es obligatorio. Esta distinción es importante porque el incumplimiento de una notificación TAN (una

[29]Entre los organismos LEIA respecto de los cuales se señala de forma específica que tienen la capacidad para emitir notificaciones de la ley TOLA se encuentran la Organización de Inteligencia de Seguridad Australiana (ASIO), diversas agencias de interceptación (IA), como varias autoridades policiales, el Servicio Australiano de Inteligencia de Seguridad (ASIS), y la Dirección Australiana de Señales (ASD).

[30]Por ejemplo, la ASIO y las IA pueden emitir los tres tipos de notificaciones (con diferentes restricciones para los distintos tipos de notificaciones), pero el ASIS y la ASD solo pueden emitir notificaciones TAR.

[31]Por ejemplo, como explicamos más adelante en la exposición sobre la historia de la ley TOLA, en el informe del INSLM se pide hacer un cambio importante en la asignación de facultades para emitir notificaciones de la ley TOLA (véase la nota 40 *infra*).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

solicitud obligatoria de "asistencia") o de una notificación TCN (una solicitud obligatoria de "capacidad") hace que el destinatario sea objeto de sanciones que pueden adoptar la forma de responsabilidad civil, multas, órdenes judiciales o procedimientos penales. *Dado que los destinatarios pueden pensar que si se niegan a cumplir una solicitud TAR esto puede llevar a que les llegue una notificación TAN o TCN, la distinción entre una notificación voluntaria y una obligatoria puede ser menos importante de lo que parece a primera vista.* En la medida en que los destinatarios interpreten que el cumplimiento de una solicitud TAR no es realmente "voluntario", el incentivo para cumplirla será mayor.

En todos los casos, los destinatarios de las notificaciones de la ley TOLA tienen prohibido revelar el contenido de dichas notificaciones y las circunstancias relacionadas con su emisión. La divulgación ilegal de las notificaciones de la ley TOLA, al igual que el incumplimiento de las notificaciones obligatorias, puede dar lugar a sanciones legales. Además, la información sobre las notificaciones de la ley TOLA es bastante limitada, ya que no se revela quiénes recibieron las notificaciones y solo se comunican estadísticas generales sobre el número de notificaciones emitidas.[32]Las restricciones a la divulgación y las limitaciones a la hora de informar

[32]Los datos sobre el número exacto de notificaciones de la ley TOLA que se han emitido hasta la fecha son poco claros.La falta de transparencia incluso en lo que respecta al número de notificaciones TOLA emitidas hace que cualquier intento de estimar empíricamente el impacto económico de esta ley sea muy difícil, si no totalmente inviable.Además, la falta de transparencia en cuanto a las empresas (o incluso al tipo de empresas) que recibieron notificaciones de la ley TOLA, qué asistencia se solicitó y cómo respondieron los destinatarios, complica aún más el desafío.

No obstante, lo que creemos es que, hasta la fecha, *solo se han emitido notificaciones voluntarias de la ley TOLA y que el número total de estas notificaciones es probablemente inferior a 50*.No hemos visto que se haya emitido ningún informe sobre notificaciones TAN o TCN. Nuestra estimación del número de notificaciones TAR se basa en lo que se ha comunicado en dos informes oficiales y en algunos discursos. Hay dos informes en que se documenta que se emitieron 18 TAR desde diciembre de 2018 hasta junio de 2020, y dichas notificaciones son las siguientes: Comisión Australiana de Inteligencia Criminal (ACIC), 1; Policía Federal Australiana (AFP), 8; Policía de Nueva Gales del Sur (NSW), 9 (véase el cuadro 45 en DHA (2019), "Telecommunications (Interception and Access) Act 1979 Annual Report 2018-19", Departamento del Interior de Australia (DHA), disponible en https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-18-19.pdf; y el cuadro 44 en DHA (2020), "Telecommunications (Interception and Access) Act 1979 Annual Report 2019-20", Departamento del Interior de Australia (DHA), disponible en https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-19-20.pdf).

Además, el Director General de la Organización de Inteligencia de Seguridad Australiana (ASIO) informó a la PJCIS en agosto de 2020 que habían utilizado las facultades para solicitar asistencia al sector al menos de veinte veces (véase https://www.asio.gov.au/publications/speeches-and-statements/director-general-opening-statement-pjcis-august-2020.html). En el discurso no queda claro si se trata de una referencia aproximada a las notificaciones TAR emitidas por los organismos específicos señalados anteriormente o si estas "veinte" notificaciones se suman a las señaladas en otros informes.En cualquier caso, tanto si la cifra es 18 como si es 50 (y ningún dato sugiere que sea mayor), el uso gubernamental de la ley TOLA ha sido bastante limitado hasta ahora.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

sobre el uso de la ley TOLA hacen que sea difícil ejercer una supervisión eficaz y complican los esfuerzos por evaluar el impacto económico de esta ley.[33]

Otra disposición importante de la ley TOLA es la garantía de los "refugios seguros", que protegen a los destinatarios de las notificaciones de la ley TOLA de la responsabilidad asociada a su cumplimiento. En el régimen anterior, no siempre estaba claro cuándo la cooperación del sector a la hora de proporcionar acceso a los datos digitales podía hacer que la parte cooperante fuera responsable de violar otras protecciones legales de seguridad o privacidad. Además, la ley TOLA prevé el reembolso de los costos derivados del cumplimiento de las notificaciones emitidas en su marco. Juntos, los refugios seguros y las disposiciones relativas al reembolso de los costos tienen el efecto de aumentar los incentivos para que los destinatarios cumplan con las notificaciones de la ley TOLA.

Como explicamos en los capítulos siguientes, el aumento de la probabilidad de que los destinatarios (desconocidos) de las notificaciones de la ley TOLA puedan llevar a cabo actividades (desconocidas) que puedan dar lugar a la elusión del cifrado aumenta la posible amplitud de los impactos económicos de esta ley y el riesgo (percibido) de que ella debilite la seguridad digital.

3.2. Historia de la ley TOLA

La motivación para aprobar la ley TOLA proviene de la creciente preocupación que hay en Australia y en todo el mundo de que el aumento del uso del cifrado supone una amenaza para la capacidad de los organismos LEIA de acceder a los datos digitales en el transcurso de su labor destinada a hacer cumplir la ley y a promover la seguridad. Desde finales de 2017, el Gobierno australiano se movió con relativa rapidez para introducir la ley TOLA y proporcionar a los organismos LEIA capacidades ampliadas para eliminar o eludir el cifrado.[34]

En julio de 2017, el Gobierno señaló su intención de abordar la cuestión.[35] En agosto de 2018, Australia se reunió con las otras naciones de la alianza Five Eyes, [36] y se

[33]Algunas limitaciones que se aplican a la divulgación de la actividad relacionada con las notificaciones de la ley TOLA pueden justificarse como necesarias para proteger la eficacia de las acciones de los organismos LEIA.

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

[35]Malcom Turnbull, 'Press Conference with Attorney-General and Acting Commissioner of the AFP — Sydney — 14 July 2017' (conferencia de prensa, 14 de julio de 2017, https://www.malcolmturnbull.com.au/media/press-conference-with-attorney-general-and-acting-commissioner-of-the-afp-s).

[36]La alianza Five Eyes es una alianza de intercambio de inteligencia establecida en virtud del Acuerdo UKUSA entre Canadá, Nueva Zelanda, el Reino Unido, los Estados Unidos de América y Australia. La alianza está diseñada para facilitar el intercambio oportuno y gratuito de información de inteligencia y seguridad nacional.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

alcanzó una postura conjunta.[37] El proyecto de la ley TOLA se publicó el 14 de agosto de 2018.[38] El Departamento de Asuntos Internos (DHA, que era el principal organismo gubernamental responsable de la ley TOLA) recibió más de 340 escritos. El proyecto de ley con las modificaciones propuestas se presentó en la Cámara de Representantes el 20 de septiembre de 2018 y se remitió a la Comisión Parlamentaria Mixta de Inteligencia y Seguridad (PJCIS) para su examen. A principios de diciembre de 2018 se publicó un informe. La PJCIS celebró audiencias públicas entre el 19 de octubre y el 30 de noviembre de 2018, y también invitó a que se presentaran más escritos. La PJCIS recibió 105 escritos en total (incluyendo los confidenciales y los retenidos) durante su examen. Hubo 11 escritos de apoyo presentados por organismos gubernamentales, la Policía o las comisiones relacionadas con los delitos. Hubo muchos más escritos de oposición de los representantes del sector de la tecnología de la información de Australia.

A la luz del número de escritos en que se expresaba preocupación por el impacto que tendría sobre las empresas cumplir con las medidas de asistencia del sector, en particular las pequeñas empresas, la PJCIS preguntó al Departamento de Asuntos Internos si el Gobierno había formulado una declaración sobre el impacto normativo del proyecto de ley. En respuesta, dicho Departamento respondió que el Gobierno había formulado una declaración en forma breve en que se concluía que el impacto normativo de las medidas de asistencia del sector sería mínimo.[39]

El 22 de noviembre de 2018, el Ministro de Asuntos Internos indicó a la PJCIS que había una amenaza inmediata y una necesidad de proporcionar a los organismos facultades adicionales y de aprobar el proyecto de ley en la última semana de sesiones de 2018. Aunque en la PJCIS no se llegó a un acuerdo total sobre todos los aspectos del proyecto de la ley TOLA, la Comisión presentó un Informe Consultivo el 5 de diciembre de 2018[40] en que se concluía que:

> "... había una necesidad genuina e inmediata de que los organismos contaran con herramientas para responder al desafío de las comunicaciones cifradas. Se decía que la ausencia de estas herramientas daba como resultado una escalada de riesgo y había obstaculizado las investigaciones de los organismos durante varios años. Y se mencionaba que, en respuesta a esta escalada de riesgos, la

[37]"Statement of Principles on Access to Evidence and Encryption", Departamento del Fiscal General, agosto de 2018, disponible en https://www.ag.gov.au/sites/default/files/2020-03/joint-statement-principles-access-evidence.pdf.

[38]La formulación de la ley TOLA se inspiró en gran medida en la Ley de Facultades de Investigación del Reino Unido, aprobada en 2016 (véase "Investigatory Powers Act 2016", Reino Unido, disponible en https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted).

[39]Véase la página 13 de la revisión de la ley TOLA por parte del Departamento de Asuntos Internos, nota 3 *supra*.

[40]PJCIS (2018), "Advisory Report on the Telecommunications and Other Legislation (Assistance and Access) Bill 2018", Parliamentary Joint Committee on Intelligence and Security (PJCIS), diciembre de 2018, disponible en https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

> Comisión recomendaba que el Parlamento estudiara de forma urgente el proyecto de ley y lo aprobara de inmediato."[41]

A pesar de los numerosos escritos e informes de las comisiones relacionados con las modificaciones propuestas, la PJCIS solo hizo recomendaciones modestas. El proyecto de ley se modificó para aclarar determinadas definiciones y se introdujeron disposiciones en las que se establecía que un proveedor de servicios fuera consultado y se obtuviera asesoramiento sobre el cumplimiento de las órdenes obligatorias de creación de capacidad para ayudar a los organismos LEIA.[42] También se modificaron las disposiciones relativas a las solicitudes y órdenes de ayuda para garantizar que no pudieran utilizarse a fin de eludir los procesos existentes en los que ya se requería una orden judicial. No obstante, seguía habiendo algunas preocupaciones.[43] El Comité Parlamentario Permanente para el Escrutinio de los Proyectos de Ley también examinó el proyecto.[44] Aunque el análisis completo de las conclusiones del Comité Permanente está más allá del alcance de este informe, cabe mencionar que el Comité planteó preocupaciones adicionales con respecto a la naturaleza potencialmente inconstitucional de excluir el examen judicial de las notificaciones de la ley TOLA que se establece en la Ley de Decisiones Administrativas (Examen Judicial) de 1977 *(Administrative Decisions (Judicial Review) Act 1977),*[45] la difuminación de la doctrina de la separación de poderes,[46] así como la incompatibilidad con los lineamientos sobre las políticas del propio Fiscal General.[47]

---

[41]Biddington, M. (2019), "Telecommunications and Other Legislation Amendment (Miscellaneous Amendments) Bill 2019 – Law and Bills Digest Section", 27 de marzo de 2019, disponible en https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6581692/upload_binary/6581692.pdf.

[42]Véanse las páginas 5 a 7 del informe de la PJCIS (2018), nota 12 *supra*.

[43]Por ejemplo, en cuanto a las definiciones de vulnerabilidad y debilidad sistémica, tecnología objetivo, imposición de objetivos pertinentes para la emisión de notificaciones de la Parte 15, así como en cuanto al proceso para que las agencias de interceptación estatales y territoriales soliciten dichas notificaciones al comisionado de la Policía Federal Australiana (AFP).

[44]Parliamentary Standing Committee for the Scrutiny of Bills, Parliament of Australia, Scrutiny Digest (Digest n.º 14 de 2018, 28 de noviembre de 2018) 23–82, disponible en https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Scrutiny_Digest/2018, en adelante Scrutiny Digest 2018.

[45]Véase Scrutiny Digest 2018, nota 25 supra, página 42.La Ley de Decisiones Administrativas (Examen Judicial) de 1977 (Cth) (ADJR) está disponible en https://www.legislation.gov.au/Details/C2021C00035/Download.

[46]Dado que se establece que los funcionarios de la rama administrativa del Gobierno podrían ofrecer inmunidad civil a los proveedores de comunicaciones designados para que cumplan con las notificaciones de la ley TOLA (véase Scrutiny Digest 2018, la nota 25 supra, pages 47, 81).

[47]Véase Scrutiny Digest 2018, nota 25 supra, página 47.Véase "A Guide to Framing Commonwealth Offences Infringement Notices and Enforcement Powers", Departamento del Fiscal General, septiembre de 2011, disponible en https://www.ag.gov.au/sites/default/files/2020-03/A%20Guide%20to%20Framing%20Cth%20Offences.pdf.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

El proyecto de ley fue aprobado por ambas Cámaras el 6 de diciembre de 2018 y dos días después obtuvo la Sanción Real para formar parte de la legislación australiana. Desde la publicación del proyecto de ley hasta la promulgación transcurrieron menos de cuatro meses: algunos han dicho que este proceso fue precipitado y que el proceso de consulta asociado fue limitado.[48]

La PJCIS solicitó que el Monitor Independiente de la Legislación sobre Seguridad Nacional (INSLM) comenzara un examen de la ley TOLA el 26 de marzo de 2019.Este examen del INSLM se encargó justo antes de que la PJCIS terminara su propio segundo informe sobre la TOLA el 3 de abril de 2019 en que se recomendaba lo siguiente: i) que se pusieran a disposición del INLSM recursos suficientes para que llevara a cabo el examen; ii) que la PJCIS elaborara un tercer informe antes de junio de 2020; y iii) que el Inspector General de Inteligencia y Seguridad y el Defensor del Pueblo del Commonwealth tuvieran recursos suficientes para poder cumplir debidamente con las responsabilidades adicionales que les asignaba la ley TOLA.[49]

El INSLM presentó su informe al PJCIS el 30 de junio de 2020, y en él se formulaban una serie de recomendaciones para modificar la ley TOLA.[50] El INSLM recomendó que no se le otorgara a los jefes de los organismos y al Gobierno la facultad de emitir y autorizar las notificaciones de la ley TOLA, y que dicha facultad se le otorgara a un nuevo órgano de supervisión judicial. En el informe del INSLM también se pedía una nueva definición de" debilidad sistémica" y que se eliminara por completo la "vulnerabilidad sistémica" del proyecto de ley.[51] En un principio, el informe del INSLM debía servir de base para un tercer informe de la PJCIS, cuya entrega al Gobierno estaba prevista para junio de 2020. El plazo para que la PJCIS presentara el tercer informe se aplazó hasta septiembre de 2020, pero en marzo de 2021 todavía no

[48]Véase Hardy, K. (2020), "Australia's encryption laws: practical need or political strategy?",Internet Policy Review, 9(3), disponible en: https://policyreview.info/articles/analysis/australias-encryption-laws-practical-need-or-political-strategy; o Miley, V. (2019), "Hastily written tech laws threaten online privacy and security", GreenLeft, disponible en https://www.greenleft.org.au/content/hastily-written-tech-laws-threaten-online-privacy-and-security.

[49]PJCIS (2019), "Review of the Telecommunications and Other Legislative Amendment (Assistance and Access) Act of 2018", Parliamentary Joint Committee on Intelligence and Security (PJCIS), abril de 2019, disponible en https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct/Report.

[50]INSLM (2020a), "Trust but Verify: A report concerning the Telecommunications and Other Legislation (Assistance and Access) Act 2018 and related matters", Australian Independent National Security Legislation Monitor (INSLM), julio de 9, 2020, disponible en https://www.inslm.gov.au/reviews-reports/telecommunications-and-other-legislation-amendment-act-2018-related-matters; y véase INSLM (2020b), "Trust but Verify: Summary of Recommendations", disponible en https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Additional_Documents.

[51]Véanse las recomendaciones 3, 9 y10 del INSLM (2020a), nota 42 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

lo había hecho.

Así, dos años después de la aprobación de la ley TOLA, esta sigue siendo controvertida. Parte de la controversia puede deberse al hecho de que esta ley se redactó y se aprobó de forma precipitada, sin una evaluación adecuada del impacto potencial o esperado que podría tener. Durante el primer examen que la PJCIS hizo sobre la ley TOLA antes de su promulgación en diciembre de 2018, se preguntó al Departamento de Asuntos Internos si el Gobierno había preparado una declaración de impacto normativo (RIS)[52] para evaluar el probable efecto económico en las empresas y la competitividad global. Dicho Departamento respondió por escrito que el Gobierno solo había preparado una declaración de impacto normativo en *forma breve*[53] en que se concluía que el impacto normativo de las medidas de asistencia del sector *sería mínimo*[54].

No hemos podido encontrar ninguna prueba sustantiva de que el impacto económico potencial de la ley TOLA haya sido considerado en detalle. No sabemos de ningún intento serio de cuantificar o incluso de caracterizar con algún nivel de detalle cómo la ley TOLA podría ofrecer beneficios en los hechos (por ejemplo, mediante la mejora de la seguridad nacional o la aplicación de la ley)[55] ni los posibles daños económicos que

[52]Según la Guía sobre Normativa del Gobierno Australiano de 2014 (la Guía), que se aplicaba en el momento de la introducción y aprobación de la ley TOLA, *toda propuesta de política destinada a introducir o abolir una norma debía ir acompañada de una declaración de impacto normativo (RIS) del Gobierno australiano, y dicha declaración se debía formular en las primeras etapas del proceso de elaboración de la política* (véase la página 4, 2014 The Australian Government Guide to Regulation, disponible en https://apo.org.au/sites/default/files/resource-files/2014-03/apo-nid270966.pdf.

[53]El primer paso en la formulación de una RIS en 2018 fue que el organismo responsable entregara un resumen escrito conocido como evaluación preliminar a la Oficina de Regulación de Mejores Prácticas (OBPR) del primer ministro. Si en la RIS se proporcionaba suficiente información como para que la OBPR entendiera la naturaleza de los asuntos políticos en cuestión, la OBPR debía dar una respuesta en un plazo de 5 días hábiles para confirmar si era necesario o no formular una RIS y, en caso afirmativo, de qué tipo. Había tres tipos de RIS: forma larga, forma estándar y forma breve. En todos los casos, el organismo debía hacer un cálculo de los costos de la norma (incluidas las compensaciones), independientemente del tipo de RIS por el que se optara (véase la Guía, nota 33 *supra*, página 11).

[54]Página 13, "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", Departamento de Asuntos Internos de Australia, noviembre de 2018, disponible en https://www.aph.gov.au/DocumentStore.ashx?id=13d6d87f-a64e-4e7c-8cc1-83d939e9fe1d&subId=660956 (en adelante, revisión de la ley TOLA por parte del Departamento de Asuntos Internos).

[55]Decir simplemente que hay delitos (terrorismo, tráfico de personas, etc.) que son atroces y suponen una grave amenaza para la seguridad nacional, aunque por supuesto es cierto, no es suficiente para demostrar una evaluación del impacto del modo en que la ley TOLA abordará en los hechos estos y otros tipos de delitos en relación con los cuales dicha ley se puede utilizar.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

esta ley podría provocar si dañara las perspectivas económicas de las empresas australianas o amenazara la confianza digital.[56]

En los capítulos siguientes explicamos por qué el cifrado es fundamental para promover la seguridad digital y, dada la importancia de la información digital para la economía australiana y mundial, cómo una amenaza al cifrado supone un riesgo de que se produzcan daños económicos considerables. Exploramos los distintos mecanismos por los que la ley TOLA puede amenazar la confianza digital y perjudicar a la economía australiana.

4. Consideraciones tecnológicas

A LECA se le ha encargado la tarea de probar la hipótesis de que los intentos legislativos y otros intentos legales de socavar el cifrado tendrán un impacto negativo en aspectos económicos como los negocios, la innovación, el comercio y la inversión interna. Si bien este informe es un análisis económico, socavar el cifrado (o, como se señala en la ley TOLA, "eliminar el cifrado") implica a la tecnología. Con ese fin, en esta sección del documento se examinan las consecuencias técnicas de la eliminación o la elusión del cifrado y se proporciona un marco sobre cómo las consideraciones tecnológicas impactan en las cuestiones económicas. El objetivo aquí no es proporcionar un análisis técnico profundo, sino simplemente describir el contexto del análisis económico.

Está ampliamente reconocido que un cifrado fuerte es esencial para algunos aspectos fundamentales de nuestra sociedad, como el comercio, la libertad, la libertad de expresión y la seguridad nacional.[57] Un cifrado fuerte podría permitir a los delincuentes comunicarse sin ser observados o interpretados, y los organismos LEIA afirman que dicho cifrado obstaculiza su capacidad para cumplir su misión. Los organismos LEIA han procurado que se aprueben leyes que obliguen a los proveedores DCP que ofrecen productos y servicios cifrados a ayudar a proporcionar acceso no cifrado a determinadas comunicaciones sobre la base de una orden judicial o una notificación legal. Este tipo de acceso legal por parte de terceros suele denominarse *acceso excepcional*[58] a contenido cifrado.

Entre los expertos técnicos hay un fuerte consenso en cuanto a que este tipo de intervenciones, incluso las más selectivas, aumentan el riesgo y tienen el efecto adverso

[56]El 1 de octubre de 2020 se presentó ante el Departamento de Asuntos Internos una solicitud de libertad de información para obtener una copia de la declaración RIS de forma breve. El 1 de marzo de 2021, dicho Departamento comunicó que la RIS era un documento exento y que no se divulgaría.

[57]Internet Society-Chatham House Roundtable on Encryption and Lawful Access, octubre de 2017 https://www.internetsociety.org/resources/doc/2018/internet-society-chatham-house-roundtable-on-encryption-and-lawful-access/

[58]Los requisitos de acceso excepcional se refieren a algún medio que otorgue a las fuerzas del orden la capacidad de acceder legalmente al contenido de las comunicaciones y los datos cifrados de forma no cifrada.
Véase https://www.internetsociety.org/resources/doc/2018/encryption-brief/

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

de erosionar la confianza en los servicios cifrados.[59] En un análisis de los métodos de acceso excepcional que se están debatiendo en la Unión Europea, los principales expertos en ciberseguridad señalaron que cada método de acceso excepcional introduciría vulnerabilidades que un tercero (por ejemplo, un actor malintencionado) podría aprovechar para afectar a todos los usuarios.[60] La simple posibilidad de que haya un acceso excepcional podría debilitar la confianza y el uso del cifrado y de los servicios que dependen de él, como el comercio electrónico o las finanzas electrónicas.

A continuación exploraremos las preocupaciones específicas asociadas con permitir el acceso a los datos cifrados del modo en que se propone en la ley TOLA.[61] En primer lugar, abordaremos las siguientes preguntas en términos generales:

- ¿Qué es el cifrado, cómo se utiliza y cuál es su valor?
- ¿Cómo podría facilitarse el acceso a los datos cifrados y cómo se define esto en la ley TOLA?
- ¿Cuáles son las posibles consecuencias técnicas de la ley TOLA?

Para resumir esta sección, describiremos los desafíos que supone crear una intervención selectiva en un servicio de cifrado, e indicaremos cómo ese tipo de intervenciones podrían utilizarse de forma malintencionada más allá del objetivo, a pesar de las mejores intenciones que los organismos LEIA o los proveedores DCP puedan tener. Consideramos que la vaguedad del lenguaje y la amplitud de los requisitos y obligaciones que se establecen en la ley TOLA agravan la preocupación que genera la capacidad de crear una intervención selectiva. Aunque es difícil cuantificar el impacto asociado a cualquier esfuerzo destinado a eliminar o socavar el cifrado, sí observamos un aumento del riesgo y la posibilidad de que disminuya la confianza en estos sistemas cifrados. La ley TOLA podría socavar y erosionar la confianza del público en los numerosos servicios cifrados que todos utilizamos a diario. La sola percepción de que el cifrado es más débil o la amenaza de que los organismos gubernamentales tengan la capacidad de recopilar información socava la confianza.

4.1. ¿Qué es el cifrado?

Hay muchas definiciones de cifrado, pero una sencilla y bastante completa es la siguiente: "cualquier procedimiento utilizado en criptografía para convertir texto no cifrado en texto cifrado con el fin de impedir que alguna persona, salvo el destinatario

[59]Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, https://www.csail.mit.edu/research/keys-under-doormats; y National Academy of Sciences.'Decrypting the Encryption Debate: A Framework for Decision Makers' (2018), https://www.nap.edu/read/25010.

[60]https://www.globalencryption.org/2020/11/breaking-encryption-myths/

[61]Estas conclusiones se han extraído del análisis de la propuesta de ley, de una revisión de la prensa especializada y de las publicaciones académicas, de los comentarios presentados como parte del expediente público, así como de entrevistas con varios proveedores de comunicaciones que ofrecen servicios cifrados.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

previsto, pueda leer esos datos".[62] Por supuesto, en el contexto del tema que nos ocupa, "texto" puede significar cualquier tipo de comunicación, como voz, imágenes, caracteres, video, chat, sitios web, etc.[63] La intención del cifrado es proporcionar un medio para evitar que otros que puedan interceptar una comunicación cifrada entiendan su contenido. Se emplea un algoritmo de cifrado para tomar el texto no cifrado en combinación con una "clave" y generar un texto cifrado. Los algoritmos de descifrado que se emplean tras la recepción invierten este proceso a fin de reproducir el texto no cifrado, lo que significa que el destinatario de un mensaje cifrado debe tener la clave para leer ese mensaje. Podemos pensar en el cifrado como un sistema que consta de muchos elementos que funcionan juntos a través de Internet. El cifrado no son solo los elementos matemáticos instanciados en el software, sino también un amplio conjunto de algoritmos y funciones esenciales, como el intercambio seguro de claves. Se supone que nadie más que el remitente y el destinatario deben tener las claves.[64]

El secreto que ofrece el cifrado es tan fuerte como su implementación. Un cifrado fuerte podría considerarse como la caja fuerte de un banco: en ambos casos acceder a lo que hay dentro es impracticable, ya que se necesitaría demasiado tiempo, dinero, recursos y/o conocimientos para romper el cifrado, al igual que para abrir la caja fuerte. Si el algoritmo de cifrado es débil, entonces un interceptor podría recuperar el texto no cifrado con bastante facilidad. Un algoritmo débil es como la cerradura poco sofisticada de una bóveda, pero poner una cerradura fuerte en esta última es inútil si la puerta se puede quitar cortando las bisagras. Todas las partes del sistema de cifrado deben contribuir a su fortaleza. Con un cifrado cada vez más fuerte, se hace muy difícil, casi imposible, romper el cifrado. También es crucial garantizar que las claves privadas solo se distribuyan a sus destinatarios, y no a terceros que podrían utilizarlas para acceder a los datos cifrados. Para llevar la analogía más lejos, incluso la más fuerte de las bóvedas se abrirá si se consigue acceder a las llaves.

También cabe mencionar que el cifrado puede aplicarse en diversos puntos de la red y por parte de diversas entidades. De hecho, hoy en día es de poco valor para los usuarios implementar sus propios servicios cifrados fuertes de extremo a extremo sin hacer uso de un servicio comercial. Como veremos, esto tiene consecuencias para los organismos LEIA.

---

[62]NIST SP 800-101 Rev. 1, https://doi.org/10.6028/NIST.SP.800-101r1, en Encryption (Cifrado), consultado en noviembre de 2020

[63]También pueden surgir preocupaciones de seguridad y privacidad relacionadas con los metadatos de las comunicaciones seguras, aunque este contenido no esté protegido mediante cifrado. Esto incluye información sobre el origen y el destino de las comunicaciones, las aplicaciones utilizadas, la hora en que se produjeron las comunicaciones, etc. La protección de los metadatos plantea muchas de las mismas preocupaciones que la protección del contenido de las comunicaciones, por lo que esta información está legalmente protegida y se requiere una orden judicial para que los organismos gubernamentales puedan obtener su contenido.

[64]La información sobre el intercambio de claves, la criptografía simétrica y asimétrica, y otras cuestiones relacionadas, si bien es importante, está fuera del alcance de este informe. Para consultar un análisis más detallado del tema del cifrado, véase < 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, Reino Unido +44 7554 065 718

4.2. ¿Cómo se utiliza el cifrado y cuál es su valor?

El cifrado tiene una gran variedad de aplicaciones. En primer lugar, se utiliza para proteger (es decir, mantener la confidencialidad y evitar la manipulación de) los datos almacenados ("datos en reposo") o los que se transmiten ("datos en movimiento"); por supuesto, los usuarios quieren que sus datos estén protegidos tanto cuando se están transmitiendo como cuando se encuentran en reposo. El cifrado se usa de diversas maneras, por ejemplo: para proteger las transacciones financieras y los registros sanitarios, para almacenar archivos de forma segura, para cifrar discos, para bloquear dispositivos, para verificar credenciales que permiten acceder a redes privadas virtuales, para navegar con seguridad por Internet, para enviar mensajes privados o anónimos, para promover la seguridad en la nube, etc. [65] Al proporcionar estas protecciones, el cifrado desempeña un papel importante para hacer posible algunos aspectos cruciales de nuestra economía, al garantizar la confianza en el comercio electrónico, las finanzas electrónicas, la salud electrónica, la capacitación en línea, el almacenamiento seguro de información y las comunicaciones privadas seguras, y al garantizar nuestras libertades civiles, como la privacidad, la libertad de expresión y la libertad de asociación.

Aunque en algunos estudios (como en los que se describen en la sección de economía de este documento) se ha intentado asignar un valor monetario al cifrado, esta es una tarea difícil dada la forma en que el cifrado está entretejido en nuestra existencia moderna, las innumerables formas en que dependemos de él en nuestra vida diaria, y los innumerables efectos de segundo y tercer orden que el cifrado tiene en nuestras vidas hoy en día.[66] Como se ha descrito anteriormente, el cifrado proporciona la base misma de la confianza en Internet, y es esta confianza la que ha permitido el tremendo crecimiento de las comunicaciones, el comercio, las finanzas y los servicios sanitarios en toda la red y en todo el mundo. Durante la pandemia de COVID-19, el cifrado ha brindado a muchas empresas la flexibilidad para trabajar desde casa, y ello ha permitido que el comercio continúe a pesar de las restricciones y las realidades prácticas de una pandemia.

El valor del cifrado radica en que brinda seguridad a estos servicios y proporciona una base de confianza. Sin un cifrado fuerte, esta confianza no existe, y esa falta de confianza perjudica a los servicios mencionados. La confianza que se obtiene a través del cifrado es la base de todas estas actividades que se llevan a cabo en Internet, y sin

[65]National Academy of Sciences.'Decrypting the Encryption Debate: A Framework for Decision Makers' (2018), https://www.nap.edu/read/25010.

[66]Véase el análisis en la sección económica de este documento. Las estimaciones de inversión en ciberseguridad se sitúan en cientos de miles de millones de dólares estadounidenses.Véase Leech, D. y John Scott (2018), "The Economic Impacts of the Advanced Encryption Standard, 1996-2017", elaborado para el Instituto Nacional de Normas y Tecnología, NIST GCR 18-017, disponible en https://doi.org/10.6028/NIST.GCR.18-017; publicado como artículo de revista: Leech, D. P., Ferris, S., y Scott, J. T. (2019).The Economic Impacts of the Advanced Encryption Standard, 1996–2017.Annals of Science and Technology Policy, 3(2), 142-257.doi:10.1561/110.00000.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

ella, las personas y las entidades pueden no estar dispuestas a participar en estas actividades en línea. De hecho, a medida que nuestra sociedad sigue avanzando hacia una economía de la información y los datos, se necesita más cifrado, no menos, y socavar su fortaleza nos lleva en la dirección equivocada.

Como ha señalado Apple, "Cada día se realizan más de un billón de transacciones seguras en Internet gracias a las comunicaciones cifradas".[67] En general se acepta como un hecho que la mejor manera de fomentar la ciberseguridad es promover una mayor adopción de un cifrado digital fuerte de extremo a extremo.[68]

---

[67]Página 1, "Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 Submission 53", Apple, Inc., disponible en https://www.aph.gov.au/DocumentStore.ashx?id=ecd6be12-ab84-43de-be61-1599e1db2a74&subId=661073.

[68]Existen numerosas declaraciones autorizadas formuladas por los responsables de elaborar las políticas de países de todo el mundo sobre el valor de la ciberseguridad.Por ejemplo:

- El fiscal general William Barr reconoció implícitamente que no había forma de proporcionar al Gobierno acceso a los datos cifrados sin crear vulnerabilidades que los actores malintencionados pudieran explotar, al argumentar que el riesgo era aceptable porque se estaba hablando de productos y servicios de consumo, como la mensajería, los teléfonos inteligentes, el correo electrónico y las aplicaciones de voz y datos, no de proteger los códigos de lanzamiento nuclear del país (véase "US Attorney general William Barr says Americans should accept security risks of encryption backdoors", TechCrunch, 23 de julio de 2019, disponible en https://techcrunch.com/2019/07/23/william-barr-consumers-security-risks-backdoors/?guccounter=1).
- Ash Carter, el antiguo secretario de Defensa de los Estados Unidos, argumentó que no tenía sentido comprar una cantidad de aviones, barcos y tanques, ni tener soldados, marineros, aviadores e infantes de marina, si no era posible conectarlos. Dijo que por ese motivo la seguridad de los datos era una necesidad absoluta para ellos, y que por eso estaban totalmente a favor de que la seguridad de los datos fuera fuerte, lo que incluía un cifrado sólido, sin duda alguna (véase la transcripción titulada "Remarks of Secretary Carter in a 'Fireside' Chat with Ted Schlein in San Francisco", Departamento de Defensa de los Estados Unidos, 2 de marzo de 2016, disponible en https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/684858/remarks-by-secretary-carter-in-a-fireside-chat-with-ted-schlein-in-san-francisc/.
- Robert Hannigan, exdirector del Cuartel General de Comunicaciones del Gobierno (GCHQ) del **Reino Unido** dijo que el cifrado era algo abrumadoramente bueno que nos mantenía a todos a salvo y seguros. Señaló que la creación de puertas traseras era una amenaza para todos y que no era una buena idea debilitar la seguridad de todos para hacer frente a una minoría" (véase "UK's ex-spy chief warns Amber Rudd's plan to pass new smartphone encryption law is dangerous", The Independent, 10 de julio de 2017, disponible en 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;
- En 2019, el Comité Permanente de Seguridad Pública y Seguridad Nacional de la Cámara de los Comunes de Canadá elaboró un informe sobre la ciberseguridad en el sector financiero como cuestión de seguridad nacional y en él concluyó que era

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

4.3. ¿Cómo puede facilitarse el acceso excepcional?

Las mismas características del cifrado que lo convierten en una parte fundamental de Internet pueden ser utilizadas por los delincuentes para ocultar actividades ilegales en un amplio conjunto de tecnologías y aplicaciones. Esto obstaculiza la capacidad de los organismos LEIA para interceptar y ver con facilidad el contenido de las comunicaciones de quienes son objeto de una investigación. Con el acceso excepcional se procura proporcionar una forma de que los organismos LEIA puedan acceder al contenido de las comunicaciones cifradas como si fuera texto no cifrado.

En términos generales, podríamos decir que el acceso excepcional consiste en:

- eliminar el cifrado o la autenticación;
- introducir debilidades o vulnerabilidades,
- o introducir hardware o software para proporcionar acceso a contenido descifrado.

Para hacer esto se podrían utilizar métodos como la custodia de claves, la alteración de la gestión de las claves, la introducción de una debilidad o vulnerabilidad en la criptografía, los métodos, los protocolos o las implementaciones de un servicio de cifrado, o simplemente mediante la desactivación del cifrado.[69]

En Australia, la ley TOLA permite a los organismos LEIA imponer obligaciones legales a los proveedores DCP y exigirles que ayuden a que dichos organismos

---

importante, por razones de seguridad y privacidad, que todos los canadienses tuvieran acceso a un cifrado fuerte, y recomendó que el Gobierno de Canadá rechazara las estrategias de otorgar acceso legal que debilitaran la ciberseguridad (véase "Cybersecurity in the Financial Sector as a National Security Issue," Canadian House of Commons, junio de 2019, disponible en https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP10589448/securp38/securp38-e.pdf).

- Según la Comisión Europea, el cifrado fuerte es la base de los sistemas seguros de identificación digital que desempeñan un papel clave en la ciberseguridad eficaz; también permite preservar la seguridad de la propiedad intelectual de las personas y proteger derechos fundamentales como la libertad de expresión y la protección de los datos personales, y garantiza que el comercio en línea sea seguro (véanse las páginas 9-10 en "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", Comisión Europea, Bruselas, 13 de septiembre de 2017, disponible en https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF).

[69]Los medios técnicos para facilitar el acceso al contenido cifrado podrían incluir una amplia gama de estrategias (algunas de las cuales exceden el alcance de la ley TOLA), como las siguientes: aprovechar las vulnerabilidades descubiertas; introducir vulnerabilidades; llevar a cabo ataques más amplios con herramientas como *keyloggers* o herramientas de *snooping*; eliminar los controles de seguridad de un sistema, software o dispositivo específico; deshabilitar o bajar de categoría los servicios de cifrado; interrumpir las sesiones de cifrado entre el navegador y el servidor; intercambiar claves; implementar la custodia de claves, u otras estrategias posibles. Una vez más, un análisis más extenso está fuera del alcance de este documento.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

obtengan acceso a los servicios cifrados y a sus datos. Lo que esa ley no dice es cómo se puede proporcionar ese acceso. No trataremos de hacer un análisis exhaustivo de los métodos técnicos que permiten proporcionar acceso a los datos cifrados (eso está fuera del alcance de este informe); en lugar de eso nos limitaremos a considerar y examinar las consecuencias técnicas generales de la ley TOLA.[70]

Un tipo de acceso para terceros autorizados (es decir, organismos LEIA) es la custodia de claves, que consiste en que un tercero "de confianza" mantiene "en custodia" un conjunto adicional de claves de descifrado que puede proporcionar a las LEIA cuando corresponda por ley. Sin embargo, debido a las preocupaciones sobre quién podría tener acceso a estas claves (por ejemplo, pueden ser robadas, mal manejadas, perdidas o divulgadas) y debido a que los métodos de custodia de claves no requieren de la ley TOLA, no examinaremos más este método en el presente informe, aparte de señalar que la comunidad técnica se ha opuesto y sigue oponiéndose a él.[71]

Otra forma de implementar dicho acceso es incorporar una debilidad o vulnerabilidad de [72] "puerta trasera" en un mecanismo de cifrado subyacente o en el software relacionado. El problema aquí es que, por diseño, este proceso introduce una debilidad o vulnerabilidad, y la consecuencia de tal manipulación socava el cifrado. Incorporar debilidades también es simplemente contrario a la norma que se aplica de forma estricta y que consiste en construir y evaluar un cifrado fuerte, así como al proceso de descubrir, notificar y resolver esas debilidades. No sólo debilita la aplicación real del cifrado, sino

[70]Australia ya cuenta con leyes que permiten el acceso legal a los datos, lo que proporcionaría a los LEIA una vía legal para obtener datos cifrados de un amplio número de proveedores de servicios.Como se ha señalado en el capítulo legal, la ley TOLA parece ampliar la legislación existente en la medida en que menciona explícitamente la eliminación del cifrado y extiende esta facultad a los DCP que no son operadores de telecomunicaciones, proveedores de servicios de telecomunicaciones y operadores de instalaciones y redes de telecomunicaciones, así como a los servicios que no son estrictamente de telecomunicaciones, muchos de los cuales ya estaban (antes de la ley TOLA) sujetos a una amplia legislación de la Comunidad Nacional de Inteligencia. La legislación anterior incluye la *Ley de Telecomunicaciones (Interceptación y Acceso) de 1979* (TIA) y la posterior legislación pertinente que se aprobó luego de los ataques terroristas del 11 de septiembre de 2001. Desde entonces el Parlamento australiano ha aprobado más de 124 leyes que modifican el marco legislativo de la Comunidad Nacional de Inteligencia.

[71]Véase Abelson, H., R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. Neumann, R. Rivest, J. Schiller, B. Schneier, M. Specter y D. Weitzner (2015), “Keys under doormats: mandating insecurity by requiring government access to all data and communications”, Journal of Cybersecurity, 1(1), págs. 69 a 79. Para consultar la versión ampliada del documento de trabajo, véase Technical Report (MIT-CSAIL-TR-2015-026), 6 de julio de2015, disponible en https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

[72]Como se ha mencionado anteriormente, un método para obtener acceso alternativo al contenido de las comunicaciones cifradas se denomina "puerta trasera", y se llama así porque desempeña una función semejante a la de una puerta trasera que ofrece un acceso alternativo a un edificio. Por supuesto, la mayoría de nosotros no querría que en nuestra casa hubiera una puerta trasera que supusiera una debilidad conocida (seguridad debilitada), y la mayoría de nosotros no querría proporcionar las llaves de la puerta al Gobierno (custodia de llaves).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

que también erosiona la confianza en el concepto de cifrado como herramienta que sustenta gran parte de lo que hacemos como sociedad en línea.[73]

4.4. ¿Cómo se define ese acceso?

Como ya comentaremos, el texto actual de la ley TOLA deja una serie de preguntas y preocupaciones sobre su aplicación. Aunque no es raro que los aspectos del lenguaje legislativo sean intencionadamente amplios en su alcance y aplicación, el único mensaje claro que escuchamos de todas las empresas que entrevistamos es que simplemente no saben qué esperar. A continuación describiremos esa falta de claridad y consideraremos sus consecuencias.

Una de las primeras cosas que uno nota al leer la ley TOLA es que se dice más sobre lo que no se puede exigir en una notificación que sobre lo que sí se puede exigir. No es de extrañar que este planteo sea una forma de limitar el alcance de manera que la ley sea más aceptable y sea más difícil estar en desacuerdo con ella. Sin embargo, al leer este texto se hace difícil captar el significado y el lector común se queda con dudas sobre cuáles son las definiciones y obligaciones.

Por ejemplo, en la ley TOLA se establece que a un proveedor de comunicaciones designado no se le debe pedir ni exigir que implemente o construya una debilidad sistémica o una vulnerabilidad sistémica, etc. Además, se establece que las notificaciones no deben tener los siguientes efectos: a) solicitar o exigir a un proveedor de comunicaciones designado que implemente o construya una debilidad sistémica, o una vulnerabilidad sistémica, en una forma de protección electrónica, o b) impedir que un proveedor de comunicaciones designado rectifique una debilidad sistémica, o una vulnerabilidad sistémica, en una forma de protección electrónica. Luego se establece que en las notificaciones no se puede exigir a un proveedor que implemente o construya una nueva capacidad de descifrado, ni que haga que los métodos sistémicos de autenticación o cifrado sean menos eficaces, ni que introduzca una vulnerabilidad o debilidad "selectiva" que ponga en peligro la seguridad de la información que esté en poder de otra persona, ni que cree un riesgo sustancial de que un tercero no autorizado pueda acceder a una información que de otro modo sería segura.[74]

A la ley se le han añadido las siguientes definiciones:[75]

> *vulnerabilidad sistémica* significa una vulnerabilidad que afecta a toda una clase de tecnología, pero no incluye una vulnerabilidad que se introduce de forma selectiva en una o varias tecnologías objetivo que están relacionadas con una persona en particular. A estos efectos, es irrelevante que la persona pueda ser identificada.

[73]A modo de ejemplo, véase la puerta trasera de Juniper del generador de números aleatorios DUAL-EC-DRBG: https://dl.acm.org/doi/pdf/10.1145/2976749.2978395.

[74]Para consultar estas citas y las anteriores de este párrafo, véanse las páginas 84 y 85 de la ley TOLA, nota 2 supra.

[75]Página 12 de la ley TOLA, nota 2 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

> *debilidad sistémica* significa una debilidad que afecta a toda una clase de tecnología, pero no incluye una debilidad que se introduce de forma selectiva en una o varias tecnologías objetivo que están relacionadas con una persona en particular. A estos efectos, es irrelevante que la persona pueda ser identificada.

Aunque con estas definiciones se procura reducir el riesgo para los usuarios que no sean objeto de la notificación, sigue habiendo una falta de claridad, y hay implicaciones que sugieren posibles consecuencias. Un primer paso sería aclarar qué se entiende por tecnología objetivo. También sería útil entender cómo se haría para que las vulnerabilidades introducidas selectivamente en las tecnologías objetivo no se utilicen de forma más general a nivel sistémico, un punto que ha sido señalado por los expertos técnicos como un problema inherente a este enfoque.[76] El método que se adopte para implementar una vulnerabilidad selectiva (o posiblemente la implementación en sí) tiene una alta probabilidad de filtrarse o de ser descubierto y explotado por terceros. Si eso ocurre, el método podría aplicarse a uno o a muchos otros objetivos.

Si bien existen algunos métodos básicos para proporcionar acceso a cosas como las comunicaciones de voz móviles y ciertos dispositivos bloqueados, en muchos servicios de Internet actuales se hace uso de un cifrado fuerte de extremo a extremo, lo que podría limitar la capacidad del proveedor de servicios para ayudar a proporcionar un acceso excepcional (esto se reconoce en la ley TOLA).[77] Además, en la actualidad no tiene sentido implementar u obtener un servicio de comunicaciones fuerte de extremo a extremo sin la ayuda de un proveedor de servicios, por lo que el proveedor de servicios no tendría la capacidad de revelar el contenido si así lo solicitaran los organismos LEIA.

De hecho, es posible descargar e implementar software de código abierto solo para este tipo de funciones, lo que hace cada vez más difícil introducir una vulnerabilidad sin que sea detectada. Es posible que ningún proveedor (ni siquiera el creador del software de código abierto, suponiendo que la ley TOLA pueda aplicarse legalmente a ese proveedor) sea capaz de proporcionar a los organismos gubernamentales la información que buscan con ese acceso.[78] La cuestión es que no es posible en la práctica impedir que la gente utilice un cifrado fuerte de extremo a extremo si está motivada para hacerlo. No es realista esperar que se revierta la invención de algoritmos de cifrado o que estos no se publiquen, al igual que no es razonable esperar que se suprima el software de cifrado de código abierto.

---

[76]Véase https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ en EternalBlue.

[77]Las empresas que ofrecen servicios que terminan en un extremo del canal cifrado presentan un listón más bajo en cuanto a la interceptación de las comunicaciones.Tienen acceso al contenido no cifrado.En estos casos, responder a la solicitud de puerta trasera debería imponer unos costos directos mínimos.

[78]Por ejemplo, los actores malintencionados que saben que son el posible objetivo de las fuerzas del orden o de las agencias de inteligencia pueden ser más propensos a emplear capas adicionales de protección de seguridad que están ampliamente disponibles, lo que haría ineficaz el acceso que la ley TOLA hace posible.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

4.5. ¿Cuáles son las consecuencias de la ley TOLA?

En numerosos estudios técnicos, económicos y empresariales se han analizado los problemas que plantea conceder un acceso excepcional al cifrado.[79] Estos van desde la indicación de las formas en que el cifrado se debilitaría, hasta los problemas que surgen debido a la erosión de la confianza y las preocupaciones más amplias de que se fracture Internet. El acceso excepcional se ha encontrado repetidamente con una fuerte resistencia por parte de los expertos técnicos durante las últimas tres décadas, y los esfuerzos recientes que apoyan el acceso excepcional no han mostrado un camino que permita superar las preocupaciones técnicas; esto incluye el enfoque que se propone en la ley TOLA. En esta sección trataremos de ofrecer una perspectiva sobre los desafíos y las consecuencias del acceso excepcional y, más concretamente, sobre las dificultades que presenta la aplicación de la ley TOLA. En el resto de esta sección consideraremos cuestiones relacionadas con los siguientes temas: el debilitamiento del cifrado; la falta de claridad en cuanto a la selectividad; el diseño y la retención de métodos; la reutilización; la escalabilidad; la filtración y el intercambio, y la incertidumbre en lo que atañe a los procesos y las obligaciones.

Debilitamiento del cifrado

En la ley TOLA se establece que no se puede pedir a un proveedor de comunicaciones que construya o implemente una debilidad sistémica o una vulnerabilidad sistémica en una forma de protección electrónica, y que no se puede impedir que un proveedor de comunicaciones designado rectifique una debilidad sistémica o una vulnerabilidad sistémica en una forma de protección electrónica.[80] En este caso, los legisladores estaban tomando medidas para evitar que se crearan vulnerabilidades sistémicas. Sin embargo, no solicitar a un proveedor que construya o implemente una debilidad sistémica o una vulnerabilidad sistémica no le impide hacerlo.

En lugar de decir que no se impedirá al proveedor de comunicaciones designado rectificar una debilidad o vulnerabilidad, el texto debería decir que el proveedor de

[79]National Academy of Sciences (2018), "Decrypting the Encryption Debate: A Framework for Decision Makers", disponible en https://www.nap.edu/read/25010; Bellovin, S., M. Blaze, D. Boneh, S. Landau y R. Rivest (2018), "Analysis of the CLEAR Protocol per the National Academies Framework", CUCS-003-18, 10 de mayo de 2018, disponible en https://mice.cs.columbia.edu/getTechreport.php?techreportID=1637; Bellovin, S., M. Blaze, S. Clark y S. Landau (2014), "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet", Northwestern Journal of Technology and Intellectual Property, vol. 12, número 1; Abelson, H., R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. Neumann y R. Rivest (2015), "Keys under doormats: mandating insecurity by requiring government access to all data and communications", Journal of Cybersecurity, 1(1), págs. 69 a 79, disponible en https://academic.oup.com/cybersecurity/article-pdf/1/1/69/7002861/tyv009.pdf, y el informe técnico MIT-CSAIL-TR-2015-026 (6 de julio de 2015) disponible en https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf; Ali, M. (2016), "Backdoor Government Decryption Hurts My Business and Yours", Harvard Business Review, 15 de septiembre de 2016, disponible en https://hbr.org/2016/09/backdoor-government-decryption-hurts-my-business-and-yours.

[80]Página XX de la ley TOLA, nota 2 supra.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

comunicaciones designado está obligado a aplicar las mejores prácticas del sector con respecto a la pronta rectificación de las vulnerabilidades y debilidades conocidas.[81]

El riesgo es que la ley TOLA pueda crear incentivos para que las empresas preserven (es decir, no revelen) las vulnerabilidades conocidas. Hacer esto crea un mayor riesgo para el público en general; hay un interés público primordial en que las vulnerabilidades sean notificadas, corregidas y resueltas tan pronto como sea posible, especialmente para reducir el riesgo de que haya ataques del "día cero" y para disminuir el impacto de estos.

Del mismo modo, algunas técnicas como el escaneo del lado del cliente y la "propuesta fantasma" del Reino Unido suelen ser presentadas por sus defensores como si utilizaran las capacidades existentes, en lugar de introducir debilidades o vulnerabilidades nuevas.[82] Pero el hecho es que estas técnicas sí introducen nuevas vulnerabilidades. Por ejemplo, en la "propuesta fantasma" se proporciona un mecanismo para eludir de forma eficaz el proceso de cifrado permitiendo que un tercero se una a una sesión sin que los participantes previstos lo sepan. Dado que este mecanismo es algo que un proveedor DCP puede replicar en toda la base de usuarios, en los hechos se convierte en un proceso ampliamente aplicable.

Falta de claridad en cuanto a la selectividad
Si bien limitar la solicitud o la notificación a un objetivo específico para limitar la exposición es el enfoque correcto, sigue sin estar claro cómo se puede lograr la selectividad sin exponer potencialmente a los usuarios que no son el objetivo. Parece que es responsabilidad del proveedor DCP tomar esa decisión, y no está garantizado que este lo vaya a hacer correctamente. Tampoco está claro cómo un proveedor DCP llevará a cabo la eliminación o la elusión del cifrado de forma selectiva (si será necesario hacer actualizaciones y cómo se hará para que estas sean selectivas y no se filtren). Esto plantea la siguiente pregunta: ¿en qué parte del sistema se implementa el método de acceso excepcional y cómo se pone en práctica?

Diseño y retención de métodos
Si bien en la ley TOLA se trata de salvaguardar el cifrado fuerte afirmando que no se debe pedir ni exigir a los proveedores que implementen vulnerabilidades ni debilidades sistémicas, no se les impide hacerlo. Aunque se podría argumentar que las empresas no

[81]Siempre existe la posibilidad de que se produzca una vulnerabilidad, pero la responsabilidad con respecto a las vulnerabilidades desconocidas por el proveedor depende de cómo se asigne el estándar de responsabilidad del deber fiduciario o la diligencia debida. Es de esperar que no constituya una responsabilidad ilimitada.

[82]Véase Callas, J. (2019), "The 'Ghost User,' Ploy to Break Encryption Won't Work", publicación en el blog de la Asociación Estadounidense por las Libertades Civiles (ACLU), 23 de julio de 2019, disponible en https://www.aclu.org/blog/privacy-technology/ghost-user-ploy-break-encryption-wont-work. Para conocer los antecedentes de la propuesta fantasma que se presentó por primera vez en el Reino Unido, véase Levy, I. y C. Robinson (2018), "Principles for a more informed exceptional access debate," LawFare Blog, 29 de noviembre de 2018, disponible en 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, Reino Unido +44 7554 065 718

están dispuestas ni son proclives a implementar tales vulnerabilidades sistémicas, una prohibición al respecto permitiría que el consumidor confiara más en el cifrado. Dado que la ley TOLA sí permite que ciertos organismos LEIA soliciten o exijan que se implementen vulnerabilidades o debilidades selectivas, ¿cómo se controla dicha vulnerabilidad y cuál es el proceso para prevenir futuras instancias de esa vulnerabilidad?

Reutilización
Aunque limitar las obligaciones a la creación de vulnerabilidades o debilidades selectivas puede parecer en principio una medida en la dirección correcta, en realidad el solo hecho de crear el mecanismo de acceso excepcional, por muy selectivo que sea, abre el sistema al mal uso y a los actores mal intencionados de forma mucho más amplia. Una intervención específica podría dar lugar a usos no previstos que no formen parte de la solicitud o notificación de la ley TOLA, lo que crearía una puerta trasera de amplia aplicación.

Además, crear una intervención significa que ahora se conoce una ruta de entrada. Conocer el método (o, peor aún, las herramientas de software o una implementación) podría dar lugar a que este se divulgara de forma involuntaria o a sabiendas a otras personas no autorizadas. La incertidumbre sobre a quién se le puede haber pedido que cree una intervención de acceso excepcional disminuye la confianza en toda la cadena de valor.

Escalabilidad
Un desafío fundamental a la hora de obligar a los proveedores a crear accesos selectivos es que no hay garantía de que estos no se vayan a aplicar de forma más amplia para convertirlos en parcial o totalmente sistémicos. Para diseñar un ataque sistémico contra un sistema, el primer paso suele ser definir un ataque acotado y luego determinar cómo aplicarlo de forma más amplia. Por consiguiente, exigir a los proveedores que intenten crear intervenciones selectivas es un primer paso para crear vulnerabilidades sistémicas. Además, si una intervención selectiva se necesita con más frecuencia, probablemente se haría más fácil de usar y más automatizada, y por lo tanto comenzaría a convertirse a una intervención sistémica.

Una intervención selectiva tiene más probabilidades de convertirse en sistémica una vez que se descubre, se crea o se divulga el conocimiento sobre la debilidad. Incluso la posibilidad de que exista puede animar a los actores malintencionados a buscarla. Una vulnerabilidad o debilidad selectiva puede convertirse en una vulnerabilidad sistémica simplemente replicando o amplificando la vulnerabilidad en una base de usuarios (a través de actualizaciones, virus u otros métodos).

Filtrado e intercambio
Las intervenciones selectivas pueden filtrarse y ponerse a disposición de una comunidad más amplia en que haya actores malintencionados que podrían utilizarlas

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

para poner en peligro al público.[83]Además, las vulnerabilidades "descubiertas" podrían no ser resueltas, sino conservadas. Una vez que se toma conocimiento de una intervención, es imperioso que el proveedor ponga en práctica los procesos de notificación y resolución establecidos en las comunidades de seguridad, pero en la ley TOLA no se exige a los proveedores que hagan esto. Es razonable decir que, una vez que se introduce una vulnerabilidad o debilidad, es solo cuestión de tiempo hasta que esta se descubra, se divulgue, se filtre, se robe o se le aplique ingeniería inversa.

Incertidumbre en lo que atañe a los procesos y las obligaciones
En el marco de la ley TOLA, se puede pedir a los proveedores DCP que conserven las vulnerabilidades inadvertidas en sus sistemas para usarlas en el futuro, lo que puede crear incertidumbre para esos proveedores en cuanto a cuándo y cómo deben participar en la divulgación de vulnerabilidades. La divulgación clara de las vulnerabilidades envía una fuerte señal de que se mantendrá un cifrado sólido, lo que aumenta la confianza de los usuarios, tanto de las entidades comerciales como de los usuarios finales individuales. También hay incertidumbre en cuanto a lo que una solicitud o notificación de la ley TOLA puede exigir a una empresa; más concretamente, hasta qué punto los proveedores están obligados a ayudar en el proceso de interceptar o descifrar las comunicaciones. La incertidumbre en torno a la ley TOLA significa que las empresas no están seguras de qué métodos se necesitarían para cumplir con una solicitud o notificación de esta ley, y ello significa que los responsables de seguridad dentro de la empresa tendrían dificultades para tomar decisiones sobre qué tecnología adoptar, qué empleados de seguridad contratar, e incluso sobre las consecuencias de asociarse con otras empresas o compartir datos. Este es un ámbito en que sería conveniente adoptar un enfoque reflexivo, adaptado y transparente.

Por su diseño, es difícil romper un cifrado fuerte (o al menos debería serlo)[84], y no está claro cómo hará cada proveedor DCP para responder a una solicitud de acceso. Esta afirmación sobre la falta de claridad se basa en las conversaciones que LECA ha mantenido con varios proveedores DCP importantes. Según nuestras entrevistas, las empresas no están seguras de sus obligaciones y no tienen claro qué métodos serían necesarios para cumplir con una solicitud o notificación de la ley TOLA.

Además, diferentes partes del ecosistema (es decir, diferentes proveedores DCP) tendrán que adoptar diferentes enfoques para eliminar o eludir el cifrado. En nuestras entrevistas hemos comprobado que las distintas clases de proveedores tienen diferentes perspectivas sobre lo difícil o perjudicial que puede ser eliminar o eludir el cifrado. Descubrimos que los operadores tradicionales (es decir, los antiguos proveedores de servicios telefónicos) tienen una visión menos crítica de la aplicación de las solicitudes

[83]En el documento CALEA II, ISOC señaló cómo podrían producirse esas filtraciones(https://cdt.org/wp-content/uploads/pdfs/CALEAII-techreport.pdf).Y véase https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ en EternalBlue.

[84]El uso de métodos como la conversión en fantasma permite añadir silenciosamente a un tercero a una sesión segura, y se podría argumentar que esto no es difícil de hacer, por eso añadimos esta aclaración.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

de la ley TOLA que la que encontramos al hablar con los proveedores de servicios web, de aplicaciones y de otros servicios de Internet.

En síntesis, la ley TOLA podría socavar y erosionar la confianza del público en los numerosos servicios cifrados que todos utilizamos a diario. La mera percepción de que el cifrado es más débil o la amenaza de que los organismos gubernamentales tengan la capacidad de recopilar información socava la confianza en todos los sistemas.

Los consumidores, ya sean entidades comerciales o particulares, pueden no sentirse inclinados a hacer negocios en un entorno en que la confianza está debilitada. Las empresas también tendrán que decidir si quieren enfrentarse a las dificultades legales, operativas y logísticas que puede suponer hacer negocios en Australia (este punto fue planteado por varias empresas importantes durante nuestras entrevistas). Numerosas empresas tecnológicas con sede en Australia han expresado su preocupación por la ley TOLA.

Por ejemplo, en 2020, Patrick Zhang, jefe de Políticas y Asuntos Gubernamentales de Aplasia, declaró que la continuidad de la viabilidad y el crecimiento de la innovación y la fabricación de tecnología en Australia dependerá en gran parte de la seguridad real y percibida de las tecnologías que sustentan la economía digital y su ecosistema.[85] Estas afirmaciones sobre los perjuicios que podrían surgir no son solo especulativas. Vault Systems, un proveedor australiano de servicios en la nube, declaró que la ley TOLA lo estaba afectando de forma sustancial y perjudicial.[86]

En consecuencia, podría ser más fácil simplemente ubicar los servicios en otro país para evitar la infinidad de desafíos y la incertidumbre económica. El *Internet Architecture Board* declaró que este riesgo podría hacer que algunos proveedores de infraestructura se reubicaran, redujeran el servicio o incluso lo bloquearan para los usuarios australianos. Esta fragmentación de Internet es una de las principales preocupaciones que tenemos hoy en día, ya que reduce el valor de una Internet mundial y extremadamente conectada.[87]

[85]"Encryption laws damage potential: Atlassian," InnovationAus, 24 de junio de 2020, disponible en https://www.innovationaus.com/encryption-laws-damage-potential-atlassian/.

[86]"Huge scope of Australia's new national security law reveals itself," ZDNet, 6 de junio de 2019, disponible en https://www.zdnet.com/article/huge-scope-of-australias-new-national-security-laws-reveals-itself/)y "Encryption laws are creating an exodus of data from Australia: Vault," ZDNet, 5 de julio de 2019, disponible en https://www.zdnet.com/article/encryption-laws-are-creating-an-exodus-of-data-from-australia-vault/.

[87]Internet Architecture Board (IAB) Comments on the Australian Assistance and Access Bill, 9 de septiembre de 2018, disponible en https://www.iab.org/wp-content/IAB-uploads/2018/09/IAB-Comments-on-Australian-Assistance-and-Access-Bill-2018.pdf.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

5. Marco económico

El objetivo principal de esta investigación es evaluar todas las pruebas disponibles sobre el impacto económico de la ley TOLA. Habría sido de esperar que esta labor se hubiera llevado a cabo antes de la aprobación de la ley, pero, como hemos explicado, eso no ocurrió. Algo más sorprendente para nosotros ha sido que *no* hemos podido encontrar en ningún sitio —ni a través de nuestra revisión de la literatura publicada ni en el transcurso de nuestra investigación primaria que supuso hacer entrevistas detalladas con grandes proveedores DCP multinacionales (que se analizan con más profundidad en el capítulo 6)— ningún estudio en que se estime el impacto económico de ninguna legislación similar a la ley TOLA. Aunque los partidarios y los detractores de normas del tipo de la ley TOLA han contribuido a un amplio corpus de literatura académica y han presentado escritos en los procedimientos relacionados con esta ley (como ya se ha señalado) y en otros procedimientos similares asociados a otras leyes, como la Ley sobre Facultades de Investigación (Investigatory Powers Bill) del Reino Unido (2016),[88] en todo ese material se observa una escasez de intentos por cuantificar los costos o los beneficios económicos que cabría esperar.

En un mundo ideal, uno buscaría un estudio en que se mencionaran todos los costos y beneficios potenciales, se los tradujera en términos monetarios y se los consolidara para llegar a una estimación de los beneficios económicos netos que cabría esperar que la ley TOLA produjera. Si se dispusiera de esta estimación, ella podría servir de base para determinar si es probable que los beneficios netos de la ley TOLA superen los costos netos. Por supuesto, una estimación monetaria del impacto económico neto agregado por sí sola no sería todo lo que los responsables de formular las políticas tendrían en cuenta a la hora de evaluar el impacto de la ley TOLA. Algunas impactos son intrínsecamente difíciles de traducir en términos monetarios (por ejemplo, la seguridad nacional y la prevención o persecución de la delincuencia). Además, otra consideración importante es la distribución de los efectos económicos (tanto en lo que respecta a la asignación de los costos y beneficios como a la forma en que estos se materializan a lo largo del tiempo).

No vivimos en un mundo ideal, y en este informe no se puede producir una estimación monetaria cuantitativa del impacto de la ley TOLA. En lugar de ello examinaremos cualitativamente los diferentes mecanismos por los que esta ley puede tener efectos económicos. Este análisis permite identificar fácilmente muchos mecanismos por los que esta ley puede generar costos directos e indirectos a los proveedores DCP, a otras empresas y a los consumidores en toda la economía. Los costos pertinentes no se limitan a los costos directos de los proveedores DCP que puedan recibir notificaciones de la ley TOLA, ni siquiera se limitan solo a los costos indirectos que afectarían a las empresas del sector de las TIC, sino que incluyen los costos indirectos de otras empresas y consumidores en general. Además, cabe esperar que los costos se acumulen a lo largo del tiempo a medida que se pongan en práctica las nuevas competencias gubernamentales que se crean en la ley TOLA.

[88] Véase la nota 27 supra.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Nuestro análisis nos lleva a la conclusión de que la ley TOLA tiene el potencial de provocar un daño económico considerable a la economía australiana y producir efectos negativos indirectos que amplificarán ese daño a nivel mundial.

Explicamos por qué cuantificar los componentes de costos y beneficios sería difícil incluso si se dispusiera de mejores datos, al tiempo que señalamos la ausencia casi total de datos pertinentes. Además, explicamos por qué la cuantificación, al menos parcial, de los costos que probablemente causará la ley TOLA es un desafío intrínsecamente más manejable que la cuantificación de los beneficios que esta ley podría aportar.

Nuestro análisis nos lleva a concluir que la fuente potencial más importante de costos relacionados con la ley TOLA está asociada a la amenaza que esta ley supone para la confianza en línea. Como explicamos, incluso un pequeño impacto en la confianza puede conducir a daños económicos que se distribuyan de forma amplia y den como resultado efectos económicos adversos que representen miles de millones de dólares. En comparación con esos costos indirectos que se acumulan con el tiempo, los costos directos en los que incurren las empresas cuyas perspectivas comerciales individuales pueden verse perjudicadas por la ley TOLA son probablemente mucho menores en conjunto, pero siguen siendo considerables para las empresas afectadas y en términos monetarios agregados. Por ejemplo, una de las multinacionales que entrevistamos relató que la ley TOLA ya había hecho que la empresa perdiera más de mil millones de dólares australianos en ingresos, y varios de los encuestados informaron de que ya habían incurrido en pérdidas de ingresos que ascendían a dos dígitos porcentuales. Lamentablemente, estos datos individuales no proporcionan una base fiable para obtener una estimación de los costos agregados en toda la economía.

5.1. Marco para comprender el impacto económico de la ley TOLA

El marco adecuado para realizar esta evaluación es comparar lo que ha sucedido (o es probable que suceda) en el mundo en que la ley TOLA se ha aprobado con un mundo hipotético en el que eso no ha ocurrido.[89] Esto plantea muchos desafíos teóricos y empíricos complejos por múltiples razones, entre las que se encuentra la necesidad de ampliar la labor abordando las siguientes cuestiones:

1. ¿Qué impactos económicos hay que tener en cuenta?
2. ¿Deberíamos centrarnos en los impactos para Australia o para el mundo?
3. ¿Cómo equilibrar los costos de la ley TOLA con los beneficios?
4. ¿El análisis del impacto es a largo o a corto plazo?
5. ¿Cómo se caracteriza el mundo hipotético en que la ley TOLA no existe?

[89] Nótese que es probable que la perspectiva de la aprobación de la ley TOLA haya impactado en el comportamiento y los resultados incluso antes de que la ley se aprobara en diciembre de 2018. Además, la continua incertidumbre sobre las futuras reformas normativas o legislativas, y los desacuerdos sobre la interpretación jurídica de esta ley y sobre cómo se utiliza o se utilizará, contribuyen a distorsionar el desafío de identificar un conjunto de elementos que permitan comparar con claridad el antes y el después, el escenario con y sin la ley, para evaluar los impactos económicos. Como veremos más adelante, una de las razones por las que puede que no se observen efectos medibles en el comportamiento debido a la ley TOLA es porque esta todavía no es totalmente "eficaz" debido a la preocupación por los cuestionamientos a la ley que siguen sin resolverse.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

6. ¿Cómo recopilar datos sobre los impactos de la ley TOLA?

Cada uno de estos desafíos se aborda en las siguientes subsecciones.

5.1.1. ¿Qué impactos económicos hay que tener en cuenta?

La evaluación del impacto económico de la ley TOLA depende de la capacidad de evaluar cómo las empresas y los consumidores afectados por esta ley, ya sea directa o indirectamente, cambiarán su comportamiento como resultado de ella. Esto es difícil porque el comportamiento depende de las expectativas. Lo ideal sería cuantificar los efectos medibles en el excedente total, el cual es la suma del excedente del productor y del consumidor en términos monetarios (en dólares australianos). Los efectos monetarios de la ley TOLA en el excedente del productor y del consumidor no son directamente observables y deben estimarse a partir de la recopilación de datos monetarios y otros datos relacionados con los resultados. Los tipos de efectos relacionados con el comportamiento y los resultados pueden interpretarse de forma amplia de modo que incluyan el efecto potencial de la ley TOLA en los ingresos, la inversión y los planes estratégicos de las empresas. Por ejemplo, el excedente del productor puede estimarse a partir de diversos datos relacionados con los resultados, como los datos sobre los ingresos, los costos operativos y las inversiones de las empresas, que pueden estimarse a partir de los datos sobre las ventas unitarias y los precios y costos por unidad. Para atribuir los cambios en estas variables a un único efecto como la ley TOLA se necesitan datos adicionales que permitan controlar por los demás efectos.

Estimar el excedente del consumidor es aún más difícil, pero incluye estimar la medida en que la demanda inframarginal del consumidor supera los precios pagados (es decir, la medida en que la disposición a pagar supera el precio).[90] Además, el excedente del consumidor también depende de la elección del producto (selección) y de la calidad.[91]

[90] La disposición a pagar no se observa directamente, sino que puede deducirse de las encuestas a los consumidores y del comportamiento en cuanto a las preferencias que se manifiesta en el mercado (es decir, la función de la demanda estimada del sector).

[91] Los consumidores suelen elegir sus compras entre varias empresas, cada una de las cuales ofrece varios niveles de productos (por ejemplo, premium, con descuento) y eligen el producto que ofrece la mejor relación calidad-precio. Frente a un bien de igual calidad, los consumidores siempre prefieren el que tenga el precio más bajo. Sin embargo, dado que la demanda de los consumidores en cuanto a la calidad y a otras características de los productos varía, tener múltiples opciones aumenta la probabilidad de que los consumidores puedan encontrar bienes que se ajusten más a sus gustos particulares. Además, cuantas más empresas haya para elegir, mayor será la competencia, lo que puede dar lugar (o no) a una mayor selección de niveles de calidad en función de la naturaleza del producto y de la dinámica de la competencia, pero en general dará lugar a precios más bajos. Sin embargo, incluso con una sola empresa, la selección de productos que se ofrecen está diseñada para maximizar el excedente del productor, lo que enfrenta a las empresas con el desafío de fijar el precio de los niveles de productos de modo de diferenciar los precios de forma óptima: es decir, fijar los precios de manera que algunos consumidores consideren racional la compensación de calidad añadida por un precio más alto; de lo contrario, los consumidores optan por el bien de menor precio y menor calidad, y el nivel de mayor calidad no es viable en el mercado.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Las respuestas conductuales se refieren a modificaciones en las prácticas de empleo de las empresas, el comportamiento de inversión y la actividad de innovación, que están relacionados. Por ejemplo, las inversiones en capacidad empresarial dependen de las expectativas sobre las perspectivas futuras de la empresa, que dependen de su ventaja competitiva y de las inversiones de la empresa en I+D y en diversos ámbitos estratégicos (por ejemplo, en su imagen de marca, en ciberseguridad, en propiedad intelectual, etc.). Como explicamos más adelante, una de las posibles respuestas conductuales que podría preverse es que las empresas reduzcan sus inversiones en I+D y en la introducción de nuevos productos en Australia cuando prevean que estos serán perjudicados por la ley TOLA, ya sea directa o indirectamente. En la medida en que esto ocurra, la estimación del impacto económico dependerá del cálculo de los beneficios netos futuros que se esperaría que las inversiones disuadidas produjeran o de las mejoras en la oferta de productos y en los precios que de otro modo se habrían producido. Esto es intrínsecamente más difícil que medir lo que realmente ocurrió.

Por consiguiente, los efectos relacionados con el comportamiento y los resultados dependen de las actitudes y expectativas de las empresas. Los impactos tienen el potencial de afectar a toda la economía e incluso a todo el mundo, y por lo tanto se extienden más allá de aquellas atribuibles directamente a las empresas que reciben solicitudes o notificaciones de la ley TOLA. De hecho, se espera que esos efectos indirectos sean mucho mayores en conjunto que los efectos directos. Sin embargo, aunque es difícil evaluar los impactos económicos directos, estimar los indirectos es aún más difícil.

5.1.2. ¿Conviene centrarse en los impactos que inciden en Australia o en los que afectan al mundo?

Aunque nos centraremos en la economía australiana, también nos interesa detectar los posibles efectos indirectos en un ámbito más amplio. El mercado de la tecnología, los productos y los servicios de las TIC es mundial y la legislación de Australia puede incidir en la probabilidad de que se apruebe una legislación similar en otros países que refuerce o debilite el impacto económico de la ley TOLA dentro de Australia a lo largo del tiempo.

La preocupación por la capacidad de los organismos LEIA de acceder a información que cada vez está más en forma digital, ya sea "en movimiento" (llamadas telefónicas, mensajes, transferencias de archivos, intercambios de identidad o credenciales) o "en reposo" (almacenada a modo de archivos o programas digitales en dispositivos o servidores de archivos en la nube), que además está cada vez más protegida por herramientas de ciberseguridad, como las tecnologías de cifrado de extremo a extremo, es considerada por algunos como una grave amenaza para la eficacia de los servicios policiales y de seguridad a nivel internacional.

En múltiples países, los responsables de formular las políticas han propuesto y debatido iniciativas legislativas que otorgarían a los organismos LEIA facultades adicionales

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

para obtener un acceso excepcional a los datos digitales.[92] Como se ha explicado anteriormente, si bien la ley TOLA se aprobó después de que en el Reino Unido se aprobara la ampliación de las facultades del Gobierno para obtener la ayuda del sector a los efectos de eludir el cifrado, es probable que las lecciones aprendidas en Australia incidan en si otros países han de seguir su ejemplo. Esto es preocupante, ya que la falta de pruebas empíricas sobre la existencia de daños económicos considerables puede confundirse con una prueba de que dichos daños no existen, lo que podría animar a otros países a aprobar una ley similar a la ley TOLA, lo que amplificaría los costos que ella genera.

5.1.3. ¿Cómo equilibrar los costos de la ley TOLA con los beneficios?

La evaluación del impacto monetario agregado neto de la ley TOLA exige considerar tanto los costos que esta ley probablemente cause como los beneficios que pueda aportar. Si bien es relativamente fácil determinar los múltiples mecanismos por los que la ley TOLA puede incidir directamente en el comportamiento de las empresas, y por lo tanto en el de los consumidores, de manera que se produzca un aumento de los costos, rastrear el mecanismo por el que la ley TOLA conducirá a un aumento de los beneficios resulta más difícil.

En las secciones siguientes mencionaremos los distintos mecanismos por los que la ley TOLA puede dar lugar a un aumento de los costos. En el resto de esta sección explicaremos por qué la estimación de los beneficios es más difícil.

Tanto en el lado de los costos como en el de los beneficios, las restricciones a la divulgación que forman parte de la ley TOLA interfieren en la recopilación de datos detallados sobre cómo la aplicación de esta ley modifica el comportamiento. Sin embargo, la falta de datos es aún más grave y el rastro de la causalidad más difícil de seguir en el lado de los beneficios que en el de los costos. El principal beneficio percibido asociado a la aprobación de la ley TOLA era que se resolvería la dificultad percibida que el aumento del uso del cifrado suponía para los organismos LEIA a la hora de cumplir con su misión de hacer cumplir la ley y defender la seguridad nacional. Presuntamente, las capacidades ampliadas que la ley TOLA otorga mejorarán la eficacia y la eficiencia de estos organismos. Esta falta de transparencia hace que sea

[92] Por ejemplo, el Reino Unido cuenta con legislación que permite a las fuerzas del orden y a los servicios de inteligencia de seguridad nacional acceder legalmente a la información cifrada desde principios de la década de 2000, facultad que se amplió mediante la Ley sobre Facultades de Investigación del Reino Unido (2016) (véase la nota 27 *supra*). Más recientemente, en los Estados Unidos, el senador republicano Lindsay Graham presentó el proyecto de ley 4051 del Senado, la Ley de Acceso Legal a los Datos Cifrados (LAEDA) en junio de 2020 (véase https://www.congress.gov/bill/116th-congress/senate-bill/4051). Y, en octubre de 2020, la alianza de inteligencia "Five Eyes" entre Australia, Canadá, Nueva Zelanda, el Reino Unido y los Estados Unidos, que son los integrantes originales de la alianza, emitió una declaración conjunta con la India y el Japón en la que pedía mayores capacidades para acceder de forma legal a los datos cifrados (véase https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925601/2020.10.11_International_statement_end-to-end_encryption_and_public_safety_for_publication_final.pdf).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

más difícil determinar cómo la ley TOLA ha modificado o puede modificar el comportamiento de los organismos LEIA (en relación con el comportamiento que habrían tenido en un mundo en que esa ley no existiera).

Sin embargo, incluso antes de profundizar en cómo resolver esa falta de datos, es posible considerar cualitativamente cómo la ley TOLA puede impactar en la eficacia de los organismos LEIA. Hay varios motivos plausibles que sugieren que los beneficios para los organismos LEIA serán pequeños. Entre ellos se encuentran los siguientes hechos: a) que cualquier persona (incluidos los delincuentes) tiene a su disposición tecnologías que permiten superponer capas adicionales de seguridad de los datos, incluido el cifrado, y b) que en muchos países ya existe una amplia legislación en que se prevé la posibilidad de acceder a los datos por medio de la ley.

El primer punto sugiere que aquellos objetivos que tengan la motivación adecuada y quieran asegurar sus datos podrán hacerlo, incluso si se aplica la ley TOLA, empleando un fuerte cifrado tanto en tránsito (p. ej., en la mensajería de extremo a extremo) como en reposo (*p. ej.*, al almacenar en un dispositivo) y haciendo uso de otras técnicas (*p. ej.*, diversas formas de direccionamiento indirecto, como el enrutamiento cebolla) para hacer que cualquier labor de asistencia por parte de los proveedores DCP resulte ineficaz. Los delincuentes saben que siempre están jugando al gato y al ratón con las fuerzas del orden. Por lo tanto, tienen un incentivo adicional para aprovechar las técnicas que utilizan capas adicionales de seguridad.

No obstante, incluso si se rechaza el primer punto, el segundo pone de manifiesto que los beneficios incrementales asociados con la ley TOLA dependen de la medida en que esta ley cree nuevas capacidades que amplíen las posibilidades de las fuerzas del orden para acceder a los datos de objetivos legítimos. Sin embargo, dado que no se sabe con certeza cómo se utilizará la ley TOLA, no se sabe a ciencia cierta cuál puede ser la magnitud de esos beneficios incrementales.

En cualquier caso, el análisis con base empírica de las políticas que se necesita para estimar los costos y los beneficios de la ley TOLA con mayor precisión solo se hace necesario si se espera que las estimaciones de los costos y los beneficios probablemente tengan una magnitud relativamente cercana. Si hay una justificación convincente (o datos) de que los costos totales son mínimos, pero los beneficios totales son sustanciales (o viceversa), entonces contar con estimaciones precisas del impacto económico es menos importante.[93]

Dado que hasta ahora no se ha llevado a cabo (o no se ha puesto a disposición del público) ningún análisis detallado del impacto económico, sería razonable concluir que los beneficios superarían a los costos con mayor facilidad si se concluyera que 1) los costos potenciales son mínimos mientras que los beneficios son grandes, o 2) tanto los costos como los beneficios potenciales son mínimos, pero los beneficios potenciales

[93]Hay cuatro casos posibles de relación entre los costos y los beneficios, que son los siguientes: (grandes, grandes), (grandes, pequeños), (pequeños, grandes), (pequeños, pequeños).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

son mayores.[94] Los argumentos cualitativos citados anteriormente sugieren que el primer caso es improbable, pero que el segundo aún debe abordarse. Por tanto, centrarse en la magnitud de los costos potenciales es un punto de partida razonable.

5.1.4. ¿El análisis de impacto es a largo o a corto plazo?

Es evidente que interesa ver si es posible medir los impactos a corto plazo de la ley TOLA dado que ella se aprobó hace apenas dos años. Sin embargo, es probable que el efecto total de esta ley se observe en el transcurso del tiempo, y el futuro tiene mucho más tiempo para que se materialice cualquier costo que pueda surgir debido a ella. Por ello, se espera que los impactos económicos más considerables de la ley TOLA se produzcan probablemente en el futuro. Por ejemplo, los impactos esperados serían mayores si la ley TOLA sigue en vigor en su totalidad, si el número de solicitudes y notificaciones emitidas en el marco de la ley aumenta más allá del bajo nivel que se ha observado durante los dos primeros años, y si se expande aún más para incluir el uso de notificaciones de capacidad técnica que exigen que los proveedores de servicios modifiquen sus sistemas o tecnología.[95]

5.1.5. ¿Cómo se caracteriza el mundo hipotético en que la ley TOLA no existe?

Tomamos la situación anterior a la ley TOLA como nuestra referencia hipotética, aunque reconocemos que en un mundo en que esta ley no se hubiera aprobado habrían ocurrido otras cosas que podrían ser susceptibles de previsión (p. ej., una versión diferente de la ley TOLA o un ritmo diferente de adopción de la tecnología de cifrado). La determinación de un escenario hipotético adecuado plantea un problema especial a la hora de evaluar el impacto económico de las inversiones en seguridad de la información (como los cortafuegos, la mejora de la supervisión de la seguridad y las tecnologías de cifrado). Esto se debe a que el rendimiento de la inversión se basa en el costo de los daños evitados, y cualquier estimación de este tipo depende de la probabilidad de que esos daños se produzcan en ausencia de la inversión en seguridad de la información, lo que es inherentemente probabilístico e incierto.[96] Una mayor elaboración del escenario hipotético formaría parte de una evaluación de equilibrio más general de los impactos económicos de la ley TOLA.

---

[94] Aquí ignoramos los casos en los que se cree que los costos son grandes, ya que eso haría menos probable que la aprobación de la ley TOLA hubiera estado respaldada por una evaluación del impacto económico.

[95] Hasta la fecha, la utilización de la ley TOLA ha sido mínima: se han emitido menos de 50 notificaciones TAR (y ninguna TAN o TCN) (véase la nota 32 *supra*).

[96] En la mayoría de las inversiones, los beneficios que el usuario percibe provienen del uso de las capacidades que la inversión hace posible (por ejemplo, es posible que un automóvil y los viajes que se hacen con él permitan amortizar la inversión en relación con los kilómetros recorridos). En el caso de las inversiones en ciberseguridad, el beneficio proviene de los daños que no se concretan (por ejemplo, la menor incidencia del fraude o de los costos incurridos en caso de filtración de datos). Al igual que ocurre con el seguro de incendios, al consumidor le gustaría poder recuperar todos los pagos que hizo al seguro por los años en los que no sufrió un incendio.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

5.1.6. ¿Cómo recopilar datos sobre los impactos de la ley TOLA?

Los desafíos que se deben afrontar al estimar el impacto económico de la ley TOLA se hacen mucho más difíciles debido a los requisitos de no divulgación que se establecen en esta ley. Estos impiden que los destinatarios de las notificaciones emitidas en el marco de la ley TOLA informen sobre los detalles de las notificaciones que han recibido o lo que ha sucedido como consecuencia de ellas. También impiden que los organismos LEIA revelen cómo pueden estar utilizando la ley TOLA. Esto hace que sea muy difícil aislar los efectos relacionados con esta ley de los muchos otros efectos que pueden incidir en el comportamiento de las empresas o en sus resultados (por ejemplo, los ingresos, la inversión en ciberseguridad, etc.). Por ejemplo, si las empresas modifican el marketing de su marca, la publicidad de sus productos o las prácticas de atención al cliente, no está claro si lo hacen como resultado de haber recibido una notificación de la ley TOLA, en previsión del modo en que suponen que esta ley afectará sus mercados, o debido a alguna causa totalmente ajena.

La información sobre las notificaciones de la ley TOLA se brinda con retraso y solo a un nivel agregado. Se informa sobre el número de notificaciones emitidas en total, pero no sobre qué tipo de empresas recibieron dichas notificaciones. Los proveedores DCP están autorizados a realizar divulgaciones estadísticas sobre el número total de notificaciones recibidas durante los seis meses anteriores y sobre si las notificaciones fueron voluntarias (TAR) u obligatorias (TAN o TCN), pero las empresas no pueden informar qué organismo LEIA emitió esas notificaciones ni otros detalles.

Los proveedores DCP *pueden* solicitar autorización para divulgar información sobre la asistencia,[97] pero no se sabe si lo harán y, en caso de que lo hagan, si se les concederá autorización. Por ejemplo, un proveedor DCP que sea inducido a proporcionar asistencia que amenace o pueda ser percibida como una amenaza para la seguridad digital de los productos o servicios de ese proveedor puede ser reacio a revelar las acciones de ese tipo por temor al efecto adverso que esto pueda tener sobre su marca.

Si bien es cierto que la plena transparencia sobre el uso de la ley TOLA por parte de los organismos LEIA probablemente perjudicaría la eficacia de las actividades en que estos organismos reciben ayuda en el marco de dicha ley y podría plantear riesgos adicionales de ciberseguridad,[98] el bloqueo casi total de los datos sobre el uso de la ley

[97] Véase el art. 186(2) de la ley TIA, nota 6 *supra* y el art. 317ZF(13)-(17) de la ley TOLA, nota 2 *supra*. Véase asimismo "Assistance & Access: Common myths and misconception", nota 130 *infra*.

[98] Por ejemplo, la plena transparencia incluiría información sobre qué proveedor DCP recibió notificaciones de la ley TOLA, qué se les pidió o exigió a los proveedores en esas notificaciones, qué hicieron estos en respuesta a ellas, qué organismo LEIA las emitió y qué hizo dicho organismo como consecuencia de la asistencia prestada por el proveedor DCP. Obviamente, ese nivel de divulgación pública serviría de aviso a los objetivos que interesan a los organismos LEIA (por ejemplo, los posibles delincuentes), y eso les permitiría tomar medidas evasivas para contrarrestar la labor de investigación de dichos organismos. La divulgación completa también podría revelar detalles sobre las capacidades de seguridad de los organismos LEIA o de los proveedores DCP que podrían ser explotados por terceros, lo que daría lugar a riesgos adicionales de ciberseguridad.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

TOLA hace casi imposible llevar a cabo una evaluación precisa de sus impactos económicos.[99]

Además, la falta de datos relacionados con la ley TOLA, junto con las normas sobre los refugios seguros, las disposiciones sobre los reembolsos que permiten a los proveedores DCP solicitar la recuperación de los costos relacionados con la asistencia, y la ambigüedad en cuanto a lo que los organismos LEIA pueden solicitar o exigir, tienen el resultado perverso de que pueden aumentar los daños económicos que se prevé que esta ley puede causares muy probable que esos daños estén asociados a los efectos indirectos. Esto se debe a que, en conjunto, estas características de la ley TOLA reducen los incentivos para que los proveedores DCP se resistan a cumplir con las solicitudes de los organismos LEIA, incluso si dichas solicitudes pueden suponer una amenaza para la seguridad digital.

Un proveedor DCP que coopere tiene menos probabilidades de ser penalizado por su cooperación tanto por sus clientes como por otras entidades con las que hace negocios, ya que esas otras entidades o clientes no pueden tener certeza de si el proveedor DCP ha recibido una notificación ni de cómo ha respondido. El secretismo que rodea la aplicación de la ley TOLA se suma a la incertidumbre comercial a la que se enfrentan todas las entidades que pueden verse afectadas por dicha ley, lo que hace que esos efectos se propaguen de forma más amplia, ya que las partes interesadas se ven obligadas a suponer que cualquiera de los proveedores DCP, o todos ellos, pueden haber tenido que cumplir con las solicitudes o los requisitos de esta ley.

Por último, la misma falta de acceso a los datos relacionados con la ley TOLA que impide estimar los impactos económicos de esta ley también dificulta su supervisión.[100] Una mayor percepción de que la supervisión de la ley TOLA puede ser inadecuada puede contribuir a aumentar la percepción del riesgo de que los organismos LEIA cometan abusos que amenacen la seguridad digital, y por tanto la confianza digital, lo que agravaría los efectos económicos adversos que esta ley pueda tener.

[99]Para estimar el impacto económico de la ley TOLA, la divulgación no tiene que ser ni completa ni pública. Unos datos más granulares y detallados permitirían hacer mejores cálculos, pero incluso unos datos relativamente generales sobre los tipos de asistencia que se han solicitado, exigido o proporcionado permitirían superar en gran medida la falta de datos. Además, estos datos podrían divulgarse en virtud de órdenes de protección que restringieran la divulgación de los datos detallados utilizados por los analistas o investigadores encargados de hacer los cálculos para estimar los efectos económicos agregados. Indicar cuál es el grado mínimo de divulgación que permitiría hacer estimaciones razonables de los impactos económicos está fuera del alcance de este informe; sin embargo, creemos que se podría permitir un acceso más protegido a los datos pertinentes que facilitaría la estimación de los impactos económicos al tiempo que se preservaría la eficacia de la asistencia otorgada a los organismos LEIA en el marco de la ley TOLA.

[100]De hecho, la estimación del impacto económico de la ley TOLA forma parte de la supervisión necesaria para proteger a Australia y a otros países contra los efectos de una legislación equivocada.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

5.2. Debate cualitativo sobre los impactos económicos

Como ya se ha señalado, es probable que las repercusiones económicas de la ley TOLA sean tanto directas como indirectas, que se acumulen y modifiquen con el tiempo, y que tengan efectos indirectos más allá de Australia. Algunas de estas repercusiones se pueden observar y cuantificar con más facilidad que otras. Por ejemplo, evaluar los efectos directos de la ley TOLA centrándose primero en las empresas comerciales que están obligadas por el ámbito de aplicación de la ley a responder a las solicitudes y notificaciones de esta, así como en los productos y servicios ofrecidos por dichas empresas que hacen uso de datos cifrados, ya sea en movimiento o en reposo, es probable que ofrezca la mayor oportunidad de detectar impactos económicos mensurables de la ley TOLA relacionados con el comportamiento o los resultados.

Además, es probable que una mayor comprensión de los efectos directos ayude a entender la naturaleza de los posibles efectos indirectos. Asimismo, es razonable centrarse primero en tratar de detectar, a partir de la experiencia pasada con la ley TOLA, si ha habido efectos mensurables, antes de tratar de evaluar las previsiones relacionadas con las repercusiones futuras, incluso si se sospecha, como hacemos nosotros, que la mayor parte del impacto económico probablemente se va a producir en el futuro. Esta lógica proporciona una forma natural de analizar cualitativamente el tipo de impactos que prevemos que podrán observarse.

En primer lugar, las solicitudes y notificaciones de la ley TOLA solo pueden estar dirigidas a los proveedores DCP, expresión que se interpreta de forma amplia e incluye a cualquier empresa que preste servicios o productos de tecnologías de la información y las comunicaciones (TIC) en que se haga uso de datos cifrados en Australia (independientemente de que esas empresas tengan su sede en Australia o en el extranjero).[101]Incluso este alcance presenta una compleja "cadena de suministro"[102]

[101]Este alcance excluye la consideración de las empresas o usuarios finales que pueden ser los compradores de los servicios de TIC que hacen uso de los datos cifrados (por ejemplo, hospitales, bancos u otros usuarios finales). Sin embargo, dado que los usuarios finales constituyen la demanda final del uso de los servicios de datos cifrados, el impacto de la ley TOLA en su comportamiento y en los resultados que los afectan (por ejemplo, en los precios que pagan y en la selección de productos entre los que pueden elegir o, de forma equivalente, en la calidad de esos productos) también es pertinente para la evaluación del impacto económico total de esta ley.

[102]Los términos cadena de suministro, cadena de valor o cadena de producción pueden utilizarse indistintamente aquí. Reflejan el concepto de que la producción de la mayoría de los bienes y servicios puede organizarse en una cadena de tareas o etapas que van desde las materias primas, hacia las etapas intermedias de producción y hasta la venta final a los usuarios finales. En su forma más simple, esto se ve como un flujo lineal de etapas que puede organizarse en una serie de empresas que se encuentran antes y después en la cadena, con algunas empresas integradas verticalmente en múltiples etapas secuenciales.Las empresas que operan en la misma etapa son competidores horizontales, mientras que las que operan en diferentes etapas son competidores verticales. En este sentido, la competencia es, en última instancia, por la demanda final que proporciona los flujos de ingresos que sustentan la actividad de la cadena de suministro. Sin embargo, la mayoría de los procesos de producción, especialmente cuando se trata de productos y servicios de TIC, no se ajustan exactamente a

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

integrada por empresas que se encuentran antes y después en esa cadena y que colectivamente son responsables de suministrar servicios y productos de datos cifrados para que sean utilizados (consumidos) por los usuarios finales, que comprenden otras empresas que hacen uso de datos cifrados en sus operaciones diarias (p. ej., bancos, hospitales y, de hecho, la mayoría de las empresas hoy en día, pero con diferentes grados de importancia para sus operaciones) y los consumidores del mercado de masas (p. ej., los usuarios domésticos de servicios de banda ancha móvil y fija).

Al principio de la cadena de suministro se encuentran los productores de tecnologías, equipos y servicios de cifrado, como las empresas que fabrican los equipos de red, contribuyen a la formulación de normas internacionales, poseen patentes o marcas de tecnologías de seguridad, etc. Estas empresas, que de forma vaga se caracterizan como el sector de la seguridad de la información, venden productos de software y hardware que se utilizan para autenticar credenciales digitales, filtrar y bloquear selectivamente el tráfico digital (p. ej., cortafuegos), y otros servicios diversos (p. ej., fuentes de monitoreo del tráfico de ciberseguridad) que son adquiridos y utilizados por los proveedores DCP que se encuentran más adelante en la cadena, como los proveedores de servicios de Internet (ISP), p. ej. Telstra y TPG, o los proveedores de servicios en la nube o edge (de borde) que proporcionan aplicaciones y servicios de contenido, como Facebook, Google o Netflix. La cadena incluye a los fabricantes de dispositivos para el usuario final y a los desarrolladores y proveedores de aplicaciones y servicios de software que hacen uso de esos dispositivos, desde los teléfonos inteligentes hasta las tabletas y los dispositivos de Internet de las Cosas (IoT).

El seguimiento de las relaciones comerciales entre las empresas de TIC se complica por el hecho de que este tipo de empresas venden tanto a otras empresas de TIC como directamente a los usuarios finales (p. ej., empresas y consumidores del mercado de masas que operan redes de datos internas y privadas). Además, muchas empresas de TIC operan en diferentes niveles dentro de la cadena de suministro y pueden vender componentes y tecnología en calidad de proveedores que se encuentran al inicio de la cadena a las mismas empresas con las que al mismo tiempo compiten en los mercados que se encuentran más adelante en la cadena (p. ej., Apple compra componentes a Samsung, ambas tienen licencias cruzadas de tecnología y ambas venden teléfonos inteligentes).

Para analizar el impacto económico de la ley TOLA, uno podría centrarse en toda la cadena de valor de las TIC que proporciona productos y servicios en que se hace uso del cifrado o de datos cifrados, considerando toda esta cadena de valor como una "caja negra" que suministra una serie de productos y servicios en que se hace uso de datos cifrados, y centrarse en cómo la ley TOLA podría incidir en la oferta y la demanda agregadas de esos productos y servicios. En un nivel abstracto y en una economía cada vez más digital, se puede considerar que esto abarca toda la economía de bienes y servicios, ya que en una economía moderna prácticamente todo hace uso directa o indirectamente de las TIC y, cada vez más, el cifrado de los datos se considera una

---

este modelo. Existen múltiples procesos paralelos y complejos bucles de retroalimentación.Las empresas pueden ser simultáneamente competidores verticales y horizontales.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

"mejor práctica" esencial para garantizar que los productos y servicios de las TIC sean "fiables" o estén protegidos de forma equivalente contra los riesgos cibernéticos, entre ellos las vulneraciones de datos que pueden amenazar la privacidad u otras formas de pérdida económica (p. ej., fraude, ataques de *ransomware*, destrucción de valor, pérdida de seguridad personal, etc.).

Desde esta perspectiva, se puede considerar que la ley TOLA impone costos a la seguridad de los datos y, por lo tanto, supone una amenaza para la "confianza" de los productos y servicios digitales, a saber, para la confianza en el uso de Internet y otras redes de datos destinadas al comercio electrónico, que, como ya se ha señalado, abarcará cada vez más a toda la economía. En el análisis económico más sencillo, aumentar el costo de prestar servicios TIC "de confianza" aumentará los costos de la oferta y disminuirá la disposición a pagar de los usuarios finales. Esto sugeriría un desplazamiento al alza de la oferta agregada y un desplazamiento a la baja de la demanda agregada, lo que daría lugar a un nuevo precio de equilibrio más alto después de la ley TOLA con un nivel más bajo de demanda agregada. Los precios serían más altos y la demanda agregada sería menor, lo que daría lugar a lo que los economistas denominan una "pérdida de peso muerto" o pérdida irrecuperable de eficiencia asociada a la imposición de la ley TOLA.

Si este análisis sencillo de los efectos abarcara todos los aspectos de este asunto, entonces, por supuesto, sería irracional haber aprobado esa política. Entre los factores que complican la situación se encuentra el hecho ya señalado de que estamos ignorando las posibles formas en que la ley TOLA podría aumentar la confianza al permitir que las fuerzas del orden sean mejores en la prevención de la delincuencia, lo que daría lugar a un desplazamiento neto al alza de la demanda agregada que podría compensar con creces cualquier amenaza que se estime que la ley TOLA pueda causar debido a un mayor riesgo de que se perciba una pérdida de privacidad o debido a los mayores costos en que puedan incurrir las empresas como resultado de las restricciones que esta ley impone al uso de las tecnologías de cifrado.

Otra complicación del análisis de la ley TOLA es que es poco probable que los efectos sean uniformes en todos los sectores de la economía, en todas las fases de la cadena de suministro de las TIC o en todos los productos y servicios que utilizan el cifrado y, por tanto, en toda la demanda final de esos productos y servicios. Una forma de abordar esta dificultad es aplicar el marco anterior de forma conceptual y por separado a los diferentes sectores, etapas de producción de las TIC o "mercados" de productos y servicios, y luego modelar las interacciones entre estos diferentes análisis de economía y equilibrio parciales para calcular los efectos globales. Estos análisis pueden llevarse a cabo construyendo un modelo de insumo-producto de la economía o de la cadena de suministro de las TIC que tenga el nivel de detalle adecuado y que permita hacer un seguimiento de las compras y las ventas que las empresas o grupos de empresas (o "sectores" o "segmentos del sector") realizan entre sí, así como del impacto de la ley TOLA en los precios y las cantidades de esas transacciones. En principio, cuanto más detallado sea el modelo y mejores sean los datos, la modelización y las herramientas de previsión que se utilicen al poner en práctica el modelo, mejor será la imagen que se podrá obtener tanto de los efectos agregados como de los efectos distributivos de la ley TOLA.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Este modelo económico ideal permitiría considerar cómo las empresas de TIC, las empresas usuarias finales y los consumidores individuales modificarían su comportamiento en respuesta a la ley TOLA, así como el impacto de esta, primero en las empresas directamente afectadas, y luego como consecuencia de las reacciones de otras empresas, y así sucesivamente. Las respuestas conductuales directas e indirectas de las empresas se propagarían por el modelo para producir un nuevo resultado de equilibrio que podría compararse con el equilibrio anterior a la ley TOLA (es decir, el del mundo hipotético en que dicha ley no existe) a los efectos de ver si los beneficios netos totales para la economía australiana o, incluso, para la economía mundial, son mayores o menores con la ley TOLA, y para mostrar cómo se distribuyen los beneficios totales.

Lamentablemente, este modelo ideal no es factible porque no existe ninguno de los elementos necesarios. Antes de considerar las herramientas y métodos económicos disponibles para construir un modelo idealizado de este tipo, basta con señalar que la falta casi total de datos pertinentes es, por sí misma, un impedimento suficiente para estimar el impacto económico de la ley TOLA, independientemente de la perspectiva de alcance que se adopte. No se dispone de datos ni siquiera para determinar de forma inequívoca, y mucho menos para medir, las repercusiones relacionadas con el comportamiento y los resultados en el subconjunto de empresas de la cadena de suministro de las TIC que se verán afectadas por la ley TOLA.

Los defensores de la ley TOLA han adoptado la perspectiva de que los efectos económicos adversos de esta ley probablemente serán mínimos por los siguientes motivos:

- los únicos afectados son los proveedores DCP que reciben notificaciones de la ley;
- en la ley se prevé la recuperación de los costos razonables en que se incurra al dar respuesta a las notificaciones; y
- la ley prohíbe que los organismos LEIA pidan a los proveedores DCP que hagan algo que suponga un daño sistémico para la seguridad de sus productos y servicios.[103]

Es decir, su argumento es que serán pocas las empresas afectadas y que las consecuencias sobre la fiabilidad ("calidad") y el precio ("costo") de los productos y servicios de esas empresas serán insignificantes, por lo que la ley TOLA no tendrá efectos económicos adversos considerables ni desde el punto de vista distributivo ni desde el punto de vista agregado.

Quienes se oponen a las leyes como la ley TOLA en que se otorga acceso excepcional (entre los que se encuentra la mayor parte de la comunidad técnica mundial y del sector de las TIC) refutan ambas afirmaciones. Tomamos como prueba de este punto de vista consensuado el Informe Carnegie (2019), que se hizo eco de las conclusiones a las que se había llegado en un documento anterior redactado por algunos de los mismos

[103]El daño sistémico a la seguridad digital se diferencia de la reducción selectiva de la seguridad digital para la persona o las personas específicamente seleccionadas que son el objetivo de una solicitud de la ley TOLA.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

expertos, en el que se concluía que no hay ninguna forma conocida de permitir el tipo de acceso selectivo a los datos cifrados que se prevé en la ley TOLA sin dar lugar a la creación de una vulnerabilidad sistémica.[104]

En el marco del análisis de los posibles efectos adversos de la ley TOLA, la creación de una vulnerabilidad sistémica y, de esa manera, el otorgamiento del acceso selectivo a los datos cifrados que esta ley hace posible, tendrá un impacto adverso en la "confianza" de la ciberseguridad.[105] Este impacto adverso en la confianza puede surgir de múltiples efectos.

En primer lugar, la posibilidad de que la ley TOLA permita que un organismo LEIA acceda a datos que el objetivo había considerado previamente como seguros significa que la ciberseguridad del objetivo se reduce. En segundo lugar, dado que de forma intrínseca en la ley TOLA no se deja en claro de quién serán los datos objetivo, esto significa que hay un aumento del riesgo cibernético para todos.[106] En tercer lugar, si se acepta la opinión del Informe Carnegie de que no hay forma conocida de permitir el acceso selectivo sin introducir una vulnerabilidad sistémica, la aplicación de la ley TOLA reduciría directamente la ciberseguridad para cualquier sistema o servicio en que se introdujera la vulnerabilidad sistémica. En conjunto, estos efectos sugieren que la ley TOLA da lugar a un mayor riesgo en materia de ciberseguridad.

Además, incluso si fuera factible limitar la vulnerabilidad sistémica, en los comentarios presentados durante la consulta pública sobre la ley TOLA antes de su aprobación en diciembre de 2018, se destacaron las múltiples formas en que la aprobación de dicha ley aumentaría la incertidumbre con respecto a las facultades del Gobierno para potencialmente perjudicar la ciberseguridad.[107] Por lo tanto, incluso si se determinara

[104]Véase "Moving the Encryption Policy Conversation Forward", Encryption Working Group, Carnegie Endowment for International Peace, septiembre de 2019, disponible en https://carnegieendowment.org/files/EWG__Encryption_Policy.pdf. En este informe se resumió la conclusión de un Grupo de Trabajo sobre el Cifrado convocado por la Fundación Carnegie para proporcionar orientación de investigadores de alto nivel de la comunidad de la ciberseguridad sobre cómo abordar la legislación que otorga acceso legal. La conclusión general fue que no veían (todavía) ninguna manera de permitir ampliamente dicho acceso legal sin introducir vulnerabilidades sistémicas.

[105]Utilizamos aquí el término "confianza" de forma abstracta para referirnos a las percepciones que las partes interesadas (clientes, empresas, responsables de formular las políticas, etc.) tienen sobre la ciberseguridad, lo que no se corresponde exactamente con el estado real de esta.

[106]Se puede argumentar que, dado que solo los delincuentes deberían ser el objetivo de las solicitudes de acceso legal, la probabilidad de que los ciudadanos que cumplen con la ley sean alguna vez el objetivo es lo suficientemente pequeña como para ser ignorada. No obstante, eso depende de que se acepte la suposición de que las facultades que la ley TOLA otorga no serían usadas de forma indebida por accidente o de forma intencional, y esas dos son preocupaciones legítimas.

[107]El Departamento de Asuntos Internos australiano publicó 343 de los comentarios recibidos durante la consulta pública (véase https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/the-assistance-and-access-bill-2018).Entre las preocupaciones

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

que la amenaza real a la ciberseguridad o, de forma equivalente, el aumento del riesgo cibernético fuera trivial, la percepción del perjuicio potencial podría dañar la confianza y eso podría dar lugar a efectos económicos adversos potencialmente considerables que no se limitarían solo a las empresas de las TIC o a los proveedores DCP que podrían ser destinatarios de las notificaciones de la ley TOLA.

Por lo tanto, una forma de pensar en la ley TOLA es considerar cuál podría ser el impacto económico que la menor confianza en la ciberseguridad tendría para la economía en su conjunto. Una menor confianza llevaría a una menor demanda de economía digital y a una menor actividad en ese ámbito, y eso reduciría o retrasaría (lo que reduciría el valor económico en términos de valores actuales) el crecimiento de la productividad y la innovación impulsados por las TIC.[108]

Una forma de dimensionar el valor económico de un aumento del riesgo cibernético percibido en toda la economía o de la reducción de la confianza es formular previsiones basadas en escenarios que representen lo que ocurre cuando hay diferentes niveles de confianza. Un buen ejemplo de este tipo de análisis fue preparado por el Zurich Insurance Group en 2015.[109] En ese estudio se utilizó un modelo macroeconómico destinado a pronosticar los beneficios potenciales en términos de crecimiento económico mundial en una variedad de escenarios que diferían con respecto al nivel de confianza en una Internet segura.

En un escenario de alto grado de confianza, el comercio electrónico no se ve amenazado por la ciberdelincuencia y el crecimiento económico es más rápido, mientras que, en el peor de los casos, la ciberdelincuencia daña tanto la confianza en la actividad económica en línea que el comercio electrónico crece mucho más lentamente. El caso de base está en algún punto intermedio. En este estudio se señala que la diferencia potencial entre las previsiones del mejor y del peor caso hacia 2030 asciende a 120

---

comunes expresadas por muchos de quienes formularon los comentarios se encuentran la falta de claridad en cuanto al alcance de las facultades que la ley TOLA otorga, la eficacia de las protecciones y la supervisión, la falta de transparencia y la ausencia de un análisis empírico del impacto económico de esta ley. Todo esto, y los cuestionamientos subsiguientes, contribuyeron a aumentar la incertidumbre sobre el probable impacto de la ley TOLA en la ciberseguridad.

[108]Existe una importante bibliografía económica en que se demuestra que la inversión en las TIC tiene el potencial de ofrecer una rentabilidad importante y contribuir al crecimiento de la productividad económica. Se puede consultar un resumen sobre este tema en Lehr, W. y Sharafat, A. (2017), "ICT Engines for Sustainable Development", en A. Sharafat y W. Lehr (eds.);ICT-centric economic growth, innovation and job creation, Ginebra, Suiza: Unión Internacional de Telecomunicaciones (UIT), disponible en https://www.itu.int/dms_pub/itu-d/opb/gen/D-GEN-ICT_SDGS.01-2017-PDF-E.pdf; o World Bank (2016), “World Development Report 2016: Digital Dividends.”, http://www.worldbank.org/en/publication/wdr2016.

[109]Véase Zurich (2015), “Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures”, informe elaborado por el Atlantic Council and Zurich Insurance Group (Zurich), septiembre de 2015, disponible en http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

billones de dólares estadounidenses, lo que representa una variación del PIB mundial acumulado que asciende al 6%. Esto demuestra la grave amenaza que supone la ciberdelincuencia para la economía mundial. El menor crecimiento se debe al efecto conjunto de la reducción de la demanda para participar en el comercio en línea y la consiguiente reducción de los incentivos por parte de las empresas del lado de la oferta para invertir en el suministro de la capacidad para apoyar el menor crecimiento de la demanda.

Para acercar el contexto a Australia, en un informe de AustCyber (julio de 2020) se estimó que la actividad digital aportaba 426 000 millones de dólares australianos a la economía del país, generaba 1 billón de dólares australianos en producción económica bruta y daba lugar a 1 de cada 6 puestos de trabajo.[110] En ese informe se estimaba que una interrupción digital de cuatro semanas debido a un ciberataque generalizado costaría el 1,5% del PIB anual de Australia.[111] Se trata de una estimación de los efectos directos de un ataque exitoso, y un aumento del riesgo cibernético significa que es más probable que ese resultado pueda ocurrir.

Lo que ambos estudios destacan es el potencial de que se produzcan grandes impactos adversos si la seguridad digital se ve comprometida y, por lo tanto, la importancia de mejorar la confianza en la seguridad digital. Desgraciadamente, no proporcionan una orientación útil sobre cómo cuantificar el modo en que la ley TOLA puede aumentar el riesgo cibernético, aparte de sugerir que los efectos podrían ser muy grandes y tener un impacto en toda la economía.[112]

También es posible considerar que puede haber efectos adversos regionales o sectoriales derivados de las amenazas asimétricas a la confianza. Por ejemplo, cabe esperar que los sectores australianos de las TIC sufran un mayor impacto adverso asociado a la ley TOLA a corto plazo, debido a la menor confianza en sus productos y servicios, que los sectores de las TIC de otros países que no se ven directamente afectados. Esto podría afectar negativamente la competitividad internacional del sector de las TIC de Australia. También se podría explorar por debajo del nivel nacional para

[110]Véase AustCyber (2020), "Australia's Digital Trust Report", disponible en https://www.austcyber.com/resource/digitaltrustreport2020. Informe de julio de 2020, 52 páginas.En el informe se estima que el 22 % de la economía australiana se sustenta en la actividad digital, que de forma directa representa el 6 % del PIB. Los sectores son los siguientes: actividad digital, 317 000 millones de dólares; ciberseguridad, 16 000 millones; comercio minorista en línea, 35 000 millones; salud digital, 2700 millones; energía solar, 700 millones; industria espacial, 3900 millones, etc. (página 11).

[111]Ibid., página 5. En el informe se estima que se perderían 30 000 millones de dólares australianos y 163 000 puestos de trabajo como resultado del ataque generalizado.

[112]El impacto podría ser grande si se produjera una única filtración de datos que tuviera un gran efecto generalizado, si se produjeran muchas filtraciones pequeñas en lo individual pero que tuvieran un gran impacto agregado, o si ocurriera una combinación de estos dos mecanismos. La cuestión es que las vulnerabilidades de ciberseguridad pueden dar lugar a múltiples tipos de daños que difieren en cuanto a su gravedad y alcance. A falta de un modelo del panorama de las amenazas y de la probabilidad de que determinadas amenazas tengan éxito, no es posible prever de forma fiable el daño que se espera que ocurra.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

observar los subsegmentos de los sectores de las TIC y otros sectores que dependen de forma heterogénea, en mayor o menor medida, del uso de datos cifrados que serían vulnerables debido a la ley TOLA.

A nivel de las empresas, se podría prever que la ley TOLA podría dar lugar a una serie de efectos directos o indirectos. Por ejemplo, la reducción de la demanda agregada de los productos de una empresa debido a la reducción de la confianza del mercado reduciría el pastel para todas las empresas. Además, la medida en que un empresa sufriera una pérdida de confianza aún mayor podría reducir la cuota de mercado de esa empresa en la menor demanda agregada. Los efectos de la reducción de la seguridad de los datos podrían ser desde menores (p. ej., la pérdida de unas pocas ventas de unos pocos productos) hasta mayores (p. ej., la amenaza existencial para el negocio futuro de una empresa si la ley TOLA lleva a los participantes del mercado a desconfiar del compromiso de la empresa con la transparencia y la seguridad de los datos de los clientes).

Este último resultado es una preocupación pertinente para las empresas cuyos modelos de negocio se basan en el software de código abierto y en los servicios y productos de venta masiva (es decir, servicios y productos que no se adaptan a cada cliente individual). Apostar por el código abierto como componente clave del modelo de negocio y de la plataforma compromete a la empresa a un nivel de transparencia que es fundamentalmente incompatible con las restricciones que la ley TOLA impone a la capacidad de las empresas para revelar las modificaciones que podrían tener que hacer en los productos y servicios que ofrecen y en el código para responder a una notificación de la ley TOLA.

Para evaluar el impacto económico de la ley TOLA, una empresa individual tiene que evaluar la probabilidad de que pueda recibir una solicitud o notificación de esta ley que afecte sus operaciones, cómo eso afectaría sus operaciones, y cuáles serían sus opciones a la hora de responder. Esto es similar a la forma en que las empresas deben evaluar su riesgo cibernético y determinar sus estrategias óptimas para invertir en productos y servicios de seguridad de la información, como cortafuegos, servicios de monitoreo de tráfico y otros recursos internos de ciberseguridad, incluido el seguro cibernético, para hacer frente a cualquier riesgo cibernético residual que no pueda ser adecuadamente abordado mediante la mejora de los procesos de ciberseguridad.[113] En las subsecciones

[113]La toma de decisiones de inversión en materia de seguridad de la información y seguro cibernético requiere una gran cantidad de información y, por tanto, es costosa en sí misma. Arora et al. (2004), Hubbard y Seiersen (2016), Jones (2005), Gordon y Loeb (2002) y otros han propuesto herramientas y métodos teóricos sobre la toma de decisiones para ayudar a estimar los costos cibernéticos y los beneficios de las estrategias alternativas de ciberseguridad para ayudar en la toma de decisiones de inversión. Véase Arora, A., D. Hall, C. Piato, D. Ramsey y R. Telang (2004) "Measuring the Risk-Based Value of IT Security Solutions",*IT Professional*, 6(6), 35-42; Hubbard, D. W. y R. Seiersen (2016).How to measure anything in cybersecurity risk, John Wiley & Sons: New York, 2016; y Gordon, L. A., y Loeb, M. P. (2002). The economics of information security investment.*ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457. Para comprender algunos de los desafíos asociados a la evaluación del impacto económico de la

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

siguientes se hace referencia a algunas de las formas en que una empresa individual podría sufrir efectos adversos debidos a la ley TOLA.

5.3. Aumento de la incertidumbre empresarial

Como ya se ha señalado, la ley TOLA aumenta la incertidumbre normativa. Una mayor incertidumbre técnica, de mercado o normativa aumenta el riesgo de las inversiones irreversibles, lo que puede retrasar o disuadir dichas inversiones. Medir el impacto de la incertidumbre empresarial es difícil en general, y no es práctico para determinar el efecto de una ley en particular como la ley TOLA.

Sin embargo, se puede obtener una idea de la importancia potencial de las leyes que afectan la incertidumbre normativa asociada al uso de la tecnología de cifrado a partir de los dos únicos estudios realizados hasta la fecha en que se pretendió estimar el impacto económico de la tecnología de cifrado. Estos estudios fueron realizados por el Instituto Nacional de Normas y Tecnología (NIST) de los EE. UU. en 2001 y 2018.

En el estudio sobre el impacto del cifrado del NIST (2001),[114] los investigadores trataron de estimar la contribución económica que la promoción de la norma sobre el cifrado de datos (DES) por parte del NIST aportó a la economía estadounidense. Llegaron a la conclusión de que la labor del NIST había acelerado varios años la adopción de la DES, lo que supuso unos beneficios netos de entre 345 y 1190 millones de dólares estadounidenses asociados a la reducción de los costos de gestión de los datos bancarios de terceros.[115]

---

ciberdelincuencia, véase Wolff, Josephine y William Lehr (2017), "Degrees of Ignorance About the Costs of Data Breaches: What Policymakers Can and Can't Do About the Lack of Good Empirical Data", 45th Research Conference on Communications, Information and Internet Policy (TPRC45), septiembre de 2017, Alexandria, VA, disponible en SSRN: https://ssrn.com/abstract=2943867.

[114]Véase Leech, D. y M. Chinworth (2001), "The Economic Impacts of NIST's Data Encryption Standard (DES) Program", estudio elaborado para el Grupo de Planificación Estratégica y Análisis Económico de la Oficina de Programas del Instituto Nacional de Normas y Tecnología (NIST) de los EE. UU., octubre de 2001, disponible en https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=918355 (en adelante, estudio del NIST sobre el impacto del cifrado 2001).

[115]El objetivo del estudio era demostrar cómo el NIST contribuía al crecimiento económico. En el estudio de caso se documentó el papel del NIST a la hora de promover la adopción de una norma de cifrado del sector, algo que ocurrió antes de lo que habría ocurrido si el NIST no la hubiera promovido. El estándar DES se adoptó en 1977, y en el estudio se analizó el comportamiento de adopción entre 1977 y 1982. En un principio, los investigadores trataron de recopilar datos de encuestas para medir directamente el impacto, lo que resultó infructuoso. La alternativa que utilizaron finalmente fue calcular el impacto en función de los resultados específicos de un sector, basándose en los costos que se habían evitado los bancos minoristas de EE. UU., que pudieron pasarse a las transacciones electrónicas (menor costo) más rápidamente de lo que habrían podido hacerlo si la norma no se hubiera adoptado. Calcularon los beneficios que las transacciones electrónicas proporcionaban en cuanto a la reducción de los costos a medida que se fueron concretando con el correr del tiempo (el mundo real), y los compararon con dos escenarios hipotéticos (el mundo en que los beneficios

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

En un estudio posterior del NIST (2018) se analizó el impacto económico del estándar de cifrado avanzado (AES), en cuya promoción el NIST también desempeñó un papel.[116] Ese estudio se basó en un enfoque basado en encuestas destinadas a obtener estimaciones de cómo la norma AES ayudaba a reducir los costos de las empresas activas en la implementación de tecnologías de cifrado debido a la existencia de un estándar federal. En el estudio del NIST (2018) se volvió a plantear un mundo hipotético en el que la evolución hacia el estándar AES, más eficiente, hubiera sido más lenta.

En este caso, los investigadores se beneficiaron de poder modelar directamente las mejoras de rendimiento que el estándar AES ofrecía en relación con el estándar que estaba sustituyendo. En el estudio del NIST (2018) se estimó que la tasa interna de retorno de la inversión del NIST en la promoción de la AES fue del 81 %, significativamente más que el costo de capital del 7 % que el NIST tenía (en el marco de los estándares gubernamentales), y que los beneficios netos agregados para la economía superaban los 250 000 millones de dólares una vez que se computaban todos los efectos indirectos y directos.

En ambos estudios se concluyó que una pequeña inversión para acelerar la implementación de las capacidades de cifrado había dado lugar a beneficios muy grandes para la economía. Esto sugiere que considerar la ley TOLA como una intervención que tiene el potencial de retrasar la implementación de técnicas de cifrado mejoradas (frenando la adopción o inclinándola hacia un cifrado menos seguro) podría tener un gran impacto negativo. Además, en ambos casos se podría entender que la labor del NIST para promover la aceptación de un estándar sectorial contribuyó a reducir la incertidumbre empresarial.

5.4. Daño a la marca empresarial

Las empresas establecen su marca a través de la publicidad y la reputación que construyen por la forma en que sus productos se comparan en el mercado con las ofertas de la competencia. Cuanto mejor sea la marca, más fácil será para la empresa vender sus productos y obtener ingresos por ventas, defenderse de los competidores o responder a los cambios adversos del mercado, y más atractiva será la empresa para los inversores. Si todo lo demás no cambia o se mantiene constante, una mejor imagen de marca se asocia con mayores ventas a lo largo del tiempo y, por tanto, con un mayor valor de mercado (que es reflejo de la evaluación del mercado respecto del valor descontado de los beneficios que se espera que la empresa tenga en el futuro). Se trata de un activo intangible que no puede medirse directamente, sino que se evalúa por referencia a los cambios en otros indicios medibles, como las ventas, los beneficios, el valor de mercado o las encuestas sobre la percepción de los inversores o los clientes.

se hubieran retrasado 3 años y el mundo en que se hubieran retrasado 6 años), y calcularon el valor presente neto de los escenarios para estimar el efecto neto de la labor del NIST.

[116]Véase Leech, D. y John Scott (2018), "The Economic Impacts of the Advanced Encryption Standard, 1996-2017", elaborado para el Instituto Nacional de Estándares y Tecnología, NIST GCR 18-017, disponible en https://doi.org/10.6028/NIST.GCR.18-017.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Cualquier cosa que amenace la percepción relativa de la confianza en una empresa puede dañar su marca y, por tanto, sus perspectivas de venta y su valor comercial. Aunque los clientes, los socios comerciales, los inversores y las personas de dentro de la empresa pueden evaluar de forma cualitativa si la ley TOLA ha tenido un impacto significativo en la marca de la empresa o no lo ha tenido, ese efecto no puede cuantificarse directamente.

Según algunas interpretaciones de la ley TOLA, el posible efecto adverso de esta ley se podría considerar como una amenaza existencial para algunas empresas cuya marca depende en gran medida del compromiso que las empresas tengan con la ciberseguridad y/o para los modelos de negocio que dependen del software de código abierto.Por ejemplo, un proveedor de ciberseguridad que ofrece tecnología de cifrado podría ver socavado su producto principal por la creación de una capacidad en Australia que amenace su oferta de servicios.En otro caso, la ley TOLA podría deshacer el modelo de negocio de una empresa que se base en el compromiso con un software transparente y de código abierto que no discrimine entre los usuarios finales.Que esa empresa se vea obligada a modificar el código en relación con un cliente objetivo y luego no pueda revelar esas modificaciones al resto de sus clientes (debido a los requisitos de no divulgación que la ley TOLA impone) sería incompatible con un componente fundamental de su modelo de negocio. Asimismo, en otro caso más, una empresa que construya su modelo de negocio sobre la base de un código propio podría ver socavado un activo fundamental si la ley TOLA la obligara a revelar un código fuente que podría filtrarse al dominio público.

5.5. Pérdida de ventas

Aunque el impacto directo en la imagen de marca de una empresa no puede cuantificarse directamente en dólares, el impacto en las ventas a menudo sí.Una empresa puede ser capaz de determinar qué acontecimiento concreto ha afectado negativamente al comportamiento de compra de determinados clientes o hacia determinados productos. Una empresa puede observar que los clientes compran menos de sus productos o servicios porque los clientes indican que están preocupados por la amenaza que la ley TOLA supone para la seguridad de los datos.

Esas ventas perdidas pueden deberse a un menor consumo por parte de los compradores (p. ej., porque reflejan la reducción de la demanda agregada en un mundo menos fiable) o a ventas que se desplazan hacia un competidor. El competidor puede ser otra empresa en el mismo mercado (Australia) o en el extranjero. Los cambios en el comportamiento de compra de los clientes y, por tanto, en las ventas de la empresa, pueden ser atribuibles a subconjuntos específicos de productos en mayor o menor grado. Las empresas suelen ponerse en contacto directamente con los clientes reales y potenciales para saber qué les interesa y por qué compran lo que compran. Las empresas también pueden deducir esto a partir de lo que compran los clientes y de la información de mercado proporcionada por terceros en que se trata de estimar el valor para los clientes de las diferentes características relacionadas con la seguridad.

Aunque, en principio, los datos sobre las ventas son una de las fuentes de efectos directos más fácilmente observables, determinar los cambios en las ventas provocados

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

por una ley específica como la ley TOLA siempre es difícil. En primer lugar, hay muchos factores que pueden incidir en el comportamiento de los clientes, y separar los efectos de esos factores puede no ser factible. En segundo lugar, cuando se prevén los efectos que ocurrirán en el futuro, hay que tener en cuenta la mayor dificultad que supone pronosticar acontecimientos futuros inciertos. En tercer lugar, los clientes no siempre son sinceros a la hora de explicar por qué compran lo que compran. Puede que no quieran brindar la información porque no quieren ofender a su proveedor o porque les preocupa que revelar demasiada información pueda poner en peligro su posición a la hora de negociar. Independientemente de la causa de que las ventas se reduzcan, la reducción de las ventas suele traducirse en una reducción de los beneficios (bajo el supuesto razonable de que las empresas evitarían las ventas incrementales que no aportaran suficientes ingresos como para cubrir los costos incrementales),[117] y un menor flujo de beneficios futuros se traduce en un menor valor económico para la empresa.

Aunque es difícil considerar cómo se podría evaluar la pérdida de ventas, hay una serie de razones que permiten prever por qué el riesgo de que haya un efecto adverso considerable en las ventas puede ser sustancial. Por ejemplo, en julio de 2020, el Tribunal de Justicia de la Unión Europea emitió una decisión muy esperada que invalidaba la utilización de una solución que permitía a las empresas estadounidenses y europeas intercambiar datos de clientes que no violaban la normativa europea sobre privacidad, lo que generó la amenaza de que las empresas que intercambiaban datos entre Estados Unidos y Europa aumentaran la protección de los datos o dejaran de intercambiarlos.[118]

Se puede considerar que la ley TOLA amenaza la capacidad de cumplir las normas de protección de datos más estrictas adoptadas por la Unión Europea y, por tanto, supone una amenaza para la capacidad de las empresas de intercambiar datos entre Australia y la Unión Europea. Además, en la medida en que la ley TOLA sea indicativa de nuevas ampliaciones de las facultades gubernamentales en Australia, o en cualquier otro lugar, para obligar a brindar acceso a datos confidenciales, eso podría provocar nuevas interrupciones en el flujo de datos.[119] Dado que los intercambios internacionales de datos son fundamentales para el buen funcionamiento de la economía digital en el mundo, la interrupción de dichos intercambios puede tener un impacto desastroso en el comercio digital mundial.

[117]En este caso no tenemos en cuenta las estrategias a corto plazo, como las ventas a pérdida o las operaciones comerciales durante una recesión temporal.

[118]Véase "The 'Schrems II' decision: EU-US data transfers in question", iapp Privacy Tracker, disponible en https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

[119]Por ejemplo, Nueva Zelanda cuenta con una decisión de adecuación de la UE, y la ley TOLA puede repercutir negativamente en las decisiones de las entidades neozelandesas de utilizar servicios de alojamiento u otros servicios prestados por empresas australianas sujetas a la ley TOLA (véase "Adequacy Decisions", Unión Europea, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

5.6. Aumento de los costos de explotación debido a la ley TOLA

Los costos de las empresas pueden aumentar como consecuencia de la ley TOLA. En primer lugar, las empresas que reciban una solicitud o notificación en el marco de esta ley pueden incurrir en costos directos. Los costos dependerán de si el cumplimiento es voluntario (solicitudes de la ley TOLA) u obligatorio (notificaciones de la ley TOLA), y de los requisitos específicos que la notificación establezca.

La ley TOLA tiene disposiciones destinadas a mitigar los costos directos que responder a las notificaciones pueda generar: a) permitiendo que los destinatarios recuperen los costos incrementales generados por la respuesta, y b) limitando el alcance de las solicitudes de la ley a aquellas que no darían lugar a la introducción de vulnerabilidades sistémicas. Dada la dificultad de estimar los costos totales de responder a las solicitudes o notificaciones de la ley TOLA, que incluyen tanto los efectos directos como los indirectos, es razonable esperar que los proveedores DCP se muestren escépticos en cuanto al compromiso de reembolsar la totalidad de los costos asociados al impacto de esta ley, o siquiera la totalidad de los costos directos en que se incurra al responder a una notificación.

Además, observamos que hay antecedentes de cómo la supervisión no ha sido del todo eficaz a la hora de limitar el alcance de los organismos gubernamentales que actúan en virtud de nuevas facultades otorgadas.[120] En consecuencia, es razonable esperar que los proveedores DCP y otras empresas afectadas por la ley TOLA tengan dudas sobre la eficacia de las disposiciones de supervisión a la luz de la falta de transparencia, la vaguedad de algunas partes de la ley y otros problemas potenciales. Después de estimar los costos directos de responder a una solicitud o notificación de la ley TOLA, la empresa tendría que ponderarlos según la probabilidad de recibir dicha solicitud o notificación. Cuanto menor sea la probabilidad de que la empresa reciba una solicitud o notificación, menor será el costo directo esperado en el que se incurrirá como resultado.

[120]Véase la amplia literatura económica sobre la elección pública y la economía de la regulación sobre la falta de claridad de las normas, que tiene una larga historia que se remonta al menos a "La riqueza de las naciones" de Adam Smith, pero que incluye sobre todo el trabajo de George J. Stigler., “The Theory of Economic Regulation”, The Bell Journal of Economics and Management Science Vol.2, No. 1 (Spring, 1971), págs. 3 a 21; y Peltzman, S. (1976), “Towards a More General Theory of Regulation”, Journal of Law and Economics, 19, 211–48. Véase también la teoría económica de las burocracias, incluidos los organismos reguladores, en particular la tesis de maximización del presupuesto de William Niskanen, “Bureaucracy and Public Economics" (Cheltenham, UK: Edward Elgar, 1994). Véase asimismo Helm, Dieter. (2006) “Regulatory Reform, Capture, and the Regulatory Burden”, Oxford Review of Economic Policy, 22 (2), 169; y Dal Bó, E. (2006), “Regulatory Capture: A Review”, Oxford Review of Economic Policy, 22(2), 203–25. Para leer sobre el reconocimiento del problema por parte del Gobierno, véase UK Cabinet Office Report - Better Regulation Task Force and Regulatory Creep Sub-Group - 2004: “Avoiding Regulatory Creep”, donde se define la falta de claridad de las normas como el proceso por el cual las normas se diseñan o se aplican de manera poco transparente y no de acuerdo con los cinco principios de la buena normativa: proporcionalidad, responsabilidad, coherencia, transparencia y focalización.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Además, aunque el cumplimiento de las solicitudes de la ley TOLA sea voluntario, es razonable prever que algunos destinatarios pueden percibirlas como un presagio de posteriores notificaciones emitidas en el marco de esa ley. Por lo tanto, la opinión de que las solicitudes de la ley TOLA tienen un impacto económico significativamente menor que las notificaciones emitidas de conformidad con esa ley es discutible.

En segundo lugar, incluso las empresas que probablemente nunca reciban una solicitud o notificación de la ley TOLA pueden tener problemas de imagen de marca o de relación con los clientes que pueden inducirlas a incurrir en costos adicionales para resolverlos. Es posible que se sientan obligadas a aumentar la publicidad de la imagen de marca y el marketing directo para compensar los riesgos percibidos para su imagen de marca o sus perspectivas de venta. Pueden tener que gastar recursos adicionales para hacer frente a las preocupaciones reales o percibidas de los clientes sobre el impacto que la ley TOLA tendrá sobre la seguridad de sus datos y la confianza en línea.

En tercer lugar, a las empresas les puede preocupar que la seguridad de los servicios o productos proporcionados por sus proveedores o la seguridad de las operaciones internas de la empresa en Australia se vean amenazadas por la ley TOLA. Las empresas pueden reevaluar sus relaciones con los proveedores y sus opciones de subcontratación (p. ej., de servicios en la nube para gestionar los datos de los clientes o los datos confidenciales de la empresa) a la luz de la mayor preocupación de que esos datos puedan ser vulnerables debido a las respuestas conductuales de los socios proveedores inducidas por la ley TOLA.

Esto podría dar lugar a que las empresas dejaran de subcontratar o tener proveedores en Australia y lo hicieran en el extranjero para evitar la ley TOLA. El ajuste de las relaciones con los proveedores o el traslado de las operaciones internas de la empresa hacia fuera de Australia conllevará costos de ajuste que deberían ser directamente atribuibles a la ley TOLA, al tiempo que tendrá efectos secundarios adversos en otros participantes del sector digital australiano, lo que aumentará los efectos indirectos de esta ley.

En cuarto lugar, las empresas pueden desviarse de su estrategia óptima de ciberseguridad debido a las limitaciones impuestas por la ley TOLA. Esto se manifestaría probablemente como un aumento de los costos de seguridad de la información y seguro cibernético para compensar o hacer frente al mayor riesgo cibernético asociado a esta ley. Una de las formas en que las empresas calculan el riesgo cibernético es mediante la estimación de la amenaza de que ocurran diferentes tipos de ataques. Una de las amenazas más difíciles de abordar son las internas, o los ciberdelitos perpetrados por empleados que por lo demás son de confianza.

Por ejemplo, una fuente común de vulneración de datos son los empleados descontentos o corruptos motivados por el deseo de venganza o de obtener ganancias ilícitas, que eluden las defensas de seguridad internas para filtrar datos hacia fuera.[121] El mejor

[121]Aunque no hay estadísticas fiables sobre qué porcentaje de las filtraciones de datos se deben a amenazas internas, está ampliamente aceptado dentro de la comunidad de la seguridad que los empleados que no siguen los procedimientos de seguridad a propósito o por

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

cortafuegos del mundo no impide que un empleado se lleve a casa archivos de datos confidenciales en una unidad USB o en papel.

Se podría considerar que la ley TOLA aumenta las amenazas internas, ya que tiene el potencial de hacer valer la autoridad del Estado para inducir a un empleado, por lo demás digno de confianza, a saltarse los protocolos de seguridad de la empresa. La falta de transparencia y las restricciones sobre la información que los destinatarios de una notificación de la ley TOLA pueden compartir con terceros (como los asesores jurídicos) u otros empleados de la empresa pueden exacerbar aún más este riesgo de amenaza interna.

Para evaluar el impacto potencial de la ley TOLA en los costos de explotación y de capital relacionados con la seguridad de la información y el seguro cibernético de una empresa, es necesario saber cómo la empresa utiliza el cifrado tanto en los datos en movimiento como en los datos en reposo y, como se ha señalado anteriormente, las opciones de modificar las estrategias de seguridad de la información y seguro cibernético para responder a esta ley. Además de dividir los desafíos de seguridad de los datos entre los que se relacionan con los datos en movimiento (por ejemplo, los servicios de comunicación electrónica, como la telefonía, el correo electrónico, el chat, la mensajería, el acceso a terminales remotos, etc.), y los que se relacionan con los datos en reposo (por ejemplo, archivos de datos confidenciales, credenciales de seguridad, etc.), será importante saber cómo se utiliza el cifrado internamente en la empresa, en sus relaciones con los socios de la cadena de suministro, como los proveedores, y con sus clientes.En cada uno de los seis casos puede haber diferentes consideraciones y opciones económicas que sean pertinentes (y pueden ser necesarios casos adicionales para abordar diferentes productos, mercados o segmentos de clientes).[122]

En quinto lugar, en respuesta a los crecientes esfuerzos nacionales por proteger los datos de los ciudadanos contra la vigilancia extranjera, las empresas digitales pueden verse obligadas a invertir en una mayor labor de localización de datos. Por ejemplo, tras la ruptura del acuerdo anterior que proporcionaba un refugio seguro para los intercambios internacionales de datos dentro de la Unión Europea después de la decisión Schrems I en 2015, Microsoft invirtió en proporcionar una solución de localización de datos en Alemania que posteriormente se abandonó en 2016 una vez que el sector aprobó un nuevo acuerdo de intercambio de refugio seguro.[123]

---

accidente son una fuente importante de filtraciones de datos, pero como la mayoría de las filtraciones de datos no se notifican y las estadísticas de las que se notifican son incompletas, no se sabe qué porcentaje son internas. En una encuesta se informó de que el 66 % de las organizaciones consideran más probables los ataques internos malintencionados o las filtraciones accidentales que los ataques externos (véase https://techjury.net/blog/insider-threat-statistics/#gref, agosto de 2020).

[122]Los seis casos se refieren a (usos de datos en reposo/datos en movimiento) x (uso interno/relaciones con proveedores/relaciones con clientes).

[123]Véase “Microsoft Cloud Germany opens using a Data Trustee Model”, eWeek, 22 de septiembre de 2016, disponible en https://www.eweek.com/cloud/microsoft-cloud-germany-opens-using-data-trustee-model que es un artículo de 2016 que salió en la prensa comercial cuando Microsoft anunció el nuevo acuerdo; y https://mspoweruser.com/microsoft-is-

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Al abandonar la solución provisional, Microsoft señaló los mayores costos y la menor eficiencia para el cliente que se derivan de adoptar una solución de localización de datos. Estas soluciones aumentan los costos y disminuyen la eficiencia al limitar la capacidad de las empresas multinacionales para aprovechar las economías de escala y de alcance. El costo de actualizar el software (que incluye distribuir parches de software para resolver nuevos problemas de seguridad) aumenta porque se incurre en costos para crear respuestas diferenciadas por el mercado, junto con los costos generales añadidos asociados con gestionar un proceso de actualización más complejo.

5.7. Reducción de las oportunidades de crecimiento futuro debido a la ley TOLA

Por último, la ley TOLA puede hacer que las empresas se replanteen sus planes estratégicos de inversión en relación con el desarrollo y el lanzamiento de nuevos productos y características. Esto podría llevar a las empresas a modificar sus planes de lanzamiento o los precios de los nuevos productos y conjuntos de características que aumentan el valor. Puede llevar a las empresas a decidir no ofrecer ciertos productos en Australia para protegerlos del impacto de la ley TOLA. Además de reducir las ventas futuras de la empresa y el potencial de crecimiento (o el excedente del productor), esto también niega a los consumidores los beneficios de tener más posibilidades de elegir y, por tanto, reduce el excedente del consumidor.

Una menor inversión en productos nuevos y más seguros puede traducirse en una menor inversión en la capacidad de la empresa, en particular una menor inversión en I+D e innovación de productos. Se puede decidir posponer estas inversiones, renunciar por completo a ellas o trasladarlas fuera de Australia. En cualquier caso, hay una pérdida directa e indirecta para la economía australiana.

5.8. Impactos a largo plazo y a nivel mundial

Aunque la ley TOLA se aprobó en 2018, dos años después sigue presentando dificultades que hacen que su futuro a largo plazo sea incierto. Si esta ley realmente

---

discontinuing-the-german-data-trustee-model/, que salió en 2018, cuando Microsoft anunció que detenía su esfuerzo de localización de datos. Aunque Microsoft no señala qué repercusiones tuvo en los costos el poner en marcha y luego abandonar su modelo de fideicomiso de datos, es razonable suponer que el proyecto costó millones de dólares. Tras la última decisión Schrems II, que anuló el refugio seguro que se había establecido unos años después de Schrems I, Microsoft reafirmó su determinación de proteger la confidencialidad de los datos de sus clientes (véase "New steps to defend your data", Microsoft Blog, 19 de noviembre de 2019, disponible en https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/).Véase "Schrems I", Baker McKenzie Data Protection, diciembre de 2019, disponible en https://www.bakermckenzie.com/en/-/media/files/insight/publications/2019/12/schrems-ibackgroundv6.pdf para obtener información sobre los antecedentes de la decisión Schrems I. Para obtener información sobre la decisión en sí, véase https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN. Para obtener información sobre la decisión Schrems II de julio de 2020, véase https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

supone una amenaza para la adopción general y la seguridad de los servicios de cifrado y, por tanto, para la seguridad digital y la confianza en el comercio digital, la aprobación más amplia de leyes similares a la ley TOLA a nivel mundial amplificará el efecto adverso. Por otro lado, si las continuas impugnaciones que se plantean a esta ley y la preocupación por la amenaza que supone para la seguridad digital logran reducir de forma suficiente la probabilidad de que las facultades que ella otorga se pongan en práctica, los efectos adversos descritos anteriormente serán temporales y se evitarán.

En este momento es imposible prever cuál de estos escenarios es el más probable.

5.9. Conclusiones

Se puede considerar que las repercusiones económicas directas e indirectas de la ley TOLA se deben a los efectos que esta ley tiene en la reducción de la confianza en la ciberseguridad. Los costos directos asociados con responder a las solicitudes y notificaciones de la ley TOLA son probablemente la fuente más pequeña y menos importante de costos totales, ya que es probable que el número de destinatarios reales de esta ley sea pequeño.

Entre los efectos indirectos, sin embargo, se encontrarán el impacto que esta ley tendrá en todos los sectores de la economía cuando los posibles destinatarios directos (entre ellos todos los proveedores DCP) y las empresas y clientes con los que interactúan respondan al mayor riesgo cibernético que la ley plantease espera que estos costos totales se acumulen a lo largo del tiempo a medida que los efectos indirectos se propaguen en olas por el sector de las TIC de Australia, del sector de las TIC a otros sectores de la economía australiana, a las economías de otras partes del mundo y luego regresen a través de los bucles de retroalimentación que componen nuestro ecosistema económico mundial interconectado.

El estudio de Zúrich (2015)[124] y el informe de AustCyber (2020)[125] indican que los posibles daños indirectos resultantes de una amenaza a la confianza digital se medirían en miles de millones de dólares. Aunque eso proporciona solo una estimación de la magnitud de los costos agregados de la ley TOLA, es suficiente para demostrar que el potencial de que ocurran daños de consecuencias nacionales e incluso internacionales, es grande.

Existen datos empíricos parciales y observados que sugieren que el impacto de la ley TOLA puede dar lugar a importantes efectos indirectos. También hay argumentos cualitativos sólidos que sugieren que los efectos adversos potenciales (los costos netos) de la ley TOLA pueden ser realmente grandes. Sin embargo, no hay datos empíricos directos que permitan cuantificar esos efectos.

Hemos examinado las investigaciones disponibles al público y no hemos encontrado estudios empíricos pertinentes ni datos adecuados con los que formular estimaciones empíricas. Para hacer frente a esta dificultad, como parte de este proyecto hemos

[124]Véase la nota 92 *supra*.

[125]Véase la nota 93 *supra*.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

llevado a cabo una nueva investigación primaria en que se recogen las opiniones de grandes empresas tecnológicas multinacionales extranjeras y de un gran número y una amplia gama de empresas australianas sobre los efectos que la ley TOLA probablemente tendrá en sus actividades, sobre si creen que se ha experimentado alguno de los efectos señalados anteriormente y, en caso afirmativo, si han hecho alguna estimación monetaria del impacto.

Esta investigación tuvo dos componentes. En primer lugar, entrevistas detalladas por videoconferencia con los principales proveedores de comunicaciones multinacionales a quienes se aplica la ley TOLA. En segundo lugar, una encuesta anónima a un mayor número de proveedores de comunicaciones a quienes se aplica la ley TOLA y a empresas relacionadas afectadas por esa ley en Australia. Los resultados de este trabajo se exponen en el siguiente capítulo. En resumen, dichos resultados respaldan la conclusión de que el impacto económico neto de la ley TOLA ha sido negativo, y de que dicha ley plantea un riesgo de producir daños sustanciales en el futuro.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

6. Resultados de las investigaciones empíricas

Como parte de nuestro análisis del impacto económico de la ley TOLA, 1) realizamos entrevistas confidenciales detalladas por videoconferencia con nueve grandes empresas que operan en Australia y que están directamente afectadas por esta ley (es decir, que pueden ser consideradas como proveedores DCP cuyo personal puede ser destinatario de notificaciones de la ley TOLA), y 2) lanzamos una encuesta anónima entre empresas que operan en Australia y que pueden estar directa o indirectamente afectadas por la ley.

Como explicamos más adelante en el resumen de esta sección, los resultados de las entrevistas y de la encuesta anónima proporcionan un fundamento empírico (limitado) y son totalmente coherentes con nuestra evaluación del impacto económico de la ley TOLA. La información general que se obtuvo fue la siguiente:

1. Es de esperar que la ley TOLA tenga un impacto adverso en las empresas y sus clientes que sea de base amplia (*es decir*, que no se limite a las empresas de los sectores de las TIC).
2. La mayor parte de los daños previstos serán indirectos y estarán asociados a la amenaza que la ley TOLA supone para la percepción de los clientes y los socios del sector sobre la confianza digital.
3. Sigue habiendo una incertidumbre considerable sobre la ley TOLA y sus efectos.
4. Los datos empíricos directos sobre los costos (o beneficios) económicos son muy limitados, pero atribuimos ese hecho a lo siguiente: a) la falta de transparencia que caracteriza a las actividades relacionadas con la ley TOLA debido a las disposiciones de no divulgación; b) el escaso tiempo transcurrido desde la aprobación de esta ley y la controversia aún vigente que impide que los organismos LEIA apliquen la autoridad que esta ley les brinda, y c) la previsión de que los efectos sean probablemente indirectos y ocurran en el futuro.
5. Los limitados datos directos que observamos apoyan la conclusión de que los beneficios específicos de las empresas son probablemente pequeños, mientras que sus costos específicos pueden ser bastante grandes.[126]
6. Los datos empíricos disponibles no proporcionan una muestra lo suficientemente grande como para ser una base fiable que permita estimar el impacto económico agregado de la ley TOLA.

Entre las nueve empresas de tecnología de la información (TI) seleccionadas para las entrevistas detalladas había seis grandes empresas tecnológicas multinacionales con unos ingresos totales de algo más de un billón de dólares estadounidenses.[127] Las otras tres empresas eran un operador de telecomunicaciones y dos proveedores de servicios electrónicos australianos. De estos últimos, uno era un exportador cuyos propietarios

[126]Las entrevistas y la encuesta de nuestra investigación se centraron en los efectos que los encuestados conocían de primera mano.

[127]Para dar algo de perspectiva, esta estimación de ingresos totales equivale a casi tres cuartas partes del PIB australiano.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

son australianos y el otro un inversor extranjero e importador de servicios innovadores en Australia.

La encuesta anónima fue diseñada y lanzada por Clarity Strategic Research (Sídney), bajo la dirección de LECA.[128] La encuesta se lanzó durante diciembre de 2020 y obtuvo respuestas de 79 empresas. Aunque, como explicamos anteriormente, el impacto económico potencial de la ley TOLA abarca toda la economía y es razonable prever que los efectos económicos más significativos pueden ser indirectos, dirigimos la encuesta a los profesionales con experiencia en TI. Lo hicimos así porque es razonable esperar que los profesionales de las TI tengan más probabilidades de estar informados sobre esta ley y sobre las consecuencias de las políticas que afectan el uso de las tecnologías de cifrado. Dado el poco tiempo y los limitados recursos disponibles para llevar a cabo la encuesta, nos ayudaron a seleccionar a los destinatarios varias asociaciones comerciales australianas que aceptaron colaborar para que llegáramos a sus miembros, que en conjunto eran 16 000 profesionales de las TI. Entre esas asociaciones se encontraban la Red Australiana de Desarrollo de la Ciberseguridad (AustCyber), [129]la Asociación Australiana de la Industria de la Información (AIIA),[130] la Communications Alliance (Alianza de las Comunicaciones)[131] y la Asociación de Profesionales de las Tecnologías de la Información (ITPA).[132]

El enfoque de nuestra encuesta se basó en el de dos encuestas anteriores. La primera fue lanzada por AustCyber en 2018 en la víspera de la aprobación de la ley TOLA, mientras que la segunda fue lanzada por la Communications Alliance y la ITPA en 2019 después de que la ley había estado en vigor durante un año. Los resultados de la encuesta que se describen en el presente ofrecen otra instantánea de las percepciones y experiencias del sector dos años después de la aprobación de la ley TOLA. Un resultado clave que surge de este análisis es la notable similitud en cuanto a lo que los participantes del sector previeron que serían los efectos de la ley TOLA y lo que informan han sido sus experiencias y expectativas hacia el futuro. Como explicaremos más adelante, antes de la aprobación de la ley TOLA la mayoría de los encuestados esperaban que esta tuviera impactos económicos adversos, y esas expectativas se han hecho realidad, a la vez que se prevén más impactos adversos en el futuro.

Antes de analizar los resultados de nuestras entrevistas detalladas y de la encuesta, resumimos brevemente los resultados de las dos encuestas anteriores.

6.1. AustCyber (2018)

Antes de la aprobación de la ley TOLA en 2018, AustCyber contrató al Centro Internacional de Política Cibernética del Instituto de Política Estratégica de Australia (ASPI) para realizar una encuesta en línea de la industria australiana. La encuesta se

[128]Véase https://claritystrategicresearch.com.au/.

[129]Véase https://www.austcyber.com/.

[130]Véase https://www.aiia.com.au/.

[131]Véase https://www.commsalliance.com.au/.

[132]Véase https://www.itpa.org.au/.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

lanzó en noviembre de 2018 y los resultados se publicaron en diciembre de ese año.[133] La encuesta se presentó a 512 empresas de TI con operaciones en Australia y se recibieron 63 respuestas. En el 76 % de ellas los encuestados indicaron que el proyecto de ley les preocupaba, y algunos de los temas que plantearon como preocupaciones clave estaban relacionados con las percepciones y la falta de claridad con respecto a lo que esta ley podría exigir a las empresas.[134] Por ejemplo, el 57 % de los encuestados esperaba que la ley TOLA tuviera un impacto negativo en su negocio en Australia y, entre ellos, el 69 % esperaba que el impacto durara más de dos años.[135] Además, el 65 % de los encuestados que se autoidentificaron como exportadores esperaban que la ley TOLA tuviera un impacto negativo en las exportaciones de las empresas.[136]

El 76 % de los encuestados que declararon estar preocupados por la ley TOLA antes de su aprobación mencionaron las siguientes preocupaciones principales:[137]

Cuadro 6.1: Preocupaciones mencionadas en la encuesta de AustCyber	%
Falta de claridad en las definiciones	81 %
Posible conflicto entre las leyes australianas y las de otros países	73 %
Percepción de que el producto de su empresa fuera menos seguro	71 %
El costo de cumplir con las notificaciones	52 %
Erosión de la capacidad de la empresa	50 %
El impacto en los ingresos de la empresa	46 %
Reducción del atractivo de su empresa para posibles inversores	46 %
Posible pérdida de propiedad intelectual	44 %
Imposibilidad de ejecutar las sanciones cuando las empresas están establecidas en otros países pero prestan servicios a Australia	40 %
Daño a la marca de la empresa	40 %
Impacto en la cadena de suministro	38 %

[133]Véase ASPI (2018), "Perceptions survey: Industry Views on the Economic Implications of the Assistance and Access Bill 2018", encuesta financiada por AustCyber y ejecutada por ASPI, 22 de diciembre de 2018, disponible en https://www.austcyber.com/resources/perceptions-survey

[134]ASPI (2018), nota 7 supra, página 3.

[135]ASPI (2018), nota 7 supra, página 8.Solo el 7 % esperaba un efecto positivo, el 22 % no esperaba ningún efecto y el 14 % no estaba seguro.

[136]ASPI (2018), nota 7 supra, página 7. El 51 % de los encuestados declaró ser exportador y, entre ellos, solo el 4 % esperaba que la ley TOLA tuviera un impacto positivo, el 17 % esperaba que no tuviera ningún impacto, y el 13 % no estaba seguro del impacto que tendría en las exportaciones de la empresa.

[137]ASPI (2018), nota 7 *supra*, página 23.Los porcentajes se calculan a partir de las respuestas de las 48 empresas que indicaron que les preocupaba la ley TOLA.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Menor atractivo de su empresa para los posibles compradores	33 %
Reducción de la transparencia	33 %
Riesgo de perder clientes	31 %
Otras preocupaciones	23 %

Además, aunque en el proyecto de ley se indicaba que el Gobierno reembolsaría a las empresas los costos derivados del cumplimiento de la legislación, solo el 5 % de las empresas esperaban que se les reembolsaran totalmente los costos de cumplimiento relacionados con la ley TOLA.[138]

6.2. Encuesta de Innovación en Australia

La segunda encuesta fue realizada en 2019 por Innovation Australia (InnovationAus), una publicación independiente centrada en las políticas públicas australianas y en cuestiones relacionadas con la innovación empresarial, [139] StartupAus, un grupo sin fines de lucro que trabaja en la defensa de las empresas nuevas de la comunidad tecnológica en Australia,[140] la Communications Alliance y la ITPA. Los resultados se publicaron en diciembre de 2019, después de que la ley TOLA estuviera en vigor durante un año.[141]

La encuesta de InnovationAus se llevó a cabo del 5 al 12 de diciembre de 2019 para que coincidiera con el aniversario de la aprobación parlamentaria de esta ley. La encuesta recibió 70 respuestas de miembros de la Communications Alliance y la ITPA. Entre los encuestados, el 40 % informó que la ley TOLA había hecho que su empresa perdiera negocios, y el 51 % informó que dicha ley había tenido un impacto muy negativo en la reputación de las empresas tecnológicas australianas en los mercados mundiales.[142] Además, tras la aprobación de la ley TOLA, el 57 % de los encuestados pensaba que era menos probable que su organización realizara operaciones de desarrollo en Australia.[143]

[138]ASPI (2018), nota 7 *supra*, página 27.

[139]Véase https://www.innovationaus.com/.

[140]Véase https://startupaus.org/.

[141]InnovAus (2019), "Industry Pulse – Encryption Laws – Survey Results", publicado por InnovAus, StartupAus, Communications Alliance y la ITPA, 18 de diciembre de 2019, disponible en https://www.innovationaus.com/wp-content/uploads/2019/12/Encryption_Law_Survey_Results.pdf.

[142]InnovAus (2019), nota 176 *supra*, página 3. Además del 51 % que pensaba que el impacto sobre la reputación sería muy negativo, el 44 % pensaba que sería algo negativo, y solo el 3 % no esperaba ningún impacto (el 0 % señaló que el impacto sería positivo).Además, el 61% de los encuestados indicó que los clientes internacionales o nacionales habían expresado su preocupación por la ley TOLA.

[143]InnovAus (2019), nota 176 *supra*, página 4. Solo el 30 % esperaba que la ley TOLA no tuviera ningún impacto en los planes de desarrollo, y el 7 % esperaba que la ley TOLA

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

6.3. Resumen de las entrevistas cualitativas por videoconferencia

Como se ha descrito, realizamos entrevistas detalladas con nueve proveedores DCP que operaban en Australia y que tenían mucha experiencia en lo que respecta a cómo sus empresas se enfrentaban a la ley TOLA y a lo que pensaban que dicha ley significaba para las perspectivas de su negocio en Australia y más allá.

En todos los casos, los entrevistados tenían claro que se opondrían a cualquier petición del Gobierno que pretendiera inducirles a crear "puertas traseras" en sus procesos de seguridad. Cumplir con una solicitud de ese tipo debilitaría la seguridad que ya proporcionan y sería contrario a los compromisos públicos que han asumido con sus clientes y demás para proteger los derechos legales y la confidencialidad de los datos que controlan. Esto incluye las solicitudes que supusieran introducir una capacidad para romper o eludir el cifrado en algún producto que ya incluya esa capacidad o que ellos pudieran comercializar como si tuviera esa capacidad.

Todos los entrevistados también dejaron claro que ya cumplen con las solicitudes gubernamentales legítimas de acceso a los datos en virtud de las leyes y reglamentos australianos vigentes. Dicho esto, solo uno de los entrevistados indicó que consideraba que la ley TOLA mejoraba la situación legal con respecto al acceso a los datos por parte del Gobierno. Ese entrevistado consideraba que el refugio seguro que la ley TOLA concede a las empresas que responden a las solicitudes de acceso legítimo era una mejora con respecto a la situación anterior a dicha ley. Esto se debe a que consideraba que la ley TOLA proporciona una claridad adicional con respecto al proceso y a la protección de la responsabilidad en relación con el marco preexistente, que era más fragmentado y, por lo tanto, burocráticamente confuso y oneroso. El entrevistado dijo que, al menos, esa había sido su experiencia hasta ahora. Además, dijo que las disposiciones sobre el reembolso de los costos directos asociados a la respuesta a las solicitudes de la ley TOLA le habían funcionado bien hasta ahora. Esta única empresa encuestada que apoyó la ley TOLA no considera que esa ley suponga un riesgo potencial de tener que romper el cifrado, revelar códigos fuentes confidenciales o amenazar considerablemente el mensaje que su marca transmite a clientes empresariales o consumidores en Australia o en el extranjero.

Las otras ocho empresas que respondieron, sin embargo, tenían impresiones negativas sobre la ley TOLA. La veían como una amenaza potencial para la seguridad y el crecimiento de la demanda de la gama de servicios de información que ofrecían y como una ley que podría imponer mayores costos para hacer frente a esos riesgos de seguridad amplificados. Una razón clave de esta percepción fue la conclusión consensuada de que la amplitud de la ley TOLA, la insuficiencia de las disposiciones de supervisión y la ambigüedad de los términos en cuanto a lo que podría exigirse, así como la falta de transparencia, suponían una amenaza para la seguridad de los datos digitales en reposo o en movimiento. Los comentarios ofrecidos replicaban muchas de las mismas preocupaciones que se habían planteado en el marco de la consulta previa a la

mejorara sus planes de desarrollo en Australia. Además, el 51 % de los encuestados que declararon tener operaciones de desarrollo en Australia esperaban que la ley TOLA hiciera menos probable que aumentaran el empleo asociado a esas operaciones.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

aprobación de la ley TOLA[144] y que se habían reflejado en las revisiones posteriores, incluida la realizada por el Monitor Independiente de la Legislación sobre Seguridad Nacional (INSLM), que se publicó en julio de 2020.[145] Aunque el Gobierno australiano ha tratado de abordar muchas de estas preocupaciones como si fueran "mitos" infundados[146], en la revisión del INSLM se recomendaron una serie de reformas para fortalecer la supervisión de la ley TOLA y una mayor aclaración de algunos de los términos que en ella se utilizan.

A pesar de las continuas garantías del Gobierno de que no se abusaría de la ley TOLA y de que su aplicación se limitaría a un conjunto limitado de contextos graves, como los que están relacionados con la persecución de delitos atroces como el terrorismo internacional, el material de abuso sexual de menores o la trata de personas, muchos encuestados no estaban plenamente convencidos, habiendo sido testigos del fracaso de disposiciones de supervisión análogas aplicadas en otros contextos en Australia y en el extranjero. Preocupaba que la capacidad de ampliar la autoridad gubernamental para acceder a los datos confidenciales de forma ambigua requiriera una vigilancia continua (y un aumento de los costos para los proveedores DCP) que permitiera protegerse de los abusos y la desviación de los cometidos que las disposiciones de supervisión pretendían evitar.

Durante el período previo a la aprobación de la ley TOLA y en el primer período posterior a su aprobación, varios encuestados destacaron la preocupación de que esta ley pudiera colocarlos en una posición insostenible (debido a las disposiciones confusas y restrictivas respecto a qué información sobre las solicitudes de la ley TOLA los destinatarios de dichas solicitudes podrían compartir). Por ejemplo, existía la preocupación de que un empleado que recibiera una notificación de la ley TOLA no pudiera compartir dicha información con la alta dirección de su empresa sin enfrentarse a sanciones legales. Este escenario expondría a los empleados y a su empresa a una responsabilidad legal inaceptable.

Las conversaciones posteriores que los encuestados tuvieron con las autoridades reguladoras responsables de la ley TOLA les han llevado a descartar ese riesgo; sin embargo, el hecho de que haya surgido es indicativo de la confusión y la incertidumbre legal (y, por tanto, empresarial) que esta ley ha provocado desde que se propuso por primera vez y que continúa hasta hoy. Además, esta opinión podría cambiar si los

[144]Véase https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Submissions.

[145]Véase "Trust but Verify: a report concerning the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 and related matters", Australian Independent National Security Monitor (INSM), junio de 2020, disponible en https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf.

[146]Véase "Assistance and Access: Common myths and misconceptions", disponible en https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/myths-assistance-access-act.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

líderes y el personal de esas autoridades reguladoras cambiaran y tuvieran puntos de vista diferentes, ya que la opinión no está explícita en el texto de la ley.

Varios encuestados indicaron que, si les exigieran romper o eludir el cifrado de uno de sus productos, no podrían hacerlo de una manera selectiva dirigida a una persona, y por lo tanto se introduciría una vulnerabilidad sistémica que se extendería y afectaría negativamente a la seguridad del producto o el servicio destinado a otros usuarios. Esto ocurre sobre todo en el caso de los proveedores DCP que se basan en y prestan servicios de código abierto, o que dependen de cifrado y protecciones de seguridad que no son personalizables para cada usuario. Algunos proveedores DCP también pueden depender de servicios de este tipo, aunque ellos mismos no los proporcionen.

Si se exigiera a un proveedor de este tipo que rompiera la seguridad de un producto en el marco de la ley TOLA, ello podría constituir una amenaza existencial que obligaría a la empresa a retirar sus operaciones y ventas de productos o servicios de Australia. Algunos de los encuestados que reconocieron este riesgo comentaron que se opondrían a cumplir una solicitud de este tipo ejerciendo sus capacidades legales para apelar e impugnar la solicitud en la mayor medida posible, y que llevarían esos esfuerzos al nivel que fuera necesario.

Independientemente de que algunos escenarios extremos sobre cómo se podría abusar de la ley TOLA se hicieran o no se hicieran realidad, la sola percepción de que debilita la seguridad era una preocupación para los proveedores DCP Les preocupaba que las partes interesadas consideraran que sus productos y servicios eran menos seguros por estar sujetos a la ley TOLA, y que esta reducción de la seguridad pudiera dar lugar a filtraciones de datos y violaciones de la seguridad, no solo en Australia, sino también en otros lugares. La percepción de que la ley TOLA representa una mala política de seguridad fue vista por todos los encuestados, excepto uno, como una amenaza potencial para sus marcas que tendrían que vigilar y considerar cuidadosamente en sus futuros planes estratégicos de desarrollo y suministro de productos dotados de seguridad para su venta en Australia.

Varios encuestados señalaron que la ley TOLA, y las señales que esta daba sobre un clima potencialmente peor en lo que respecta a la interferencia del Gobierno y la regulación de los productos de seguridad, sería un factor que tendrían en cuenta en sus futuros planes de construcción de operaciones de desarrollo y ventas en Australia. Por ejemplo, sería un factor que tendrían en cuenta al seleccionar proveedores de servicios, como los centros de datos ubicados en Australia que estarían sujetos a esta ley. Además, dado que los destinatarios de las notificaciones de la ley TOLA están legalmente impedidos de compartir información sobre las notificaciones de la ley que reciben, sus clientes podrían no saber qué proveedores DCP han recibido dichas notificaciones y cuáles han sido sus respuestas.

Uno de los entrevistados es un proveedor DCP con sede en Australia que estaba creciendo rápidamente y buscaba expandirse a mercados internacionales que percibía como una oportunidad de mil millones de dólares. Después de la ley TOLA, el impacto adverso sobre la marca de sus productos lo llevó a abandonar los planes de expansión de sus ventas de exportación, lo que supuso la pérdida de una importante oportunidad

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

de crecimiento para esa empresa. El entrevistado señaló que perdieron negocios con clientes existentes que decidieron trasladar sus actividades a otros proveedores cuyos productos y servicios consideraban fuera del alcance de la ley TOLA.

Varios entrevistados señalaron que sus clientes habían planteado la preocupación por la seguridad de sus datos y que este era un factor que tenían que abordar al pensar en los planes futuros. Han tenido que tranquilizar a los clientes sobre la determinación que tienen de proteger la confidencialidad de los datos.

Con la excepción del caso mencionado anteriormente, la mayoría de los encuestados indicaron que los costos impuestos por la ley TOLA hasta el momento no habían sido excesivos, aunque la mayoría expresó su escepticismo respecto de que las disposiciones de reembolso de los gastos relacionados con la ley les fueran a inmunizar contra los efectos adversos en materia de costos. Los encuestados esperaban que los costos más importantes relacionados con la ley TOLA fueran probablemente indirectos (por ejemplo, el daño a la imagen de marca o la reducción de la demanda de los servicios o productos de los proveedores DCP australianos) más que directos (por ejemplo, los recursos de personal dedicados a cumplir con una solicitud específica).

La mayoría de los encuestados habían adoptado en los procesos protecciones adicionales relacionadas con la ley TOLA (con los costos correspondientes),[147] pero la mayoría no indicó que esta ley hubiera provocado ya un cambio en el diseño de sus ofertas de productos o en sus decisiones de contratación de personal con respecto a la localización de este en Australia o en el extranjero. Sin embargo, las protecciones adicionales de los procesos relacionadas con la ley TOLA indican que ese tipo de decisiones pueden convertirse en factores que se tomarán en cuenta en el futuro. Varios encuestados comentaron que la falta de datos sobre costos directos considerables ocasionados por la ley TOLA no era sorprendente a la luz de lo poco que la autoridad que la ley otorga se ha ejercido desde la aprobación.Lo atribuyeron al hecho de que los efectos de la nueva ley tardan en hacerse sentir, además de la continua controversia que ella ha generado y los llamamientos a modificarla.

Además, algunos consideraron que la ley TOLA era un paso desafortunado en una dirección que, si se generalizara con la aprobación de leyes imitadoras más amplias, amplificaría aún más la amenaza mundial que la ley TOLA ya supone para la seguridad de los datos.

Por último, a la luz de la decisión de julio de 2020 (Schrems II)[148] en la Unión Europea, que anuló la solución de refugio seguro llamada Privacy Shield que se había aprobado para proteger los acuerdos internacionales de intercambio de datos contra el incumplimiento de las leyes de protección de datos de la Unión Europea, varios

[147]Por ejemplo, varios encuestados mencionaron que esas protecciones del proceso suponían añadir otra capa de revisión del proceso para los planes de inversión y desarrollo de productos con el fin de abordar el posible impacto de la ley TOLA.

[148]Véase "The 'Schrems II' decision: EU-US data transfers in question", 16 de julio de 2020, disponible en https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

encuestados indicaron que les preocupaba que la ley TOLA pudiera suponer un riesgo para los flujos internacionales de datos hacia y desde Australia. Cualquier amenaza de este tipo, si resulta estar justificada, podría imponer costos considerables al buen funcionamiento de los mercados mundiales de datos y comunicaciones.

6.4. Resultados de la encuesta de LECA

6.4.1. Participantes en la encuesta en línea

Como se ha señalado anteriormente, la encuesta realizada por LECA con la ayuda de Clarity Strategic Research contó con 79 encuestados. Al igual que en las dos encuestas anteriores, los encuestados representaban a empresas que operan en Australia de múltiples sectores de la economía y que representan una gama de tamaños (medidos sobre la base de la cantidad de empleados o los ingresos):

- 54 de las empresas tenían su sede en Australia (68 % o 54/79).
- El tamaño de las empresas encuestadas oscilaba entre menos de 10 empleados (34 % o 27/79) y más de 500 empleados (28 % o 22/79).
- Una proporción considerable declaró que todos sus empleados estaban ubicados en Australia (46 % o 36/79), mientras que otra proporción menor, pero de todos modos considerable (27 % o 21/79) declaró que menos de la mitad de sus empleados estaban ubicados en Australia.
- Cuando se clasifican en función de los ingresos empresariales totales, el 43 % (o 34/79) de las empresas eran pequeñas (<5 millones de dólares australianos), mientras que el 13 % (o 10/79) son grandes (>5000 millones de dólares australianos).
- No es de extrañar que la mayoría de las empresas encuestadas se dedicaran a negocios relacionados con las tecnologías de la información (54 % o 43/79), y que muchas de ellas se dedicaran a varias líneas de negocio relacionadas con las tecnologías de la información.
- Entre las empresas que no estaban relacionadas con las TI (43 % o 34/79), los encuestados dijeron que sus empresas se dedicaban a los servicios (44 % o 15/34), la administración pública y la seguridad (18 % o 6/34) o a otros sectores (38 % o 13/34), que iban desde la industria manufacturera hasta la educación.[149]
- Los cargos de los encuestados indicaban que prácticamente todos, si no todos, se dedicaban a tareas relacionadas con las tecnologías de la información, lo que no es de extrañar teniendo en cuenta a quién se envió la encuesta.

Estos resultados se resumen en los siguientes cuadros:

Cuadro 6.2: QA1i: ¿Dónde tiene su sede la empresa?

	Número	%
Australia	54	68 %
Otro sitio	23	29 %

[149] Dos (3 % de los 79) encuestados no respondieron.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

No responde	2	3 %
Total	79	100 %

Cuadro 6.3: QA3i: ¿Cuántos empleados tiene en total (aproximadamente)?		
Total de empleados (n.º)	Número	%
No responde	10	13 %
0-10	27	34 %
11-499	20	25 %
Más de 500	22	28 %
Total	79	100 %

Cuadro 6.4:Proporción de empleados en Australia	Número	%
No responde	12	15 %
10 % o menos	16	20 %
10<%<100	15	19 %
100 %	36	46 %
Total	79	100 %
0 %	4	5 %
<50 %	21	27 %

Cuadro 6.5:¿La empresa se dedica a la TI?		
Sector	Número	%
No responde	2	3 %
Sector de la TI	43	54 %
No se dedica a la TI	34	43 %
Total	79	100 %

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Cuadro 6.5B: Ubicación de la sede y línea de negocio				
	Línea de negocio			
Ubicación de la sede	TIC	No se dedica a las TIC	No responde	Total
Australia	31 (39 %)	23 (29 %)	0 (0 %)	54 (68 %)
No se encuentra en Australia	12 (15 %)	10 (13 %)	1 (1 %)	23 (29 %)
No responde	0 (0 %)	1 (1 %)	1 (1 %)	2 (3 %)
Total	43 (54 %)	34 (43 %)	2 (3 %)	79 (100 %)

Cuadro 6.6: Líneas de negocio de TI		
	Código	Número
Operaciones, equipos y servicios de redes de telecomunicaciones	1-3, 10,13	18
Proveedor de servicios de Internet, portales de búsqueda en la red, otros servicios de Internet	4-5	7
Servicios de almacenamiento electrónico	6	6
Desarrollador de software, proveedor	7-8	25
Fabricación y venta de equipos informáticos	9-12, 13-14	17
Otras TI (especificar)	97	13
No sabe, no responde	98-99	3
Total		89

Cuadro 6.7: Líneas de negocio de las empresas no informáticas			
Sector	Código	Número	%
Servicios	10, 12, 18	12	46 %
Administración pública y seguridad	14	6	23 %
Otros (fabricación, construcción, educación)	3, 5, 7, 15	8	31 %
Total		26	100 %

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

6.4.2. Importancia de los servicios de cifrado para las empresas

Los encuestados indicaron de forma abrumadora que los servicios y capacidades de cifrado eran muy importantes o bastante importantes para sus empresas de múltiples maneras, tanto en lo que respecta a las comunicaciones (datos en movimiento) como en lo que atañe a los datos almacenados (datos en reposo) para su uso interno y en las relaciones comerciales con los proveedores y clientes. El 96 % (o 76/79) de los encuestados indicaron que los servicios de cifrado eran muy importantes o bastante importantes para al menos una categoría de uso.[150] Además, el cuadro 6.8 demuestra que más del 85 % (o 67/79) de los encuestados consideraban que los servicios y capacidades de cifrado eran muy o bastante importantes para la mayoría de los contextos de uso considerados por separado, y de ellos, más del 53 % (o 42/79) respondieron que los servicios y capacidades de cifrado eran muy importantes.

Además, los encuestados indicaron que adquirían las capacidades de cifrado necesarias de diversas maneras: a veces diseñándolas internamente y otras recurriendo proveedores externos de productos y servicios de uso general (es decir, las capacidades de cifrado pueden ser una característica integrada en un producto o servicio de TI) o a proveedores de servicios de cifrado especializados. Los métodos de adquisición de las capacidades pueden variar según el uso (es decir, datos en movimiento o datos en reposo, uso interno, con proveedores o con clientes). Algunos encuestados utilizaban diferentes enfoques en los distintos contextos y, en ocasiones, utilizaban múltiples enfoques en contextos concretos. Aunque los resultados de nuestra encuesta anónima no nos permiten rastrear las codependencias entre las empresas encuestadas (es decir, algunos encuestados pueden ser consumidores y/o proveedores de servicios de cifrado para otros encuestados), está claro que el uso de las capacidades y servicios de cifrado está muy extendido en las diferentes empresas de TI y en las empresas que no se dedican a la TI que participaron en nuestra encuesta.

Estos resultados son indicativos de lo mucho que se depende de los servicios de cifrado en todo tipo de empresas de la economía y también son indicativos de la red potencialmente enmarañada de repercusiones que pueden transmitirse a través de las empresas de Australia y del mundo si las capacidades de cifrado de solo un subconjunto de empresas se ven amenazadas. La propagación de estos efectos adversos a través de la economía podría amplificar y aumentar el impacto directo adverso. Lamentablemente, el reducido número de respuestas que recibimos en la encuesta y la falta de mejores datos sobre el comercio de bienes y servicios que dependen de las capacidades de cifrado no nos permiten estimar ni modelar las formas en que los efectos directos e indirectos podrían repercutir en la economía.

[150] Solo un encuestado indicó que no utilizaba servicios de cifrado, solo uno indicó que los servicios de cifrado no eran muy ni bastante importantes para al menos una de las categorías de uso, y solo otro encuestado prefirió no responder en relación con todas las categorías de uso, lo que representa solo un 4 % (o 3/76) del total de encuestados.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Cuadro 6.8: ¿Qué importancia tienen los servicios y capacidades de cifrado para su empresa?

	Muy importante o bastante importante	Poco (nada) importante o no se utilizan	No sabe o no contesta	Total	% de la col. (a) que respondió "muy importante"
	(a)	(b)	(c)	(a)+(b)+(c)	
Comunicaciones internas de la empresa	85 %	14 %	1 %	100 %	53 %
Datos internos almacenados de la empresa	92 %	6 %	1 %	100 %	73 %
Comunicaciones (datos en movimiento) con proveedores	90 %	9 %	1 %	100 %	59 %
Datos almacenados (datos en reposo) en manos de proveedores	91 %	6 %	3 %	100 %	70 %
Comunicaciones (datos en movimiento) con los clientes	91 %	8 %	1 %	100 %	65 %
Datos almacenados (datos en reposo) en los productos/servicios que la empresa proporciona a los clientes	87 %	11 %	1 %	100 %	71 %

6.4.3. Conocimiento de la ley TOLA, familiaridad y actitud hacia ella

De los 79 encuestados, 58 indicaron que habían oído hablar de la ley TOLA. Esos 58 encuestados pertenecían en su mayoría a empresas con sede en Australia (68 %) cuya actividad principal se basa en las tecnologías de la información (60 % o 35/58); el 40 % (o 23/58) de los encuestados indicaron que estaban muy o bastante familiarizados con la ley TOLA.

Cuadro 6.9: Conocimiento de la ley TOLA por parte de los encuestados, según la ubicación de la sede

	La conoce	No la conoce/ No responde	Total
Australia	42 (53 %)	12 (15 %)	54 (68 %)
No se encuentra en Australia	16 (20 %)	9 (11 %)	25 (32 %)

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Total	**58 (73 %)**	21 (27 %)	79 (100 %)

Cuadro 6.10: Conocimiento de la ley TOLA por parte de los encuestados, según el tipo de empresa

	La conoce	No la conoce/ No responde	Total
TI	35 (44 %)	8 (10 %)	43 (54 %)
No se dedica a la TI	23 (29 %)	13 (16 %)	36 (46 %)
Total	**58 (73 %)**	21 (27 %)	79 (100 %)

Cuadro 6.11: Nivel de familiaridad con la ley TOLA

Muy/bastante familiarizado	23	40 %
No muy familiarizado	29	50 %
No familiarizado	4	7 %
No responde	2	3 %
Total	58	100 %

6.4.4. Actitud de los encuestados hacia la ley TOLA

Entre los que conocían la ley TOLA, una gran proporción (62 % o 36/58) tenía una opinión muy negativa o bastante negativa respecto a las modificaciones que introdujo en la *Ley de Telecomunicaciones de 1997*. Solo el 10 % (o 6/58) tenía una opinión positiva. En el siguiente gráfico se resume la familiaridad con la ley TOLA y las actitudes hacia ella de los 58 encuestados que conocían la Ley.

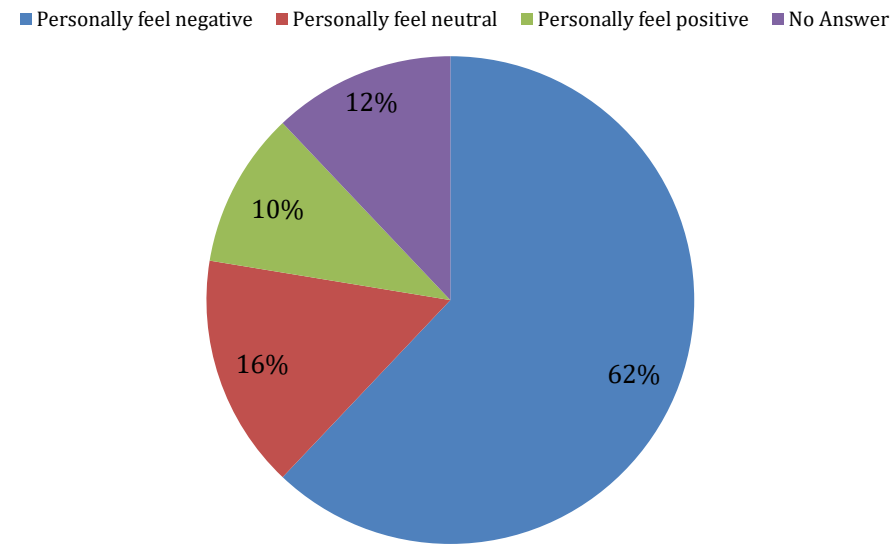
Cuadro 6.12: Opinión de los encuestados acerca de la ley TOLA

Muy positiva	0 %
Bastante positiva	10 %
Neutra	16 %
Bastante negativa	26 %
Muy negativa	36 %
No responde	12 %

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Total	100 %

Figura 6.1
De los 58 casos que conocían la Ley TOLA



Cuando se les preguntó a los encuestados cómo pensaban que la ley TOLA afectaba diversos asuntos relacionados con las políticas, la mayoría de ellos creía que la ley TOLA había tenido un impacto adverso en las relaciones exteriores de Australia y en la seguridad e integridad de los datos digitales, y, lo que es más importante aquí, un impacto adverso en la economía del país. Los encuestados tenían sentimientos encontrados respecto al impacto de esta ley en la seguridad nacional de Australia. El impacto positivo más significativo de la ley TOLA (pero de todos modos muy inferior a la mayoría) fue en la aplicación del derecho penal en el país (véase el cuadro 6.13).

Cuadro 6.13: Expectativas de los encuestados sobre el impacto de la ley TOLA en diversos asuntos

	Negativo	Sin impacto	Positivo	No responde	Total
La seguridad nacional de Australia	33 %	22 %	24 %	21 %	100 %
Las relaciones exteriores de Australia	53 %	7 %	9 %	31 %	100 %
El bienestar económico nacional de Australia	52 %	10 %	16 %	22 %	100 %
La seguridad e integridad de la información que se procesa, almacena o comunica por medios electrónicos o similares	59 %	12 %	10 %	19 %	100 %

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

La aplicación del derecho penal en Australia	12 %	29 %	34 %	24 %	100 %
La aplicación del derecho penal en otros países	10 %	50 %	7 %	33 %	100 %

6.4.5. Impacto de la ley TOLA en la empresa de los encuestados

Cuando se les preguntó si la ley TOLA había incidido en sus empresas de diversas maneras, el 41 % de los encuestados respondió que la ley TOLA había incidido en sus empresas de una o varias maneras (cuadro 6.14A), y, en promedio, el 18 % de los encuestados que conocían la ley (58 de los 79) respondieron que dicha ley había incidido en sus empresas en relación con cada una de las categorías (cuadro 6.14B).

Tabla 6.14A: Empresas que declararon que la ley había impactado en varias categorías

Sin impacto	59 %
Una categoría de impacto	5 %
Dos o más categorías de impacto	36 %

Cuadro 6.14B: ¿Ha tenido la ley TOLA un impacto en la empresa?

	Sí, ha tenido un impacto	Sin impacto	No sabe	No responde	Total
Ventas	16 %	47 %	31 %	7 %	100 %
Reputación de la empresa	14 %	45 %	36 %	5 %	100 %
Relaciones con los proveedores	16 %	52 %	28 %	5 %	100 %
Relaciones con los clientes	16 %	48 %	31 %	5 %	100 %
Decisiones de marketing, desarrollo de productos	31 %	43 %	22 %	3 %	100 %
Gastos de explotación y de capital (OPEX/CAPEX)	21 %	45 %	33 %	2 %	100 %
Otras áreas de la empresa	21 %	40 %	36 %	3 %	100 %
Promedio	19 %	46 %	31 %	4 %	

Cuando a los encuestados se les preguntó además si los efectos habían sido positivos o negativos hasta la fecha y sobre las expectativas que tenían en cuanto a los efectos en

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

el futuro en una serie de asuntos empresariales, los encuestados que habían observado un impacto destacaron una vez más la amplia gama de efectos (véanse los cuadros 6.15A, 6.15B y 6.15C). Aunque la mayoría de las empresas no declaró haber sufrido un impacto (cuadro 6.14), entre las que sí lo hicieron en una categoría, las que sufrieron un impacto negativo superan a las que experimentaron un impacto positivo en todas las categorías. Además, se prevé que los efectos negativos continúen en el futuro en las 15 áreas de impacto y, en lo que respecta a la gran mayoría de los efectos negativos (11 de las 15 áreas de impacto o el 73 %) hay más empresas que esperan efectos negativos en el futuro que las que han experimentado efectos negativos hasta la fecha (cuadro 6.15C): el porcentaje aumenta del 18 % al 20 %. Por tanto, las expectativas de los encuestados son coherentes con la opinión de que los impactos económicos continuarán, o incluso empeorarán, en el futuro. Por último, en general, el 36 % (o 21/58) de las empresas experimentaron un impacto negativo en su negocio en una o varias de las áreas hasta la fecha y esperan que eso ocurra en el futuro (cuadro 6.15D).

Cuadro 6.15A: Empresas que han experimentado un impacto hasta la fecha (desde 2018)

Porcentaje de empresas que han experimentado un impacto	Negativo	Sin impacto	Positivo	No responde	Total
Ingresos totales a nivel global	10 %	12 %	3 %	74 %	100 %
Ingresos por servicios de cifrado a nivel global	9 %	16 %	2 %	74 %	100 %
Costos operativos globales de la empresa, incluidos el cumplimiento de la normativa y la corrección	16 %	14 %	2 %	69 %	100 %
Inversión global en servicios de cifrado	21 %	9 %	3 %	67 %	100 %
Nivel global de la inversión y financiación	17 %	9 %	3 %	71 %	100 %
Gasto global en estrategia de innovación en relación con los servicios de cifrado	21 %	7 %	5 %	67 %	100 %
Inversión global en el desarrollo de nuevos productos	22 %	7 %	2 %	69 %	100 %
Gasto global en investigación y desarrollo	19 %	9 %	3 %	69 %	100 %
Valor global de la marca o la reputación	19 %	10 %	3 %	67 %	100 %
Valor global de otra propiedad intelectual (patentes, derechos de autor, etc.)	14 %	14 %	2 %	71 %	100 %
Capacidad global para atraer a personal de buena calidad para trabajar en la empresa	12 %	17 %	2 %	69 %	100 %

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Capacidad global para comprar los productos y servicios de cifrado que la empresa necesita	10 %	17 %	3 %	69 %	100 %
Confidencialidad, seguridad o privacidad de los servicios de cifrado a nivel global	28 %	9 %	2 %	62 %	100 %
Entorno de riesgo para la empresa a nivel global	36 %	2 %	2 %	60 %	100 %
Niveles de empleo en servicios de cifrado a nivel global	14 %	9 %	3 %	74 %	100 %

Cuadro 6.15B: Empresas que esperan recibir el impacto en el futuro

Porcentaje de empresas que han experimentado un impacto	Negativo	Sin impacto	Positivo	No responde	Total
Ingresos totales a nivel global	14 %	7 %	7 %	72 %	100 %
Ingresos por servicios de cifrado a nivel global	14 %	9 %	2 %	76 %	100 %
Costos operativos globales de la empresa, incluidos el cumplimiento de la normativa y la corrección	21 %	10 %	2 %	67 %	100 %
Inversión global en servicios de cifrado	28 %	9 %	0 %	64 %	100 %
Nivel global de la inversión y financiación	19 %	9 %	3 %	69 %	100 %
Gasto global en estrategia de innovación en relación con los servicios de cifrado	24 %	9 %	0 %	67 %	100 %
Inversión global en el desarrollo de nuevos productos	21 %	7 %	3 %	69 %	100 %
Gasto global en investigación y desarrollo	19 %	12 %	2 %	67 %	100 %
Valor global de la marca o la reputación	19 %	9 %	5 %	67 %	100 %
Valor global de otra propiedad intelectual (patentes, derechos de autor, etc.)	16 %	14 %	0 %	71 %	100 %
Capacidad global para atraer a personal de buena calidad para trabajar en la empresa	14 %	16 %	5 %	66 %	100 %
Capacidad global para comprar los productos y servicios de cifrado que la empresa necesita	19 %	12 %	2 %	67 %	100 %
Confidencialidad, seguridad o privacidad de los servicios de cifrado a nivel global	29 %	5 %	3 %	62 %	100 %

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

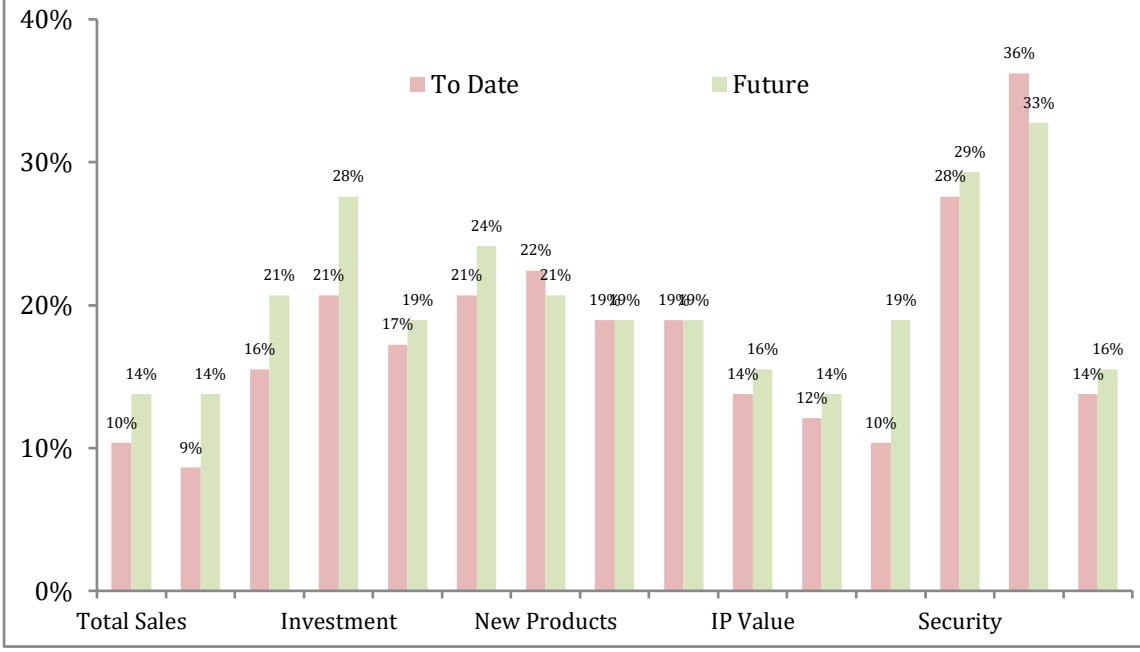
Entorno de riesgo para la empresa a nivel global	33 %	2 %	2 %	64 %	100 %
Niveles de empleo en servicios de cifrado a nivel global	16 %	7 %	3 %	74 %	100 %

Cuadro 6.15C: Empresas que han recibido a la fecha o esperan recibir en el futuro un impacto negativo de la ley TOLA en su negocio

Porcentaje de empresas que han experimentado un impacto	Hasta la fecha	En el futuro
Ingresos totales a nivel global	10 %	14 %
Ingresos por servicios de cifrado a nivel global	9 %	14 %
Costos operativos globales de la empresa, incluidos el cumplimiento de la normativa y la corrección	16 %	21 %
Inversión global en servicios de cifrado	21 %	28 %
Nivel global de la inversión y financiación	17 %	19 %
Gasto global en estrategia de innovación en relación con los servicios de cifrado	21 %	24 %
Inversión global en el desarrollo de nuevos productos	22 %	21 %
Gasto global en investigación y desarrollo	19 %	19 %
Valor global de la marca o la reputación	19 %	19 %
Valor global de otra propiedad intelectual (patentes, derechos de autor, etc.)	14 %	16 %
Capacidad global para atraer a personal de buena calidad para trabajar en la empresa	12 %	14 %
Capacidad global para comprar los productos y servicios de cifrado que la empresa necesita	10 %	19 %
Confidencialidad, seguridad o privacidad de los servicios de cifrado a nivel global	28 %	29 %
Entorno de riesgo para la empresa a nivel global	36 %	33 %
Niveles de empleo en servicios de cifrado a nivel global	14 %	16 %
Promedio (de las filas)	18 %	20 %

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Figura 6.2
Impacto Negativo Pasado y Futuro
% de firmas Australianas y Extranjeras



Cuadro 6.15D: Número de categorías en que se ha recibido un impacto negativo o se espera recibirlo		
Número de efectos negativos (a nivel global y en Australia) Total de casos que conocían la ley TOLA = 58	Número de casos hasta la fecha	Número de casos en el futuro
0 (incluye No responde) en todas las categorías	37 (64 %)	37 (64 %)
1 de 15 categorías	0 (0 %)	0 (3 %)
2 de 15 categorías	2 (3 %)	0 (0 %)
3 de 15 categorías	2 (3 %)	2 (2 %)
4 o más de 15 categorías	17 (29 %)	18 (31 %)
Total	58 (100 %)	58 (100 %)
Impacto negativo en al menos 1 de las 15 categorías	21 (36 %)	21 (36 %)

6.5. Conclusiones de la investigación empírica

En resumen, en las entrevistas a las empresas de TIC y en las respuestas a nuestras encuestas se mencionaron los riesgos económicos hipotéticos que esbozamos en el capítulo 5. En ambos casos, la opinión de que la ley TOLA supone una amenaza

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

económica para las perspectivas de negocio de las empresas de TIC y para la economía australiana y mundial se vio respaldada en los hechos.

Los datos también fueron indicativos de la falta de datos empíricos que hay hasta el momento sobre costos (y, menos aún, sobre beneficios) que puedan atribuirse directamente a la ley TOLA. Sin embargo, esta falta de datos empíricos *no* es prueba de que no haya ningún efecto. Aunque valía la pena averiguar si había datos empíricos de que se hubieran generado costos desde 2018, nos habría sorprendido encontrar esos datos dada la muy limitada actividad relacionada con esta ley sobre la que se ha informado, y dados los cuestionamientos y controversias que persisten y hacen que el futuro de la ley TOLA sea incierto. Además, las normas de no divulgación y el secreto que rodea la actividad relacionada con la ley TOLA constituyen un gran obstáculo para la recopilación de datos sobre las repercusiones económicas de esta ley.No obstante, los escasos datos recopilados son reveladores. El hecho de que el único entrevistado en cuya opinión el impacto de la ley TOLA sería mayoritariamente favorable considerara que su principal efecto era la racionalización de la legislación existente sobre el acceso legal a los datos digitales por parte del Gobierno es coherente con la opinión de que los beneficios directos de esta ley son probablemente pequeños. Por el contrario, el único encuestado que pudo cuantificar el daño económico que padeció como resultado de la ley TOLA estimó que ese daño era del orden de los mil millones de dólares en ingresos de exportación perdidos, lo que es coherente con la expectativa de que los posibles daños económicos directos pueden ser bastante grandes.

Por otra parte, el tamaño de la encuesta anónima y los desafíos que dependen de los datos de la encuesta imponen a la hora de inferir los efectos económicos limitan nuestra capacidad para cuantificar la magnitud de dichos efectos. Sin embargo, los resultados son coherentes con lo observado en las encuestas anteriores y demuestran que las preocupaciones que existían antes de la aprobación de la ley TOLA siguen siendo preocupaciones hoy en día; y, si esas preocupaciones se hacen realidad, los impactos económicos adversos podrían ser amplios.

Las respuestas a la encuesta ponen de manifiesto que los impactos negativos son ampliamente compartidos tanto por las empresas de TIC como por las que no lo son, y que muchas empresas aún no comprenden la amenaza que la ley TOLA supone para su negocio.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

7. Apéndices sobre acrónimos, abreviaturas y definiciones

7.1. Acrónimos, abreviaturas y definiciones

- Ley ASIO. Ley de la Organización de Inteligencia de Seguridad Australiana de 1979
- ASIO. La Organización de Inteligencia de Seguridad Australiana, que está incluida en la lista de organismos gubernamentales australianos que pueden emitir solicitudes o notificaciones en el marco de la ley TOLA.
- Cth significa Commonwealth, y se utiliza para distinguir la legislación del Commonwealth de la legislación estatal.
- DCP. Proveedor de comunicaciones designado. Los proveedores DCP son un concepto amplio en el marco de la ley TOLA, que abarca las entidades a las que se aplica esta ley; véase la lista de categorías de proveedores DCP en el artículo 317C de la ley TOLA, que se reproduce más adelante.
- INSLM. Monitor Independiente de la Legislación sobre Seguridad Nacional (vínculo), que publicó un informe de revisión de la ley TOLA el 20 de julio de 2020 (vínculo).
- PJCIS. Comisión Parlamentaria Mixta de Inteligencia y Seguridad, que realizó una investigación sobre la ley TOLA antes de su promulgación, y desde entonces ha realizado otras revisiones.
- TOLA. La *Ley de Modificación de la Legislación sobre Telecomunicaciones y otras Leyes (Asistencia y Acceso)* , también conocida como ley del cifrado o ley sobre asistencia y acceso (vínculo). La ley TOLA ha sido objeto de revisión por parte del INSLM. La ley TOLA consta de 5 anexos: nuestro trabajo se centra en el anexo 1 (relacionado con la eliminación y elusión del cifrado o el acceso excepcional).
- TAR, TAN y TCN son tres tipos de notificaciones que pueden emitirse en el marco de la ley TOLA, ya sea de forma oral o por escrito (317H).
  - TAR = Solicitud de Asistencia Técnica, mediante la cual se puede pedir a un proveedor DCP que emprenda acciones voluntarias (317L).
  - TAN = Notificación de Asistencia Técnica, mediante la cual se puede ordenar un proveedor DCP que proporcione asistencia técnica (317M).
  - TCN = Notificación de Capacidad Técnica, mediante la cual se puede ordenar a un proveedor DCP que lleve a cabo acciones específicas, entre ellas hacer posible una capacidad (317T)
- TIA. Ley de Telecomunicaciones (Interceptación y Acceso) de 1979.
- TA. *Ley de Telecomunicaciones de 1997*.
- Ley SD. Ley de Dispositivos de Vigilancia de 2004 (ley SD).
- MACMA. Ley de Asistencia Recíproca en Materia Penal de 1987.
- Ley ASIO. Ley de la Organización de Inteligencia de Seguridad Australiana de 1979

7.2. Definiciones de la ley TOLA

317B Definiciones

la protección electrónica incluye:

a) la autenticación, y

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

b) el cifrado

tecnología objetivo:

(a) a los efectos de esta Parte, un servicio de telecomunicaciones concreto, en la medida en que el servicio sea utilizado, o es probable que sea utilizado, (ya sea directa o indirectamente) por una persona concreta, es una ***tecnología objetivo*** que está relacionada con dicha persona; y

(b) a los efectos de esta Parte, un servicio electrónico concreto, en la medida en que el servicio sea utilizado, o es probable que sea utilizado, (ya sea directa o indirectamente) por una persona concreta, es una ***tecnología objetivo*** que está relacionada con dicha persona;

(c) a los efectos de esta Parte, un software concreto instalado, o que se vaya a instalar, en:

(i) una computadora concreta, o

(ii) un equipo concreto;

que sea utilizado, o es probable que sea utilizado, (ya sea directa o indirectamente) por una persona concreta, es una ***tecnología objetivo*** que está relacionada con dicha persona, y

(d) a los efectos de esta Parte, una actualización concreta de software que se ha instalado en:

(i) una computadora concreta, o

(ii) un equipo concreto;

que sea utilizado, o es probable que sea utilizado, (ya sea directa o indirectamente) por una persona concreta, es una ***tecnología objetivo*** que está relacionada con dicha persona, y

(e) a los efectos de esta Parte, un equipo concreto del cliente que sea utilizado, o es probable que sea utilizado, (ya sea directa o indirectamente) por una persona concreta, es una ***tecnología objetivo*** que está relacionada con dicha persona;

(f) a los efectos de esta Parte, un dispositivo de procesamiento de datos concreto que sea utilizado, o es probable que sea utilizado, (ya sea directa o indirectamente) por una persona concreta, es una ***tecnología objetivo*** que está relacionada con dicha persona.

A efectos de los apartados (a), (b), (c), (d), (e) y (f), es irrelevante que la persona pueda ser identificada.

Proveedores de comunicaciones designados

317C Proveedor de comunicaciones designado, etc.

A los efectos de esta Parte, en el cuadro siguiente se definen:

(a) ***un proveedor de comunicaciones designado***; y

(b) las ***actividades*** que un proveedor de comunicaciones designado puede hacer.

Proveedor de comunicaciones designado y actividades que puede hacer

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Número	Una persona es un proveedor de comunicaciones designado si...	... y las actividades que la persona puede hacer son las siguientes: ...
1	la persona es un operador o proveedor de servicios de telecomunicaciones	(a) la operación por parte de la persona de redes o instalaciones de telecomunicaciones en Australia; o (b)
2	la persona es un intermediario de servicios de telecomunicaciones que organiza la prestación de servicios de telecomunicaciones enumerados por parte de un proveedor de servicios de telecomunicaciones	(a) la organización por parte de la persona de la prestación de servicios de telecomunicaciones enumerados por parte de un proveedor de servicios de telecomunicaciones; o (b) la operación por parte del proveedor de servicios de telecomunicaciones de redes o instalaciones de telecomunicaciones en Australia, o (c) la prestación por parte del proveedor de servicios de telecomunicaciones de los servicios de telecomunicaciones enumerados.
3	la persona presta un servicio que facilita, o es auxiliar o incidental a, la prestación de un servicio de telecomunicaciones enumerado	la prestación por parte de la persona de un servicio que facilita, o es auxiliar o incidental a, la prestación de un servicio de telecomunicaciones enumerado.
4	la persona presta un servicio electrónico que tiene uno o varios usuarios finales en Australia	la prestación por parte de la persona de un servicio electrónico que tiene uno o varios usuarios finales en Australia.
5	la persona presta un servicio que facilita, o es auxiliar o incidental a, la prestación de un servicio electrónico que tiene uno o varios usuarios finales en Australia	la prestación por parte de la persona de un servicio que facilita, o es auxiliar o incidental a, la prestación de un servicio electrónico que tiene uno o varios usuarios finales en Australia.
6	la persona diseña, suministra o actualiza software que se utiliza, es para utilizar o es probable que se utilice en relación con: (a) un servicio de telecomunicaciones enumerado; o (b) un servicio electrónico que tenga uno o varios usuarios finales en Australia.	(a) el diseño por parte de la persona de un software de este tipo; o (b) el suministro por parte de la persona de un software de este tipo, o (c) la actualización por parte de la persona de un software de este tipo.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

7	la persona fabrica, suministra, instala, mantiene u opera una instalación	(a) la fabricación por parte de la persona de una instalación para ser utilizada, o que es probable que sea utilizada, en Australia; o (b) el suministro por parte de la persona de una instalación para ser utilizada, o que es probable que sea utilizada, en Australia; o (c) la instalación por parte de la persona de una instalación en Australia; o (d) el mantenimiento por parte de la persona de una instalación en Australia, o (e) la operación por parte de la persona de una instalación en Australia.

Proveedor de comunicaciones designado y actividades que puede hacer		
Número	**Una persona es un proveedor de comunicaciones designado si...**	**... y las actividades que la persona puede hacer son las siguientes: ...**
8	la persona fabrica o suministra componentes para ser utilizados, o que es probable que sean utilizados, en la fabricación de una instalación para ser utilizada, o que es probable que sea utilizada, en Australia	(a) la fabricación por parte de la persona de un componente de este tipo, o (b) el suministro por parte de la persona de un componente de este tipo.
9	la persona conecta una instalación a una red de telecomunicaciones en Australia	la conexión por parte de la persona de una instalación a una red de telecomunicaciones en Australia.
10	la persona fabrica o suministra equipos de clientes para ser utilizados, o que es probable que sean utilizados, en Australia	(a) la fabricación por parte de la persona de un equipo de cliente de este tipo, o (b) el suministro por parte de la persona de un equipo de cliente de este tipo.
11	la persona fabrica o suministra componentes para ser utilizados, o que es probable que sean utilizados, en la fabricación de equipos de clientes para ser utilizados, o que es probable que sean utilizados, en Australia	(a) la fabricación por parte de la persona de un componente de este tipo, o (b) el suministro por parte de la persona de un componente de este tipo.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

12	la persona: (a) instala o mantiene equipos de clientes en Australia, y (b) lo hace de una manera que no es en calidad de usuario final del equipo.	(a) una instalación de este tipo de equipos de clientes por parte de la persona, o (b) un mantenimiento de este tipo de equipos de clientes por parte de la persona.
13	la persona: (a) conecta equipos de clientes a una red de telecomunicaciones en Australia, y (b) lo hace de una manera que no es en calidad de usuario final del equipo.	una conexión de este tipo por parte de la persona de equipos de clientes a una red de telecomunicaciones en Australia.
14	la persona es una sociedad constitucional que: (a) fabrica; o (b) suministra; o (c) instala; o (d) mantiene; dispositivos de procesamiento de datos.	(a) la fabricación por parte de la persona de dispositivos de procesamiento de datos para ser utilizados, o que es probable que sean utilizados, en Australia; o (b) el suministro por parte de la persona de dispositivos de procesamiento de datos para ser utilizados, o que es probable que sean utilizados, en Australia; o (c) la instalación por parte de la persona de dispositivos de procesamiento de datos en Australia; o (d) el mantenimiento por parte de la persona de dispositivos de procesamiento de datos en Australia.

Proveedor de comunicaciones designado y actividades que puede hacer		
Número	**Una persona es un proveedor de comunicaciones designado si...**	**... y las actividades que la persona puede hacer son las siguientes: ...**

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

15	la persona es una sociedad constitucional que: (a) diseña; o (b) suministra; o (c) actualiza; software que pueda instalarse en una computadora, u otro equipo, que esté, o es probable que esté, conectado a una red de telecomunicaciones en Australia.	(a) el diseño por parte de la persona de un software de este tipo; o (b) el suministro por parte de la persona de un software de este tipo, o (c) la actualización por parte de la persona de un software de este tipo.

Nota 1: Véanse también los artículos 317HAA, 317MAA y 317TAA (prestación de asesoramiento a los proveedores de comunicaciones designados).
Nota 2: Véase también el artículo 317ZT (base constitucional alternativa).

317E Actos o cosas enumeradas

(1) A los efectos de la aplicación de esta Parte a un proveedor de comunicaciones designado, se entiende por ***acto o cosa enumerada***:
- (a) eliminar una o varias formas de protección electrónica que sean o hayan sido aplicadas por el proveedor o en su nombre; o
- (b) proporcionar información técnica; o
- (c) instalar, mantener, probar o utilizar software o equipos; o
- (d) garantizar que la información obtenida en relación con la ejecución de una orden o autorización se facilite en un formato determinado; o
- (da) un acto o cosa que se hace para ayudar en o facilitar lo siguiente:
  - (i) el cumplimiento a una orden o autorización en el marco de una ley del Commonwealth, un Estado o un Territorio; o
  - (ii) la recepción eficaz de información en relación con una orden o autorización en el marco de una ley del Commonwealth, un Estado o un Territorio; o
- (e) facilitar acceso o asistir para que se acceda a cualquiera de los siguientes que sean objeto de las actividades que el proveedor puede llevar a cabo:
  - (i) una instalación;
  - (ii) un equipo del cliente;
  - (iii) un dispositivo de procesamiento de datos;
  - (iv) un servicio de telecomunicaciones enumerado;
  - (v) un servicio que facilita, o es auxiliar o incidental a, la prestación de un servicio de telecomunicaciones enumerado;
  - (vi) un servicio electrónico;
  - (vii) un servicio que facilita, o es auxiliar o incidental a, la prestación de un servicio electrónico;
  - (viii) software que se utiliza, es para utilizar o es probable que se utilice, en relación con un servicio de telecomunicaciones enumerado;

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

(ix) software que se utiliza, es para utilizar o es probable que se utilice, en relación con un servicio electrónico;
(x) software que puede instalarse en una computadora, u otro equipo, que esté, o es probable que esté, conectado a una red de telecomunicaciones; o

(f) ayudar a probar, modificar, diseñar o mantener una tecnología o capacidad; o
(g) notificar determinados tipos de cambios o avances que afecten las actividades que el proveedor de comunicaciones designado puede llevar a cabo, si los cambios son pertinentes para la ejecución de una orden o autorización; o
(h) modificar o facilitar la modificación de cualquiera de las características de un servicio prestado por el proveedor de comunicaciones designado; o
(i) sustituir o facilitar la sustitución de un servicio prestado por el proveedor de comunicaciones designado para:
(i) otro servicio prestado por el proveedor; o
(ii) un servicio prestado por otro proveedor de comunicaciones designado; o
(j) un acto o cosa que se hace para ocultar el hecho de que se ha hecho algo de forma encubierta en el desempeño de una función, o el ejercicio de una facultad, conferida por una ley del Commonwealth, de un Estado o de un Territorio, en la medida en que la función o la facultad esté relacionada con:
(i) aplicar el derecho penal, en la medida en que se refiera a delitos graves en Australia; o
(ii) ayudar a que se aplique la legislación penal vigente en un país extranjero, en la medida en que dicha legislación se refiera a delitos graves cometidos en el extranjero; o
(iii) los intereses de la seguridad nacional de Australia, los intereses de las relaciones exteriores de Australia o los intereses del bienestar económico nacional de Australia.

(2) El inciso (1)(j) no se aplica a lo siguiente:
(a) hacer una declaración falsa o engañosa, o
(b) incurrir en una conducta deshonesta.

Condiciones de cumplimiento

317ZK Condiciones para la concesión de la ayuda, etc.

Alcance

1) Este artículo se aplica si un proveedor de comunicaciones designado debe cumplir con una solicitud en el marco de:
a. una notificación de asistencia técnica; o
b. una notificación de capacidad técnica.

……

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Condiciones

4) El proveedor de comunicaciones designado debe cumplir con la solicitud en las condiciones que sean:
    a. acordadas entre las siguientes partes:
        i. el proveedor;
        ii. el negociador de costos que corresponda; o
    b. a falta de acuerdo, determinadas por un árbitro designado por las partes.

317V Criterios de decisión

El Fiscal General no debe entregar una notificación de capacidad técnica a un proveedor de comunicaciones designado a menos que:

(a) el Fiscal General esté convencido de que los requisitos impuestos por la notificación son razonables y proporcionados; y

(b) el Fiscal General esté convencido de que el cumplimiento de la notificación es:

(i) viable; y

(ii) técnicamente factible.

Nota: Véase asimismo el artículo 317ZAA.

El proveedor tiene derecho a solicitar una evaluación del cumplimiento de lo anterior y, al llevar a cabo una evaluación en relación con una notificación de capacidad técnica, los evaluadores deben:

(a) considerar:

(i) si la notificación de capacidad técnica propuesta contraviene el artículo 317ZG; y

(ii) si lo que se solicita en la notificación de capacidad técnica propuesta es razonable y proporcionado; y

(iii) si el cumplimiento de la notificación de capacidad técnica propuesta es viable; y

(iv) si el cumplimiento de la notificación de capacidad técnica propuesta es técnicamente factible; y

(v) si la notificación de capacidad técnica propuesta es la medida menos invasiva que sería eficaz para lograr el objetivo legítimo de la notificación de capacidad técnica propuesta; y

(b) dar la mayor importancia a la cuestión mencionada en el subinciso (a)(i).

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

8. Sobre los autores

8.1. George Barker

George Barker es director de LECA y experto en análisis económico del derecho y la regulación. Actualmente es profesor asociado honorario de la Universidad Nacional de Australia (ANU) y miembro del Wolfson College de la Universidad de Oxford. Ha impartido clases de economía de la regulación al personal de los organismos reguladores australianos y de las empresas reguladas, ha realizado investigaciones sobre el bien público y ha prestado testimonio y asesoramiento económico pericial sobre una amplia gama de asuntos relacionados con la regulación de la industria de las tecnologías de la información y las comunicaciones (por ejemplo, la regulación de Internet, la asignación y el uso del espectro, los operadores y los servicios de telecomunicaciones, y el acceso a la red), y los sectores de los servicios públicos (por ejemplo, la energía y el transporte), así como la ley de competencia, la propiedad intelectual, los contratos y la legislación fiscal que afectan a una amplia variedad de otros sectores en Australia, Asia Pacífico, América del Norte y Europa. El Dr. Barker ha contribuido a numerosas revisiones de las políticas de la competencia y la regulación en Australia, Asia Pacífico, América del Norte y Europa. El Dr. Barker ha prestado testimonio como perito en todo el mundo ante organismos reguladores y ante tribunales que revisan las decisiones reguladoras en las instancias de apelación, así como en casos de arbitraje en La Haya, y ante ministros y parlamentos que participan en investigaciones y procesos de reforma en Australia, el Reino Unido, la UE, Nueva Zelanda, China, Corea, Japón y Filipinas. Por ejemplo, ha prestado testimonio como perito ante los tribunales federales de EE. UU., el Tribunal Federal de Australia y el Tribunal Superior de Nueva Zelanda, y sus análisis han sido citados en la Cámara de los Lores del Reino Unido, por el Tribunal Superior de Inglaterra y Gales y por la Comisión Europea. Fue director del Centro de Derecho y Economía de la Universidad Nacional de Australia de 1997 a 2017 y recibió la beca Olin de Derecho y Economía de la Universidad de Cornell (EE. UU.) en 2000, y ha sido profesor visitante en la London School of Economics (LSE) (2015-2018), en el Centro de Derecho y Economía del University College London (2010-2015), en la Universidad de Oxford 2008 y en el Instituto Británico de Derecho Internacional y Comparado (BIICL) (de 2009 a la actualidad). Fue analista jefe y asesor económico del Tesoro de Nueva Zelanda de 1984 a 1997. Forma parte del Consejo Editorial del European Journal of Law and Economics.Obtuvo un doctorado en Economía por la Universidad de Oxford en 1992, y tiene un máster en Economía (con honores) y una licenciatura en Derecho.

8.2. William Lehr

William Lehr tiene más de veinticinco años de experiencia como economista y consultor del sector de las telecomunicaciones e Internet. Asesora regularmente a altos ejecutivos del sector y a los responsables de elaborar las políticas en los Estados Unidos y en el extranjero sobre las consecuencias que los acontecimientos pertinentes para el ecosistema de Internet tendrán en el

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

mercado, el sector y las políticas. Es investigador científico en el Laboratorio de Ciencias de la Computación e Inteligencia Artificial (CSAIL) del Instituto Tecnológico de Massachusetts, y actualmente participa en varios proyectos de investigación multidisciplinaria dentro del Grupo de Arquitectura de Redes Avanzadas del CSAIL. La investigación del Dr. Lehr se centra en la economía y la política reguladora de los sectores de la infraestructura de Internet. Participa en múltiples proyectos de investigación multidisciplinaria centrados en cuestiones como el acceso a Internet de banda ancha, la ciberseguridad, las arquitecturas de red de próxima generación y la gestión del espectro. Además de su trabajo académico, el Dr. Lehr asesora a clientes del sector público y privado en los Estados Unidos y en el extranjero sobre cuestiones relacionadas con la estrategia y las políticas de las TIC. El Dr. Lehr es doctor en Economía de Stanford y tiene un MBA en Finanzas de la Wharton School, así como un MSE, un BA y un BS de la Universidad de Pensilvania. Para obtener más información, visite http://people.csail.mit.edu/wlehr/. A los efectos de este trabajo, el Dr. Lehr fue nombrado director consultor de LECA.

8.3. Mark Loney

Mark Loney es director de Consultoría en LECA y experto en sistemas y tecnologías de comunicaciones avanzadas, políticas públicas y gestión del sector público. Mark fue un alto ejecutivo en el servicio público australiano durante quince años y brinda asesoramiento independiente sobre la gestión del espectro y los asuntos relacionados con la regulación de las telecomunicaciones a clientes internacionales desde 2019. Mark fue director ejecutivo de la Autoridad Australiana de Comunicaciones y Medios de Comunicación (ACMA) de 2005 a 2018, y desempeñó un papel clave en el establecimiento de este organismo regulador de la convergencia de las comunicaciones de Australia de 2004 a 2005. Mark dirigió el desarrollo, la implementación y la firma de acuerdos regulatorios relacionados con los servicios de radiodifusión, radiocomunicaciones y telecomunicaciones durante más de veinte años en la Agencia de Gestión del Espectro, la Autoridad Australiana de Comunicaciones y la ACMA. Fue jefe adjunto de la delegación australiana en la Conferencia Mundial de Radiocomunicaciones de 2003. Mark se incorporó a la administración pública australiana en 1988, en el Departamento de Defensa, donde se dedicó a la investigación de comunicaciones complejas durante casi 9 años. Desde 2010 ha sido coautor de artículos para series de conferencias del IEEE, como DySPAN, así como para el Journal of Telecommunications Policy (TelPol). En 2014 asesoró al Gobierno de Mongolia sobre la rápida transición a las redes móviles de próxima generación (LTE/LTE Advanced) y las cuestiones asociadas, como los requisitos de backhaul y seguridad. Es licenciado de la Universidad de Curtin y ha realizado estudios de posgrado en la Universidad Nacional de Australia.

8.4. Doug Sicker

Douglas Sicker es un destacado experto mundial de los EE. UU. en tecnologías de red y su aplicación e implicaciones en otros sectores como los sistemas inalámbricos y la ciberseguridad, tanto hoy como en el futuro. En la actualidad,

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718

Doug es Decano Asociado Senior de Informática y profesor de ciencias de la computación e ingeniería eléctrica en la Universidad de Colorado, Denver | Anschutz Campus. Anteriormente, Doug ocupó la cátedra Lord Endowed en la Escuela de Informática y en la Facultad de Ingeniería de la Universidad Carnegie Mellon (CMU) y fue jefe de departamento en Ingeniería. También ha sido recientemente director interino del CyLab de la CMU, que reúne a expertos de diversas disciplinas de la universidad para colaborar en la investigación y la educación de vanguardia, con el fin de ayudar a crear un mundo en el que se pueda confiar en la tecnología. Doug también es director ejecutivo del Grupo de Asesoramiento Técnico sobre Internet de Banda Ancha (BITAG). Se ha desempeñado como director de tecnología de la Administración Nacional de Telecomunicaciones e Información (NTIA) y de la Comisión Federal de Comunicaciones (FCC), y como asesor principal del Instituto Nacional de Justicia del Departamento de Justicia, y fue presidente del comité directivo del Consejo de Fiabilidad e Interoperabilidad de la Red. Anteriormente fue Director de Arquitectura Global en Level 3 Communications, Inc. Ha publicado ampliamente en los campos de las redes, los sistemas inalámbricos, la seguridad de las redes y la política de redes. A los efectos de este trabajo, el Dr. Sicker fue nombrado director consultor de LECA.

Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, Reino Unido +44 7554 065 718