LECA

الشركاء الاستشاريون في القانون والاقتصاد

التأثير الاقتصادي للقوانين التي تضعف التشفير

أعده

جورج باركر، ويليام ليهر، مارك لوني، دوجلاس سيكر

5 نيسان/ أبريل 2021 م

للتواصل: د/ جورج باركر (LECA)

البريد الإلكتروني:

George.Barker@cleconsult.com

بتفويض من جمعية الإنترنت

Internet Society

فهرس المحتويات

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

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

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

1. ملخص تنفيذي [1]

في كانون الأول/ ديسمبر من عام 2018، أقرَّ البرلمان الأسترالي تعديلاً لتشريع تكنولوجيا الاتصالات وغيره (المساعدة والنفاذ) قانون 2018 (المعروف باسم TOLA) [2] وهو القانون الذي وسَّع سلطة الحكومة وقدرتها على الالتفاف حول حماية البيانات الرقمية. وقد شكل هذا القانون الإطار الذي يُمكن هيئات الاستخبارات وإنفاذ القانون أو ما يُطلق عليها LEIAs [3] من مطالبة أو سؤال مقدمي خدمات تكنولوجيا المعلومات، أو من يُطلق عليهم -في اللغة المستخدمة في قانون TOLA- مقدمو خدمات الاتصالات المحددة DCPs، بتقديم المساعدة للوصول لمحتوى البيانات المشفرة، الأمر الذي قد يتطلب مشاركة معلومات سرية من الشركات، أو تطوير إمكانات جديدة لهذا الغرض.

ويركز هذا التقرير على تقييم الدلائل المتاحة عن تأثيرات قانون TOLA على الاقتصاد الأسترالي والاقتصادات العالمية. ويقودنا التحليل إلى استنتاج أن هذا القانون يمكن أن يسبب ضرراً اقتصادياً جسيماً على الاقتصاد الأسترالي، وأن يتسبب في حدوث انتشار سلبي يعظّم هذا الضرر على المستوى العالمي. ووصفُ الضرر هنا بأنه "جسيم" يعني حدوث أضرار اقتصادية تبلغ عدة مليارات من الدولارات، وهي أضرار واسعة النطاق، ومن المحتمل أن تحدث (مبدئياً) في الأعوام القادمة.

وهناك العديد من الآليات التي قد يتسبب قانون TOLA من خلالها بوقوع أضرار اقتصادية. فعلى سبيل المثال، يعمل هذا القانون على زيادة حالة عدم اليقين في قطاع الأعمال. وقد توصلت الدراسات التي أجراها المعهد القومي الأمريكي للمعايير والتقنية NIST في عامي 2001 و2008 إلى أن التدخلات التي حدثت برعاية الحكومة، والتي أدت إلى تقليص الإحساس بعدم اليقين في الأمن الرقمي، قد أسفرت عن مزايا وفوائد إجمالية تُقدَّر بعدة مليارات من الدولارات. [4] إن قانون TOLA قد يضيع فرص إدراك مزايا مماثلة، بسبب تغذيته لحالة عدم اليقين في أفضل طرق تأمين المعلومات الرقمية بين أوساط المشاركين في السوق الرقمية.

ثانياً، يمكن أن يتسبب قانون TOLA في الإضرار بصورة ووضع العلامة التجارية لمقدمي خدمات الاتصالات المحددة DCPs العاملين في أستراليا، الذين يتعرضون للتهديد الذي يمثله هذا القانون للأمن الرقمي للمنتجات والخدمات التي يقدمونها. ومن جهة أخرى، فإن العملاء، ومنهم شركات السوق الكبيرة للإنترنت ومستخدموها، لديهم مخاوف أن يتسبب قانون TOLA في إضعاف أمن

[1] شكر: نتقدم بالشكر لجمعية الإنترنت على الدعم المادي لإخراج هذا البحث. ونؤكد أن ما يعبر عنه هذا التقرير من آراء، وربما أخطاء، هي مسؤوليتنا فقط.

[2] يُعرف أيضاً بقانون التشفير أو قانون المساعدة والنفاذ:
https://www.legislation.gov.au/Details/C2018A00148/Download

[3] LEIA تعني هيئات الاستخبارات وإنفاذ القانون التي تضم الهيئات الحكومية المخولة قانوناً بطلب نفاذ الحكومة للبيانات.

[4] انظر: NIST (2015-2018)، ستأتي مناقشته بتوسُّع لاحقاً، ويُذكر في الهامشين 110 و112 لاحقًا.

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

بياناتهم الخاصة، وهو ما قد يدفعهم لنقل أعمالهم إلى وجهة أخرى. وهذه الاستجابات من شأنها أن تؤدي إلى خفض أرباح مقدمي خدمات الاتصالات المحددة DCPs وزيادة تكاليف التشغيل، وذلك لاضطرار هؤلاء لاتباع إستراتيجيات بديلة لمواجهة التهديدات المرتبطة بقانون TOLA. وهذه الآثار المباشرة ليست بالضرورة مقتصرة فقط على مقدمي خدمات الاتصالات المحددة DCPs الذين تلقوا بالفعل تحذيرات بمقتضى هذا القانون، بل قد تمتد لتشمل أيضاً أولئك الذين يتوقعون إنذارات بمقتضى هذا القانون، أو الجهات الأخرى التي يعتريها القلق بشأن تأثيره، ليس من مقدمي خدمات الاتصالات المحددة DCPs فقط، بل أيضاً من عملائهم. ومن المتوقع، عامةً، أن تكون هذه الآثار المباشرة وغير المباشرة واسعة النطاق، بل أن تتراكم عبر الوقت بتتابع آثارها عبر الاقتصاد.

ثالثاً، ربما يُعد أكبر مصدر متفرد للآثار الاقتصادية السلبية المتوقعة ذلك التهديد غير المباشر لقانون TOLA للثقة في الخدمات الرقمية، ومنها الإنترنت. فنحن في خضم انتقال عالمي نحو اقتصادرقمي، إذ تؤدي التجارة الإلكترونية والمعلومات الرقمية على شبكة الإنترنت دوراً أكبر مما سبق، الأمر الذي يؤثر على جميع الدول والقطاعات والأعمال. وكلما زادت الثقة في تلك الخدمات والشبكات التي تدعم هذه الأنشطة (مثل مقدمي خدمات الاتصالات المحددة DCPs)، كانت آفاق النمو الاقتصادي أكثر إشراقاً. إن خفض الثقة في أمن البيانات من شأنه أن يؤدي إلى خفض الطلب الإجمالي عبر مختلف قطاعات الاقتصاد الرقمي، بل سيتسبب ذلك في أن تتحمَّل الشركات تكاليف أعلى، في محاولة منها لمواجهة الأضرار الناجمة عن انخفاض الثقة.[5] بالإضافة إلى ذلك، ولما كانت جميع قطاعات الاقتصاد تستخدم التكنولوجيا الرقمية، فإن هذه الآثار ستنتشر في شتى مناحي الاقتصاد، وستلقي بظلالها على كل النواحي التشغيلية الحديثة الخاصة بالأعمال. ومن ثَم، فمن الممكن أن تكون حتى التهديدات البسيطة للأمن السيبراني، أو بالمثل للثقة الرقمية، سبباً في تكبُّد تكاليف باهظة. وتشير إحدى الدراسات أن تهديدات الثقة الرقمية يمكن أن تُترجَم إلى أضرار عالمية تصل إلى تريليون دولار أو أكثر.[6] ولا يمكن في ظل المعلومات المتاحة حالياً قياس حجم هذه الآثار السلبية أو نِسَبها أو تحديدها مقارنةً بقانون TOLA. بالإضافة إلى ذلك، ولما كان من المتوقع أن تظهر هذه الآثار في الأعوام المقبلة، فإن تقدير مدى تأثيرها يعتمد على صياغة توقعات ملائمة لما يمكن أن يحدث في حالتي وجود هذا القانون أو غيابه. ومثل هذه التوقعات ستعتمد على مجموعة كبيرة من افتراضات ستكون في الأغلب مثيرة للجدل.

وعلى الرغم من أننا نستطيع يمكننا تحديد أكثر من اتجاه لانتشار الأضرار الناجمة عن قانون TOLA، فإن الدلائل المتاحة بالفعل لا تسمح بصياغة دقيقة لحجم الأضرار الاقتصادية

[5] في عام 2019، أجاب 18% من المستخدمين الذين لا يثقون في الإنترنت أنهم يُجرون عمليات شراء أقل. انظر: https://www.internetsociety.org/wp-content/uploads/2019/06/CIGI-Ipsos-Trust-User-Privacy_Report_2019_EN.pdf).

[6] على سبيل المثال، انظر: دراسة مجموعة تأمين زيورخ (2015)، الهامش 105 لاحقًا.

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

المحتملة التي يسفر عنها هذا القانون. ويرجع ذلك إلى عدد من الأسباب ستُناقَش مناقشةً كاملةً في هذا التقرير، ومنها:

- تقدير التأثير الاقتصادي لقانون TOLA يُعد أمراً معقداً ومحفوفاً بالتحديات. فقد يكون للقانون آثار سلبية مبلثرة وغير مبلثرة على الصعيد الاقتصادي، وفي عدة اتجاهات. وبعض من هذه الآثار يسهل تتبُّعه وتقديره أكثر من بعضها الآخر، إلا أن الوقوف على إجمالي الآثار يتطلب عدم التركيز على ما هو واضح وملاحظ بالفعل فقط.
- حتى تاريخه، فإن استخدام قانون TOLA محدود. فمنذ سَنِّ القانون، أُثير العديد من المخاوف من خلال مراجعات للقانون، ومن قِبل الكثير من أصحاب المصلحة بشأن ما يمكن أن يسببه هذا TOLA من أضرار اقتصادية كبيرة، وهو ما أدى إلى دعوات إلى إجراء تعديلات عليه بهدف التقليل من هذا التهديد. إن المدة الزمنية القصيرة بين تاريخ سَنِّ القانون وما أُثير من مخاوف حول أفضل طرق الاستجابة لمعارضة القانون قد تفسر محدودية الدليل التجريبي على تكلفة تنفيذ هذا القانون.
- يُعد الوصول إلى البيانات المرتبطة بقانون TOLA لاستخدامها في تقدير التأثير الاقتصادي أمراً محدوداً للغاية بسبب غياب الشفافية، وفي ظل شروط عدم الإفصاح التي يتضمنها القانون. وهذه الفجوات في البيانات تهدد فاعلية الرقابة المرجوة، ومن ذلك قدرة المحللين على محاولة صياغة تقديرات نظرية وعملية سليمة لتأثيرات هذا القانون.

من جهة أخرى، وعلى الرغم من أن هذا التقرير يركز بالأساس على التكلفة المرتبطة بتنفيذ قانون TOLA، فإن تقدير المزايا التي ترتبط بتنفيذ هذا القانون يُعد أيضاً أمراً أكثر صعوبة. ومن غير الواضح هل عَمِل هذا القانون -أو سيعمل- على تحسين وصول هيئات الاستخبارات وإنفاذ القانون LEIA للبيانات الرقمية ودعم كفاءتها التشغيلية. إضافةً إلى إن تشجيع الاستخدام الواسع النطاق للتشفير من الطرف للطرف، بوصفه أحد أهم وسائل دعم الأمن السيبراني، يُعد أمراً مقبولاً عامةً.[7] إلا أن قانون TOLA يمثل تحدياً أمام هذا الاستخدام الواسع الانتشار للتشفير من الطرف للطرف، وذلك لأن تصميم هذا القانون يقوم على تفعيل إمكانية الوصول لمحتوى البيانات المشفرة.

وتعترينا الدهشة أنه لم يكن هناك جهود حقيقة سابقة لتقييم التكلفة أو المنافع الاقتصادية لقانون TOLA أو التشريعات المماثلة (ذات الآثار الاقتصادية على الأمن الرقمي) في أستراليا أو غيرها.

[7] "التشفير من الطرف للطرف -الذي يكون فيه المفاتيح التي يحتاجها المستخدم لفك شفرة الاتصال المشفر على الجهاز الذي يجري الاتصال- يوفر أعلى درجات الأمن والثقة، لأنه مصمم بحيث يكون المتلقي المقصود فقط هو من لديه القدرة على استخدام المفتاح لفك شفرة الرسالة". (انظر: https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning)

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

وفي ظل غياب وجود بحوث يجريها طرف ثالث يمكن الاعتماد عليه لتقدير التأثير الاقتصادي لقانون TOLA، أجرينا بحثاً أولياً على هيئة مقابلات مطولة عبر الفيديو مع عدد من مقدمي خدمات الاتصالات المحددة DCPs المتعددي الجنسيات، وأيضاً من خلال استبيان بدون ذكر أسماء (مُعمى) لمقدمي خدمات الاتصالات المحددة DCPs، وكلهم يعملون في أستراليا. وكما هو مشروح بالكامل في التقرير، فإن البيانات التي جرى الحصول عليها من هذا البحث تتفق تماماً وتدعم نتائج التحليل المذكور في باقي التقرير. ويدعم البحث الذي أُجري على تجارب مقدمي خدمات الاتصالات المحددة DCPs وتوقعاتهم الخاصة بقانون TOLA النتائج التالية:

1- توقع أن يتسبب قانون TOLA في تأثيرات سلبية على الأعمال وعملائهم، وأن تكون هذه التأثيرات واسعة النطاق (أي لا تقتصر على الشركات العاملة في قطاعات تكنولوجيا الاتصالات والمعلومات).
2- معظم الأضرار المتوقعة ستكون غير مباشرة، وستكون مرتبطة بالتهديد الذي يفرضه قانون TOLA على تصور العملاء وشركاء الصناعة بشأن الثقة الرقمية.
3- مازال هناك استمرار للحالة القوية من عدم اليقين في قانون TOLA وتأثيراته.
4- إن الدليل التجريبي المباشر على التكاليف الاقتصادية للقانون (أو المزايا) محدود للغاية، ولكننا نُرجِع ذلك إلى: (أ) الضبابية التي تكتنف أنشطة قانون TOLA بسبب شروط عدم الإفصاح التي يتضمنها القانون؛ (ب) وقصر المدة الزمنية منذ سَنِّ القانون، والجدال المستمر لمنع هيئات الاستخبارات وإنفاذ القانون من استخدام السلطة المخولة لهم بمقتضى هذا القانون؛ (ج) وتوقع أن تكون التأثيرات غير مباشرة وأن تحدث في المستقبل.
5- إن الدليل المباشر المحدود الذي نلاحظه يدعم نتيجة أن المزايا التي تعود على الشركات ربما تكون بسيطة، بينما ربما تكون التكاليف التي تتحمَّلها الشركات كبيرة.
6- لا توفر البيانات التجريبية المتاحة قاعدة يمكن الاعتماد عليها لتقييم الأثر الاقتصادي الدولاري الإجمالي لقانون TOLA.

وبالتوافق مع توقعاتنا، فإن الدليل التجريبي على التأثيرات المباشرة لقانون TOLA ضعيف وصعب الملاحظة. لكن غياب مثل هذا الدليل التجريبي لا يُعد مؤشراً على غياب الأثر. وفي الوقت نفسه، فإن محدودية الأدلة التي أمكن جمعها أمرٌ في ذاته له دلائل. فطبقاً لأحد الأفراد الذين اشتركوا في البحث، والذين تعرضوا لتأثيرات اقتصادية سلبية، فإن قيمة الأثر الاقتصادي تُقدَّر بنحو مليار دولار (أسترالي)، [8] بينما يرى المشارك الوحيد في البحث، الذي قيَّم تأثير قانون TOLA تقييماً إيجابياً، أن تأثير القانون الرئيسي هو ترشيد هذا القانون للتشريعات القائمة

[8] إن النتيجة السلبية تعود مباشرةً إلى الضرر الذي يسببه قانون TOLA لصورة الهُوية الخاصة بمقدمي خدمات الاتصالات المحددة DCPs، وهو ما يسفر عن خسائر في المبيعات الحالية والمستقبلة. انظر: فصل 6 لتطلع على مناقشة أكثر كمالاً لنتائج المقابلات والاستبيان.

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

بالفعل. وكلتا الملاحظتين تتفقان مع النتيجة الرامية إلى أن المزايا التي ستنعكس على الشركات ستكون ربما مزايا بسيطة، بينما ستكون التكلفة التي تتحمَّلها الشركات كبيرة. وعلى الرغم من أن البحث التجريبي يدعم النتيجة النهائية للتقرير، فإن حجم العينة التي جرى عليها البحث تحول دون استخدامها أساساً لتحديد حجم هذه الأضرار بدقة أكثر.

ملخص

نستطيع أن نستنتج من هذا التحليل أن قانون TOLA يمثل خطراً جسيماً سيسفر عن أضرار مستقبلية اقتصادية بحتة على الاقتصاد الأسترالي، مع احتمالية انتشار هذا التأثير السلبي خارج أستراليا. ويشير الدليل المبدئي إلى أن بعض الشركات قد واجهت أضراراً اقتصادية كبيرة بالفعل، لكن يبدو أن معظم الأثر الضار الإجمالي سيحدث في المستقبل، وسيكون واسع الانتشار، وذلك في حال استمرار تهديد قانون TOLA للتشفير. بالإضافة إلى ذلك، فإن حالة الارتباك وعدم اليقين التي تعرض لها مقدمو خدمات الاتصالات المحددة DCPs، بسبب هذا القانون مستمرة، ويجب التطرق لها بشكل وافٍ.

إن تحديات تقدير التأثير الاقتصادي تقديراً دقيقاً من الأمور الصعبة، ولم يكن هناك أي بحث عام ذي قيمة لمحاولة تحديد كمِّ التأثير الاقتصادي لقانون TOLA، أو أي تشريع مماثل في أستراليا أو غيرها. إلا أن غياب وجود هذا الدليل التجريبي لا يعني عدم وجود تأثير كبير، بل على العكس، يعني أن عبء إثبات وجهة النظر يجب أن يقع على الرؤى التي تتوقع حدوث منافع كبيرة بوصفها نتيجة لتطبيق هذا القانون، بسبب وضوح الأضرار الجسيمة التي يفرضها تطبيق هذا القانون بشكل جلي.

2. مقدمة وعرض

يركز هذا التقرير على تقديم تقييم دليل التأثير الاقتصادي لقانون TOLA، وهو القانون الخاص بتعديل التشريع الأسترالي لتكنولوجيا الاتصالات والتشريع الآخر (المساعدة والنفاذ) قانون 2018 (المعروف بقانون TOLA).[10]

ويُعد هذا القانون تشريعاً مهماً مركباً. وكما سنشرح لاحقاً، فهو تعديل لسبعة قوانين مهمة أصدرها البرلمان الأسترالي تتعلق بأمن المعلومات، وهو أيضاً استكمال لجهود تشريعية ذات صلة في عدد من الدول الأخرى مثل المملكة المتحدة البريطانية والولايات المتحدة الأمريكية. ومن ثَم، فمن

[9] قبيل قانون TOLA وطبقا لتشريع قائم، منحت مجموعة من مقدمي خدمات الاتصالات المحددة DCPs الحكومة حق النفاذ لبيانات رقمية. ويرى شخص واحد من الذين أجابوا عن الاستبيان أن قانون TOLA يقلل التكاليف عن طريق ترشيد تعرض الشركات للتشريع القائم. وهذا الشخص لم يقدم تقديراً لحجم التوفير في النفقات، إلا أنها لا يُعد كبيراً جداً.

[10] للاطلاع على نص قانون TOLA، راجع: https://www.legislation.gov.au/Details/C2018A00148/Download، وأحياناً يُشار إلى هذا القانون بقانون التشفير، أو قانون النفاذ والمساعدة الأسترالي، أو قانون AAA.

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

المتوقع أن يكون لهذا القانون تبعات على الجهود المبذولة لتأمين البيانات الرقمية، وذلك على المستوى القومي (داخل أستراليا) وعلى المستوى الدولي.

ويركز هذا التقرير على خلق قدرات حكومية لتطويق التشفير عن طريق التوسع في سلطة الحكومة، لطلب (أو فرض) مساعدة مقدمي خدمة الاتصالات الرقمية DCPs، للوصول إلى البيانات الرقمية، ومنها البيانات المشفرة. ووفقاً لقانون TOLA، فإن تعريف مقدمي خدمات الاتصالات الرقمية يتسع ليشمل مجموعة كبيرة من الأعمال والأنشطة التي توفِّر منتجات وخدمات تكنولوجيا المعلومات والحوسبة ICT.

ويقدم الفصل الثالث عرضاً مختصراً عن تاريخ قانون TOLA وتأثيره القانوني. فبعد عملية مختصرة وسريعة، سُنَّ القانون في كانون الأول/ ديسمبر 2018. ومن ثَم، فإنه مرَّ بأكثر من عملية مراجعة، كل منها أوصت بإجراء تعديلات على التشريع وعلى طريقة التطبيق.

ويشرح الفصل الرابع الدور المحوري الذي يؤديه التشفير في تأمين البيانات الرقمية، ويلقي الضوء على بعض من المضامين الفنية لإدخال إمكانات موسعة بهدف تطويق التشفير.

ويتطرق الفصل الخامس للآثار الاقتصادية المحتملة لقانون TOLA. والنتيجة التي نصل إليها من هذا التحليل أن القانون قد يتسبب في تحمُّل تكاليف اقتصادية مستقبلية لا يُتوقَّع أن تُعوَّض عن طريق تحقيق أي منافع اقتصادية في المستقبل. وهذه نتيجة مؤكدة، على الرغم من صعوبة الوصول إلى تحديد دقيق لصافي التأثير الاقتصادي للقانون في ظل البيانات المتاحة وما يصاحبها من بحث، الأمر الذي يرجع في جزء منه إلى حالة الضبابية التي يخلقها القانون.

ويعرض الفصل السادس النتائج الأولية للبحث الذي أُجري بوصفه جزءاً من المشروع. وتضمن مقابلات مفصلة مع مقدمي خدمات الاتصالات الرقمية المتعددي الجنسيات، كما تضمن استبياناً دون ذكر الأسماء عن مقدمي خدمات الاتصالات الرقمية العاملين في أستراليا لتقييم تجاربهم وتوقعاتهم بشأن قانون TOLA منذ إقراره عام 2018. وكان الاستبيان مماثلاً لحالتين سابقتين من الأنشطة: الأولى أُجريت عشية سَنِّ القانون، والثانية بعد مرور عام. وعلى الرغم من أن هذه النتائج الأولية لا تقدم أساساً كافياً موثوقاً فيه لتحديد التأثير المتوقع للقانون، فإن هذه النتائج جاءت متسقة وداعمة للنتائج التي جرى التوصل إليها في الفصل الخامس.

وبالنظر إلى النتيجتين، يقودنا هذا التحليل إلى استنتاج أن قانون TOLA يمكن أن يسفر عن أضرار اقتصادية مستقبلية على الاقتصاد الأسترالي، مع احتمالية انتشار هذا الضرر الاقتصادي خارج أستراليا. ويوضح الدليل المبدئي أن بعض الشركات قد واجهت أضراراً اقتصاديةً كبيرة بالفعل، على الرغم من أن معظم الأضرار المجمعة يبدو أنها ستكون في المستقبل، وستكون واسعة الانتشار في حالة استمرار تهديد هذا القانون للتشفير. بالإضافة إلى ذلك، فإن حالة

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

التخبط وعدم الوضوح التي تنتاب مقدمي خدمات الاتصالات الرقمية بسبب هذا القانون مستمرة، ويجب تناولها تناولاً كافياً.

وعلى الرغم من تحديات تقييم الآثار الاقتصادية لقانون TOLA، لا يوجد أي بحث عام ذي قيمة يتطرق لتقدير حجم الأثر الاقتصادي لهذا القانون، أو أي تشريع مماثل في أستراليا أو غيرها. لكن غياب الدليل التجريبي لا يعني عدم وجود تأثير، بل يعني أن تركيز البحث وهدفه يجب أن يتحولا إلى معرفة هل يمكن أن يؤدي القانون إلى تحقيق منافع اقتصادية مهمة أم لا، إذا كان خطر حدوث أضرار اقتصادية كبيرة وواسعة أمراً جلياً.

3. الهيكل القانوني لقانون TOLA وخلفيته

في القسمين التاليين، نقدم عرضاً للهيكل القانوني لقانون TOLA، كذلك نعرض خلفية تاريخية عن هذا القانون حتى تاريخه. أولاً، نشرح كيف يؤدي القانون إلى توسيع سلطة الحكومة للحصول على مساعدة قطاع الصناعة في الوصول إلى المعلومات الرقمية المشفرة. ثانياً، نعرض تاريخ القانون منذ بدايته من خلال المراجعات المتعددة التي ما زالت قائمة.

3. 1 عرض لهيكل قانون TOLA

أدخل قانون TOLA تغييرات واسعة ومهمة على سبعة قوانين صدرت عن البرلمان الأسترالي، وقد جاء القانون لـ"طرح الإجراءات اللازمة للتعامل مع التحديات التي يفرضها التشفير الذي ينتشر استخدامه" من قبل هيئات الاستخبارات وإنفاذ القانون LEIA.[11] وهذه التشريعات المتأثرة بالقانون هي:[12]

1- قانون تكنولوجيا الاتصالات 1997[13] (TA1997)
2- قانون تكنولوجيا الاتصالات (النفاذ والتنصت) قانون 1979 م[14] (TIA Act)
3- قانون أجهزة المراقبة 2004 م[15] (SD Act)
4- قانون الجرائم 1914 م[16] (Crimes Act)
5- قانون المساعدة المتبادلة في الأمور الجنائية 1987 م[17] (MACMA)

[11] هذه المقولة مأخوذة من الفقرة الافتتاحية لمذكرة التفاهم التفصيلية التي صاحبت مقدمة قانون TOLA، والتي قُدمت إلى البرلمان الأسترالي في أيلول/ سبتمبر 2018. انظر: "مذكرة التفاهم التفصيلية" التي وُزِّعها على مجلس النواب وزيرُ الشؤون الداخلية السيد بيتر داتون بشأن مقدمة قانون TOLA، وذلك في 20 أيلول/ سبتمبر 2018، وهي متاحة على: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r6195%22 (تذكر فيما بعد بمذكرة التفاهم التفصيلية 2018).

[12] انظر: الفقرة 1 في مذكرة التفاهم التفصيلية 2018، الهامش 11 السابق.

[13] قانون تكنولوجيا الاتصالات 1997 TA متاح على: https://www.legislation.gov.au/Series/C2004A05145

[14] قانون تكنولوجيا الاتصالات للنفاذ والتنصت TIA متاح على: https://www.legislation.gov.au/Series/C2004A02124

[15] قانون أجهزة المراقبة SD متاح على: https://www.legislation.gov.au/Series/C2004A01387

[16] قانون الجرائم متاح على: https://www.legislation.gov.au/Series/C1914A00012

[17] قانون المساعدة المتبادلة في الأمور الجنائية MACMA متاح على: https://www.legislation.gov.au/Series/C2004A03494

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

6- قانون منظمة الأمن والاستخبارات الأسترالية 1979 م[18](ASIO Act)
7- قانون الجمارك 1901 م[19](Customs Act)

3.1.1 توسعة سلطة الحكومة للنفاذ إلى البيانات المشفرة

يتألف قانون TOLA -ذلك التشريع المهم- من 228 صفحة، ويضم خمسة جداول تتناول النواحي المختلفة من القدرات الحكومية اللازمة للوصول القانوني إلى المعلومات الرقمية. ويركز هذا التحليل للقانون على الجدول رقم واحد، الذي يطرح قدرات جديدة لطلب أو فرض المساعدة من قطاع الصناعة للوصول إلى المعلومات الرقمية، وينطبق ذلك على "قطاع أكبر من مقدمي الخدمة". [20]ومن ثَم، فالتركيز هنا على التأثير الاقتصادي لقانون TOLA، وعلى الطلب على التشفير واستخدامه.

وباختصار: فإن قانون TOLA يسمح لمجموعة مختارة -ولكن كبيرة- من هيئات الاستخبارات وإنفاذ القانون LEIA بتوجيه طلب أو أمر لمقدم خدمة الاتصالات المحددة DCP، لتوفير المساعدة الفنية لإزالة التشفير أو تطويقه بثلاث أدوات قانونية، تمثل ما نشير إليه إجمالاً "بإنذارات قانون TOLA" :[21]

1- طلب المساعدة الفنية TAR– وهو التماس يطلب من مقدم خدمة الاتصالات المحددة أن:

1-يقدِّم تطوعاً المساعدة لهيئة حكومية؛

2- و/ أو يبني تطوعاً القدرة لمساعدة هيئة حكومية.

2- إنذار المساعدة الفنية TAN– مماثل للـ TAR، لكنه يوجه إجبارياً، وهو بمنزلة أمر أكثر منه طلب يصدر لمقدم خدمة الاتصالات المحددة، ويجب أن يكون محدداً في طلب المساعدة فقط، وليس بناء القدرة بهدف المساعدة.
3- إنذار بناء القدرة الفنية TCN - وهو أيضاً أمر إجباري يطلب أو يتوجه بالأمر لمقدم خدمة الاتصالات المحددة، لخلق قدرة جديدة لتمكين تطويق التشفير، [22]ويمكن أيضاً أن يكون لطلب تقديم المساعدة أو العون.

---

[18] منظمة الامن والاستخبارات الأستراليةASIO متاح على: https://www.legislation.gov.au/Series/C2004A02123
[19] قانون الجمارك متاح على: https://www.legislation.gov.au/Series/C1901A00006
[20] انظر: الفقرتين 8 و10 من مذكرة التفاهم التفصيلية 2018، الهامش 3 السابق.
[21] يتطرق قانون TOLA لهذه الأمر في الجدول رقم 1، الذي يتضمن أكثر من نصف القانون، ومن المقترح إضافة جزء جديد عن "جزء 15- مساعدة قطاع الصناعة" لقانون TA 1997 (انظر: صفحات 4-109 من قانون TOLA، الهامش 2 السابق).
[22] بينما يشمل إنذار TAR أو TAN جملة: "إزالة واحدٍ أو أكثر من أشكال الحماية الإلكترونية" (أي إزالة التشفير) بوصفه واحدة من البنود المدرجة أو الأشياء التي يمكن المطالبة بها (انظر: قسم (a) (1) 317 E من قانون TOLA، الهامش 2 السابق)، فقد استبعد قانون TOLA مطالبة مقدمي خدمات

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

ويخضع كل نوع من أنواع إنذارات قانون TOLA لمتطلبات قانونية مختلفة بشأن من يحق له إصدار الإنذار، وظروف وقواعد التشغيل التي تحكم استخدام القدرة الفنية، وما الذي يمكن أن يُطلَب أو يُفرَض، والرقابة وبدائل الاستئناف المتاحة لمتلقي الإنذارات.

وتخلق تلك الإنذارات التي يمكن للجهات الحكومية إصدارها بمقتضى قانون TOLA قدرات جديدة للحكومة لمطالبة قطاع الصناعة بما يأتي: (أ) تقديم المساعدة؛ (ب) و/ أو خلق القدرة على تطويق التشفير. وكلا النوعين من القوى مثير للمخاوف، وخاصة عندما يتعلق الأمر بمطالبة متلقي الإنذار بخلق القدرة على تطويق التشفير. وفورَ حدوث ذلك، فإن هذه القدرة تمثل الأساس اللازم لإزالة التشفير عن أي معلومات رقمية يُطبَّق عليها القانون، وليس المعلومات الرقمية المستهدفة فقط، التي كانت هدف الإنذار في المقام الأول. [23]

وفي حالة عدم الإلمام بالطبيعة المحددة لهذه القدرة، فمن المستحيل معرفة حجم التهديد الذي يواجه الأمن الرقمي بسببها. وقد تناول قانون TOLA هذا القلق الواضح عن طريق تحديد الطلبات الصادرة بمقتضى القانون فقط للطلبات التي لا تتسبب في إحداث "ثغرات أمنية في النظام". وذلك يعني أن أي طلب موجه لقطاع الصناعة لتقديم المساعدة أو بناء القدرة سيركز بدقة على الأهداف المحددة التي تستهدفها سلطة الحكومة، دون صُنع أي ثغرة أمنية قد تؤثر على جهات أخرى لم تكن مستهدفة من الأساس. [24] وكما ناقشنا من قبل، فإن فاعلية هذا التحديد ما زالت تثير المخاوف.

إن أنواع المساعدة أو القدرات التي يمكن أن تطالب بها الهيئات الحكومية بمقتضى قانون TOLA أنواعٌ متسعة ومركبة. وهي تشمل "إزالة واحد أو أكثر من أشكال الحماية الإلكترونية"، وهو ما يشمل التشفير، ولكنه أيضاً يشمل "توفير المعلومات الفنية" و"تسهيل الوصول إلى المرفق، أو جهاز المستهلك، أو جهاز تشغيل البيانات أو خدمة النقل، أو البرمجية... إلخ" [25] وعلى الرغم من أن القانون الأسترالي يضع شروطاً تفوِّض الهيئات الحكومية بطلب مساعدة القطاع الصناعي في تنفيذ الإنذارات القانونية، وفي الوصول إلى البيانات الرقمية، فإن قانون TOLA قد وسَّع نطاق

الاتصالات المحددة بتمكين القدرة على إزالة التشفير من إنذارات الTCN (انظر: (i) (c) (4) T 317s من قانون TOLA، الهامش 2 السابق). ولأنه بمقتضى إنذار TCN يمكن مطالبة مقدمي خدمات الاتصالات المحددة بتوفير القدرة على تمكين آخر E 3317s ، فإن الTCN قد يسفر عن مطالبة مقدمي خدمات الاتصالات المحددة بتوفير القدرة التي قد تساعد هيئات الاستخبارات وإنفاذ القانون على تطويق التشفير.

[23] على سبيل المثال، قد يتيح بناءُ القدرة الأساسَ لتطويق الأمن الرقمي من قبل آخرين لم يكونوا في الأساس هدفاً لإنذارات قانون TOLA. وانتهاكات هؤلاء قد تكون مقصودة (مثل الفاعلين الأشرار الذين يسعون عن عمد إلى النفاذ إلى المعلومات السرية) أو غير مقصودة (مثل الفاعلين الذين يتسببون في الإضرار بالأمن الرقمي من خلال التجاهل أو الإهمال). والنقطة هي أنه فور خلق القدرة على تطويق التشفير، فإن تقييد إساءة استغلال هذه القدرة يصبح تحدياً.

[24] يحدد قانون TOLA الثغرات الأمنية في النظام أو الضعف النظامي، إما بوصفه ثغرة أمنية، وإما بوصفه ضعفاً يؤثر على "مجموعة كاملة من التقنيات". (انظر: الصفحات 12، 84-81 من قانون TOLA، الهامش 2 السابق).

[25] قانون TOLA 317Es يتيح أنواعاً مختلفة من المساعدة التي يمكن أن تطلب بمقتضى قانون TOLA (انظر: الصفحات 18-20 من قانون TOLA، الهامش 2 السابق).

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

هذه السلطة بشكل كبير.[26] بالإضافة إلى ذلك،وكما أشرنا إليه من قبل، فإن القدرة على طلب أو فرض المساعدة في تطويق التشفير أمرٌ من الواضح أنه جديد على أستراليا.[27] فهذا القانون يوسع نطاق السلطة الممنوحة لهيئات الاستخبارات وإنفاذ القانون LEIA لتطويق التشفير، إلا أن حدود هذه السلطة، إذا توافرت، غير واضحة.

بالإضافة إلى التوسع في أنواع المساعدة التي تطلبها أو تفرضها الجهات الحكومية من قطاع الصناعة، فإن قانون TOLA يعمل أيضاً على توسيع نطاق شركات الاتصالات وتكنولوجيا المعلومات التي ينطبق عليها هذا القانون، وهذا يمثل تحولاً جذرياً، فقبل إصدار هذا القانون، كان مقدمو خدمات الاتصالات CSPs معتادين بالفعل على التعاون مع هيئات الاستخبارات وإنفاذ القانون فيما يتعلق بمنح حق الوصول القانوني للبيانات الرقمية في سياقات مختلفة (مثل منح المساعدة مثلاً في علميات التنصت القانوني). وهذا القانون يوسِّع نطاق الشركات الملزَمة بهذه الالتزامات القانونية، لتضم كيانات تُصنَّف على أنها مقدمو خدمات اتصالات محددة DCPs، وهو ما يعرف في إطار قانون TOLA بأي "شخص" يقع في أحد التصنيفات الخمسة عشر المحددة في القسم 317C[28] المذكورة بالكامل في الملحق.

وعلى الرغم من أن بعض كيانات الأعمال والمعرفة، كمقدمي خدمات اتصالات محددة DCPs، كانت بالفعل مُلزَمة بالتزامات قانونية للتعاون مع هيئات الاستخبارات وإنفاذ القانون لتوفير الوصول القانوني للمعلومات الرقمية، فإن قانون TOLA قد وسَّع نطاقَ شركات الاتصالات وتكنولوجيا المعلومات التي تنطبق عليها هذه الالتزامات، ووسع نطاقَ الأنشطة التي تخضع لهذا القانون. ولأن كثيراً من شركات الاتصالات وتكنولوجيا المعلومات لديه أنشطة متعددة في مجالات مختلفة، والتصنيف الملائم للأنشطة والمجالات غير محدد، فمن الواضح أن نطاق قانون TOLA متسع.

لكن الأمر غير الواضح هو أي نوع من شركات الاتصالات وتكنولوجيا المعلومات، في حالة وجودها، أو أي أنشطة تكون معفاة من تلقي إنذارات بمقتضى قانون TOLA. وهذا النطاق المتسع -وغير الواضح- للقانون يعني أن تأثيره المحتمل هو أيضاً واسع، لأنه يشمل بالضرورة كل

[26] على سبيل المثال، فإن الجزء 14 من قانون TA 1997 يفرض التزامات على النواقل وعلى مقدمي خدمة النقل لمساعدة هيئات الاستخبارات وإنفاذ القانون، "كما هو ضروري" على" فرض القانون الجنائي" و"المساعدة في التحقيق والمقاضاة" للجرائم و"حماية الأمن القومي". (انظر: الصفحات 322-328 من قانون TA 1997 وIA Act، الهامش 5 السابق). وأضف إلى ذلك أن الفصل الخامس من TIA ACT يفرض التزامات على النواقل ومقدمي خدمات النقل للتعاون مع هيئات الاستخبارات وإنفاذ القانون ومنح المساعدة في تنفيذ إجراءات التدخل القانونية (مثل التنصت) (انظر: الصفحات 360-410 من TIA ACT، الهامش 6 السابق)

[27] نتفادى القول بأن سلطة TOLA لتطويق التشفير أمرٌ جديد، لأن: (أ) سلطة الحكومة لطلب مساعدة قطاع الصناعة في الوصول للمعلومات المشفرة موجودة في المملكة المتحدة من قبل قانون TOLA، الذي استعار قانون القوة التحقيقية الإنكليزي لعام 2016. (انظر: قانون القوى التحقيقية لعام 2016) المملكة المتحدة، المتاح على: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (ب) هناك العديد من التوصيات لإجراء تعديلات على قانون TOLA، وبالنظر إلى تعقيد القانون والقوانين التي تتداخل معه ويعدلها، فمما يخرج عن نطاق هذا التقرير أن يوفر التحليل القانوني الكافي للقانون ومدى حداثة الإمكانات التي يوفرها. وقد يرفض بعض الباحثين القانونيين تفسير التعديلات الطارئة على قانون TOLA بأنها تمنح السلطة للحكومة لتطويق التشفير، وكذلك تشريعات ما قبل القانون، التي تُعد جزءاً من الإطار القانوني المرتبط بقدرة الحكومة على الوصول القانوني إلى المعلومات.

[28] الصفحات 14-18 من قانون TOLA، الهامش 2 السابق.

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

قطاع الاتصالات وتكنولوجيا المعلومات. بالإضافة إلى ذلك، فإن معظم الأعمال في القطاعات الأخرى غير الاتصالات وتكنولوجيا المعلومات تعتمد اعتماداً كبيراً على قطاع الاتصالات وتكنولوجيا المعلومات، ولديها وظائف تؤهلها لكي تكون ضمن المشركات التي ينطبق عليها قانون TOLA. وافتراضياً، فإن أيشركة تتعامل مع موردين أو عملاء من خلال موقع إلكتروني أو تطبيق تُصنَّف على أنها مقدم خدمة اتصالات محددة DCP.

كذلك، يتسع أيضاً بمقتضى القانون نطاقُ هيئات الاستخبارات وإنفاذ القانون التي يمكن أن تصدر إنذارات، فهي تشمل الهيئات المسؤولة عن إنفاذ القانون المحلي والأمن القومي وإنفاذه خارج الوطن والأنشطة الأمنية (ومن ذلك جمع المعلومات الاستخباراتية).[29] والسلطة الممنوحة لمختلف هيئات الاستخبارات وإنفاذ القانون بمقتضى قانون TOLA موضحة بدرجات متفاوتة من الدقة. فعلى سبيل المثال، فإن عدد هيئات الاستخبارات وإنفاذ القانون التي يمكن أن تصدر طلب المساعدة الفنية TAR (التطوعي) أكثر من عدد الهيئات التي يمكن أن تصدر إنذار المساعدة الفنية TAN أو إنذار القدرة الفنية TCN (الإجباري).[30] ويتعلق الكثير من التعديلات المقترحة على قانون TOLA والمخاوف المثارة بشأنه بالحاجة إلى تطبيق رقابة أفضل، وذلك لضمان عدم إساءة استغلال القدرات الجديدة اللازمة للوصول للبيانات الرقمية وتطويق التشفير. وتتمثل بعض التعديلات في مراجعة شروط الجهات التي يحق لها إصدار إنذارات، والظروف المحيطة بتلك الإنذارات، والمراجعة اللازمة قبل إصدارها، وتنويع الإجراءات المرتبطة بالرقابة. والمراجعةُ القانونية الكاملة أو التقييم لمدى فاعلية شروط المراقبة والجهود المبذولة لتحديد تأثير قانون TOLA تتعدى حدودَ هذا التقرير، ولكن يكفي القول بأن الكثير من توصيات الإصلاح قد نُفذت.[31]

وتلخيصاً لما سبق، فإن قانون TOLA يخلق إمكانات جديدة مهمة لعدد كبير من هيئات الاستخبارات وإنفاذ القانون، لطلب أو فرض المساعدة من نطاق واسع من كيانات الاتصالات وتكنولوجيا المعلومات، بهدف الوصول إلى المعلومات الرقمية السرية وتطويق التشفير، لكن طبيعة هذه القوى وحدودها غير واضحة.

3.1.2 تفاصيل إنذارات قانون TOLA وشروط أخرى مهمة

ومن الاختلافات المهمة بين أنواع الإنذارات التي تصدر بمقتضى قانون TOLA أن التزام المتلقي بتنفيذ طلب المساعدة الفنية TAR يكون اختيارياً، بينما يكون الالتزام بإنذار المساعدة الفنية TAN أو بناء القدرة الفنية TCN إجبارياً. وترجع أهمية هذا الاختلاف إلى أن عدم الالتزام بإنذار

[29] تشمل هيئات الاستخبارات وإنفاذ القانون التي لها حق إصدار إنذارات بمقتضى قانون TOLA: منظمة الامن والاستخبارات الأسترالية ASIO، وعدداً من هيئات الإيقاف IA ، مثل الشرطة و وكالة الاستخبارات السرية الأسترالية ASIS، ومديرية الإشارات الأسترالية ASD.

[30] على سبيل المثال: فإن منظمة الأمن والاستخبارات الأسترالية ASIO، وهيئات الإيقاف IA قد تصدر ثلاثة أنواع من الإنذارات (حسب القيود المفروضة على الأنواع المختلفة من الإنذارات)، إلا أن وكالة الاستخبارات السرية الأسترالية ASIS ومديرية الإشارات الأسترالية ASD تصدر فقط TARs.

[31] على سبيل المثال، وكما سنشرح لاحقاً في القسم الخاص بتاريخ TOLA، فإن تقرير INSLM يدعو لإجراء تغيير كبير في تخصيص السلطة المخول إليها إصدار إنذارات TOLA (انظر: الهامش 40 اللاحق).

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

المساعدة الفنية TAN (طلب إجباري للمساعدة)، أو بناء القدرة الفنية TCN (طلب إجباري لبناء القدرة الفنية)، يجعل المتلقي عرضة للعقوبة، سواء من جانب المسؤولية المدنية، أو فرض الغرامات، أو التعرض لإجراءات قضائية. ولأن الطلب الاختياري قد يكون في ذاته مؤشراً لإنذار إجباري، فإن الاختلاف بين أنواع الإنذارات لا يمثل في حقيقة الأمر الأهمية التي تبدو عليها لأول وهلة، بل إن البعض لا يَرى TAR أمراً "اختيارياً"، لأن الدافع للالتزام به كبير.

وفي كل الأحوال، فإن متلقي إنذارات قانون TOLA ممنوع من الكشف عن محتوى هذه الإنذارات أو الظروف التي ترتبط بإصدارها. والكشف غير القانوني عن إنذارات هذا القانون له عقوبات قانونية، مثله مثل عدم الالتزام بتنفيذ تلك الإنذارات. بالإضافة إلى ذلك، فإن المعلومات المتاحة عن إنذارات القانون محدودة للغاية، لعدم إمكانية الكشف عن هوية متلقي الإنذارات، [32] ولا تتوافر إلا إحصاءات قليلة عن عدد الإنذارات التي صدرت بمقتضى هذا القانون. وهذه القيود المفروضة عن الكشف عن محتوى الملاحظات وعن الإبلاغ عن كيفية استخدام هذا القانون تجعل من الرقابة الفعالة أمراً صعباً، بل تعقِّد الجهود المبذولة لتقييم التأثير الاقتصادي للقانون. [33]

ومن الشروط الأخرى المهمة المرتبطة بقانون TOLA ضمانُ "المرفأ الآمِن"، الذي يحمي المتلقين من مقدمي خدمات الاتصالات المحددة لإنذارات قانون TOLA من أي مسؤولية ترتبط بالتزامهم بالقانون. فطبقاً للنظام السابق، لم يكن من الواضح دائماً متى يكون الطرف المتعاون مسؤولاً عن انتهاك حماية الأمن أو الخصوصية، وذلك في حالة تعاون قطاع الصناعة على إتاحة الوصول إلى البيانات الرقمية. بالإضافة إلى ذلك، فإن هذا القانون يسمح باسترداد التكاليف

32 إن تسجيل عدد الإنذارات التي أُصدرت بمقتضى قانون TOLA غير واضح. فإن غياب الشفافية بشأن هذا الرقم يجعل أي محاولات لتحديد التأثير الاقتصادي للقانون أمراً صعباً، إن لم يكن مستحيلاً. بالإضافة إلى ذلك، فإن غياب الشفافية بشأن الشركات (أو حتى أنواعها) التي تتلقى إنذارات هذا القانون ونوعية المساعدة المطلوبة وكيفية استجابة المتلقي تجعل التحدي أكثر صعوبة.

وعلى الرغم من ذلك، نرى أنه حتى تاريخه قد أُصدرت إنذارات الTAR غير الملزمة فقط، وأن إجمالي عدد الإنذارات التي أُصدرت لا يتعدى 50. ولم نرَ أي تقارير لإصدار إنذارات من نوعية TAN أو TCN. ونقدر أن عدد إنذارات TAR تعتمد على ما ذُكر في التقارير الرسمية وفي الخطابات. فهناك تقريران يشيران إلى إصدار 18 إنذاراً من نوع TAR من كانون الأول/ ديسمبر 2018 وحتى حزيران/ يونيو 2020 كما يأتي: لجنة **الاستخبارات الجنائية الأسترالية ACIC -1- والشرطة** الفيدرالية الأسترالية AFP -8- وشرطة نيو سوث ويلز -9- (انظر: جدول 45 لإدارة الشؤون الداخلية 2019، التقرير السنوي قانون الاتصالات (الإيقاف والنفاذ) قانون 1979 لعام 2018-2019 الصادر عن إدارة الشؤون الداخلية: https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-18-19.pdf

وجدول رقم 44 في تقرير إدارة الشؤون الداخلية لعام 2020، التقرير السنوي لقانون الاتصالات (الإيقاف والنفاذ)، قانون 1979 لعام – 2020-2019 الصادر عن إدارة الشؤون الداخلية: https://www.homeaffairs.gov.au/nat-security/files/telecommunications-interception-access-act-1979-annual-report-19-20.pdf)

بالإضافة إلى ذلك، فإن المدير العام لمنظمة الأمن والاستخبارات الأسترالية ASIO قد أخبر الPJCIS في آب/ أغسطس 2020 بقوله: "استخدمنا سلطة مساعدة قطاع الصناعة أقل من 20 مرة". انظر: https://www.asio.gov.au/publications/speeches-and-statements/director-general-opening-statement-pjcis-august-2020.html

ومن غير الواضح: هل يشير هذا التصريح إلى إنذارات TAR التي أصدرتها هيئات معينة مذكورة، أم أن هذه الإنذارات "العشرين" هي ما ذُكر في تقارير أخرى. وفي كل الأحوال، سواء أكان الرقم 18 أم 50 (ولا يوجد بيانات تشير إلى أنه أكثر من ذلك)، فإن استخدام الحكومة لقانون TOLA محدود حتى الآن.

33 يمكن تبرير بعض القيود المفروضة على الإفصاح عن الإنذارات الصادرة بمقتضى قانون TOLA بأنها قيود ضرورية لحماية فعالية أفعال هيئة الاستخبارات وإنفاذ القانون.

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

الناجمة عن الالتزام بإنذاراته. وتزيد شروط كل من "المرفأ الآمِن" واسترداد التكاليف التحفيزَ على الالتزام بالإنذارات.

وكما سنشرح في فصول لاحقة من هذا التقرير، فإن تزايد احتمالات أن تتلقى أطراف (غير معروفة) إنذارات (غير معروفة) بمقتضى قانون TOLA، بسبب ممارسة أنشطة (غير معروفة) يمكن أن تؤدي إلى تطويق التشفير، يزيد من التأثير الاقتصادي المحتمل للقانون، ومن المخاطر (المنتظرة)، بأن يؤدي القانون إلى إضعاف الأمن الرقمي.

3.2 تاريخ قانون TOLA

إن الدافع وراء سنِّ قانون TOLA يعود إلى القلق المتزايد في أستراليا، وفي العالم كله، من الاستخدام الزائد للتشفير، الذي يمثل تهديداً لقدرة هيئات الاستخبارات وإنفاذ القانون على الوصول إلى البيانات الرقمية لإنفاذ القانون وتحقيق الأمن. ومنذ أواخر عام 2017 م، تحركت الحكومة الأسترالية تحركاً سريعاً نسبياً لطرح قانون TOLA، وتقديم إمكانات موسعة لهيئات الاستخبارات وإنفاذ القانون لإزالة التشفير أو تطويقه. [34]

وفي تموز/ يوليو 2017 م، أعلنت الحكومية عن نيتها للتطرق لهذا الأمر. [35] وفي آب/ أغسطس 2018 م، التقت حكومةُ أستراليا دولَ العيون الخمس Five Eyes [36]، إذ توصلوا إلى موقف مشترك. [37] وأُصدرت بالفعل مسودة القانون يوم 14 آب/ أغسطس 2018 م [38] وتلقت إدارة الشؤون الداخلية (DHA التي كانت الهيئة الحكومية الرئيسية المسؤولة عن القانون) 340 طلب تعديل. وقُدمت مسودة القانون والتعديلات المقترحة لمجلس النواب يوم 20 أيلول/ سبتمبر 2018 م، وأُحيل الأمر للجنة البرلمانية المشتركة المعنية بشؤون الأمن والاستخبارات PJCIS للنظر في الأمر، وقد صاحب ذلك تقديم تقرير نشر في أوائل كانون الأول/ ديسمبر 2018 م. وقد عقدت PJCIS جلسات استماع عامة في الفترة من 19 تشرين الأول/ أكتوبر إلى 30 تشرين الثاني/ نوفمبر 2018 م، أيضاً دعت إلى تقديم مزيد من اقتراحات التعديلات. وإجمالاً تلقت الـ PJCIS 105 طلبات تعديل (منها الطلبات السرية التي حُجبت).وكان هناك 11 طلباً مقدماً من هيئات حكومية ومن لجان تابعة للشرطة ولجان جنائية داعمة للقانون. كذلك كان هناك الكثير من الطلبات المعارضة للقانون من ممثلي قطاع تكنولوجيا المعلومات الأسترالي.

---

[34] واكر-مونرو- برندان (2019)- طلقة في الظلام- قوانين التشفير القترحة في أستراليا" مراجعة قانون Adelaide 40(3) .

[35] مالكوم تيرنبول- "مؤتمر صحفي مع النائب العام والمفوض المؤقت للAFP بمدينة سيدني"- 14 تموز/ يوليو 2017 (المؤتمر الصحفي، 14 تموز/ يوليو 2017).

[36] تحالف الFive Eyes هو تحالف لمشاركة المعلومات، وقد أُنشئ بمقتضى اتفاقية UKUSA بين كندا ونيوزيلندا والمملكة المتحدة والولايات المتحدة الأمريكية وأستراليا. وقد صُمم هذا التحالف ليعمل على تسهيل المشاركة السهلة والجيدة للمعلومات الاستخباراتية والأمن القومي.

[37] "بيان مبادئ الوصول إلى الدليل والتشفير"، إدارة النيابة العامة، آب/ أغسطس 2018- متاح على:
https://www.ag.gov.au/sites/default/files/2020-03/joint-statement-principles-access-evidence.pdf.

[38] قانون TOLA والاقتباس من قانون القوة التحقيقية بالمملكة المتحدة الذي أُقِر عام 2016 (انظر: قانون القوى التحقيقية- المملكة المتحدة https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted).

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

وفي ضوء عدد من تقدموا بطلبات تعديل، وعبَّروا عن قلقهم حيال تأثير القانون على الأعمال، خاصةً الأعمال الصغيرة في حال الالتزام بإجراءات مساعدة قطاع الأعمال، سألت الـ PJCIS إدارة الشؤون الداخلية هل أعدت الحكومة بياناً عن التأثير التنظيمي لمشروع القانون، فردت لجنة الشؤون الداخلية DHA بأن الحكومة جهَّزت بياناً قصيراً عن التأثير التنظيمي، مفاده أن "التأثير التنظيمي لإجراءات مساعدة قطاع الصناعة سيكون بسيطاً". [39]

وفي يوم 22 تشرين الثاني/ نوفمبر 2018 م، تلقت PJCIS تحذيراً من وزير الشؤون الداخلية بأن هناك تهديداً وشيكاً، ومن ثَم، هناك حاجة لإمداد الهيئات بسلطات إضافية، والموافقة على مشروع القانون في الأسبوع الأخير من عمل البرلمان لعام 2018 م، وعلى الرغم من أن الـ PJCIS لم يصل إلى اتفاق كامل بشأن كل ما يتعلق بمشروع قانون TOLA، فإن اللجنة قد تقدمت بتقرير استشاري يوم 5 كانون الأول/ ديسمبر 2018 م [40] مفاده:

"... هناك احتياج حقيقي وحثيث لإمداد الهيئات بالأدوات اللازمة للاستجابة لتحديات الاتصالات المشفرة. فإن غياب هذه الأدوات يؤدي إلى تصعيد المخاطر، وقد أدى قبل ذلك إلى تعطيل تحقيقات الهيئات عدة سنوات، واستجابةً لهذه المخاطر المتصاعدة، فإن اللجنة توصي بنظر البرلمان سريعاً في مشروع القانون وإقراره على الفور." [41]

وعلى الرغم من العدد الكبير من طلبات التعديلات وتقارير اللجنة المتعلقة بالتعديلات المقترحة، فإن الـ PJCIS أجرى تعديلات بسيطة فقط. وعُدِّل مشروع القانون لتوضيح بعض التعريفات، وإدخال بعض الشروط التي تنص على استشارة مقدم الخدمة والحصول على المشورة فيما يتعلق بالالتزام بالإنذارات الإجبارية، لبناء القدرات اللازمة لمساعدة هيئات الاستخبارات وإنفاذ القانون LEIA. [42] وعُدلت أيضاً الشروط الخاصة بالطلبات وأوامر المساعدة لضمان عدم استخدام هذه الطلبات لتطويق العمليات القائمة بالفعل. لكن هذه التعديلات لم تتطرق لكل المخاوف. [43] ثم راجعت اللجنة البرلمانية الدائمة لتدقيق مشاريع القوانين مشروع القانون. [44] ولا يدخل في إطار هذا التقرير التحليل الكامل لنتائج اللجنة الدائمة، لكن اللجنة

[39] انظر: صفحة 13، مراجعة إدارة الشؤون الداخلية لقانون TOLA، الهامش 3 السابق.

[40] PJCIS (2018) "التقرير الاستشاري عن مسودة قانون الاتصالات والتشريع الآخر (المساعدة والنفاذ) – 2018"
اللجنة البرلمانية المشتركة للاستخبارات والأمن ، كانون الأول/ ديسمبر 2018، متاح على:
https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1.

[41] بيدينجتون إم، (2019) "تعديلات تشريع الاتصالات والتشريعات الأخرى" (تعديلات متنوعة) مسودة القانون 2019- قسم استيعاب مسودة القوانين والقانون" 27 آذار/ مارس 2019:
https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/6581692/upload_binary/6581692.pdf

[42] انظر: الصفحات 5-7 ، تقرير اللجنة البرلمانية المشتركة للاستخبارات والأمن (2018) ، الهامش 12 السابق.

[43] كما في حال التعريفات الخاصة بالثغرات الأمنية والضعف الأمني، التكنولوجيا المستهدفة، وفرض الأهداف الخاصة بإصدار الجزء 15 من الإنذارات، وكذلك تحديد عمليات هيئات الإيقاف الخاصة بالدولة والمناطق التي تُطرَح أمام مفوضية الـAFP في مثل هذه الإنذارات.

[44] اللجنة البرلمانية الدائمة لتدقيق مشاريع القوانين، برلمان أستراليا، (Scrutiny Digest Digest رقم 14 لعام 2018، 28 تشرين الثاني/ نوفمبر 2018) - 23-82:

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

أثارت مخاوف أخرى تتعلق بعدم دستورية استبعاد المراجعة القضائية لإنذارات قانون TOLA، وذلك طبقاً للقرارات الإدارية (المراجعة القضائية) قانون 1977 م [45] وبمبدأ الضبابية في الفصل بين القوى، [46] وكذلك بشأن عدم التوافق مع إرشادات السياسة الخاصة بالنائب العام. [47]

وقد عُرض مشروع القانون على كلا المجلسين يوم 6 كانون الأول/ ديسمبر 2018 م، وحصل على الموافقة الملكية يوم 8 كانون الأول/ ديسمبر 2018 م، ليصبح جزءاً من القانون الأسترالي. وقد استغرق الأمر أقل من أربعة أشهر منذ تاريخ إقرار التشريع في صورة مسودة للعرض إلى وقت الإقرار، وهو ما وصفه البعض بعملية متسرعة، وبأن عملية التشاور المصاحبة لتشريع القانون كانت محدودة. [48]

وقد طالب الـ PJCIS بأن تبدأ اللجنة المستقلة للرقابة على تشريعات الأمن القومي INSLM عملية مراجعة لقانون TOLA يوم 26 آذار/ مارس 2019 م. وقد بدأت عملية المراجعة قبيل استكمال الـPJCIS للتقرير الثاني الخاص بالقانون يوم 3 نيسان/ أبريل 2019 م، الذي أوصى بما يأتي: (أ) توفير الموارد الكافية للجنة لتمكنيها من إتمام عملية المراجعة؛ (ب) ومطالبة الـ PJCIS بإصدار تقرير ثانٍ بحلول شهر حزيران/ يونيو 2020 م؛ (ج) وبأن تُوفَّر موارد كافية للمفتش العام للهيئة الاستخباراتية والأمن وأمين مظالم الكومنولث لضمان تنفيذهم جيداً للمسؤوليات الإضافية المنوطين بها بمقتضى قانون TOLA. [49]

وقد قدَّمت الـ INSLM التقرير الخاص بها للـ PJCIS يوم 30 حزيران/ يونيو 2020 م، التي قدَّمت

---

https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Scrutiny_Digest/2018, فيما بعد Scrutiny Digest 2018.

[45] انظر: Scrutiny Digest 2018، الهامش 25 السابق، صفحة 42. قانون القرارات الإدارية (المراجعة القضائية) 1977 (ADJR) (Cth) https://www.legislation.gov.au/Details/C2021C00035/Download.

[46] عندما يمكن لمسؤولي الفروع الإدارية الحكومية أن يمنحوا حصانة مدنية لبعض مقدمي الاتصالات المحددين للالتزام بالإنذارات الصادرة بمقتضى قانون TOLA (انظر: Scrutiny Digest 2018، الهامش 25 السابق، صفحات 47 و81).

[47] انظر: Scrutiny Digest 2018، الهامش 25 السابق، صفحة 47. "دليل صياغة إنذارات انتهاك جرائم الكومنولث وقوى فرض القانون"- إدارة النيابة العامة، أيلول/ سبتمبر 2011 https://www.ag.gov.au/sites/default/files/2020-03/A%20Guide%20to%20Framing%20Cth%20Offences.pdf

[48] انظر: هاردي كيه (2020) " قوانين التشفير الأسترالية: حاجة عملية أم إستراتيجية سياسية؟" مراجعة السياسة الداخلية (3) 9 https://policyreview.info/articles/analysis/australias-encryption-laws-practical-need-or-political-strategy

أو ما يأتي في (2019) "القوانين التكنولوجية التي تكتب سريعاً تهدد الخصوصية والأمن على الإنترنت" جرينليفت، https://www.greenleft.org.au/content/hastily-written-tech-laws-threaten-online-privacy-and-security

[49] اللجنة البرلمانية المشتركة للاستخبارات والأمن (2019) " مراجعة التعديلات التشريعية للاتصالات وغيرها من التشريعات – قانون (المساعدة والوصول للمعلومات) 2018 ، اللجنة البرلمانية المشتركة للاستخبارات والأمن PJCIS نيسان/ أبريل 2019:
https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/ReviewofTOLAAct/Report.

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

بدورها مجموعة من التوصيات لإجراء تعديلات على قانون TOLA.[50] وقد أوصت الـ INSLM بأن تُسحَب سلطة إصدار وإقرار الإنذارات التي تصدر بمقتضى هذا القانون من رؤساء الهيئات والحكومة، وتُحوَّل إلى هيئة جديدة تتولى الرقابة القضائية. ودعا تقرير الـ INSLM أيضاً إلى صياغة تعريف جديد لـ"الضعف النظامي"، ولحذف مصطلح الـ"الثغرة الأمنية" بشكل كامل من مشروع القانون.[51] وقد كان تقرير الـ INSLM في الأساس يهدف إلى تغذية تقرير ثالث للـ PJCIS بالمعلومات اللازمة، الذي كان مخططاً له أن يُسلَّم إلى الحكومة في حزيران/ يونيو 2020 م. وقد أُجِّل التقرير الثالث للـ PJCIS إلى أيلول/ سبتمبر 2020 م، لكن الـ PJCIS لم تُسلِّم التقرير حتى آذار/ مارس 2021 م.

ومن ثَم، وبعد مرور عامين على إقرار قانون TOLA، فإنه يبقى مثيراً للجدل، ويرجع جزء من ذلك إلى أن هذا القانون قد صِيغَ وأُقِر بشكل متسرع، دون إتمام تقييم كافٍ للتأثير المتوقع أو المحتمل له. وخلال البحث الأول الذي أجرته الـ PJCIS للقانون قبيل إقراره في كانون الأول/ ديسمبر 2018 م، سُئلت إدارة الشؤون الداخلية هل أعدت الحكومة بياناً تنظيمياً للتأثير المتوقع لهذا القانون RIS[52] لتقييم التأثير الاقتصادي المتوقع على الأعمال والمنافسة العالمية. وقد أجابت إدارة الشؤون الداخلية كتابياً بأن الحكومة قد أعدت فقط نسخة قصيرة[53] من البيان التنظيمي للتأثير، الذي توصل إلى نتيجة مفادها: "التأثير التنظيمي لإجراءات المساعدة من قطاع الصناعة سيكون بسيطاً".[54]

ولم نتمكن من إيجاد أي أدلة جوهرية على أن التأثير الاقتصادي المحتمل لقانون TOLA قد رُوعِيَ بشكل مفصل. ولسنا على علم بأي محاولة جادة لتقييم أو إحراز القانون لأي منافع

---

[50] INSLM (2020a) "ثق ولكن تأكد: تقرير بشأن قانون الاتصالات والتشريع الآخر (المساعدة والنفاذ) قانون 2018، والشؤون ذات الصلة "مراقب تشريعات الأمن القومي المستقل INSLM ، 9 تموز/ يوليو 2020 **https://www.inslm.gov.au/reviews-reports/telecommunications-and-other-legislation-amendment-act-2018-related-matters**

انظر: أيضاً INSLM (2020b) "ثق ولكن تأكد: ملخص التوصيات":
https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/AmendmentsTOLAAct2018/Additional_Documents.

[51] انظر: التوصيات 3 و9 و10 من INSLM (2020a)، الهامش 42 السابق.

[52] طبقاً لدليل التنظيم لحكومة أستراليا (الدليل)، الذي كان مطبقاً وقت عرض قانون TOLA وإقراره، فإن "كل مقترح سياسة مقدم لعرض أو إلغاء تنظيمٍ ما يجب أن يصاحبه بيان تأثير تنظيمي للحكومة الأسترالية" أو RIS، ويجب أن يُصاغ ذلك في مرحلة مبكرة من صياغة المقترح". (انظر: الصفحة 4 ، 2014، الدليل التنظيمي للحكومة الأسترالية، https://apo.org.au/sites/default/files/resource-files/2014-03/apo-nid270966.pdf

[53] أول خطوات الإعداد لتقديم بيان التأثير التنظيمي RIS في 2018 كان للهيئة المسؤولة عن أن تقدم ملخصاً مكتوباً يُعرَف بالتقييم المبدئي لمكتب تنظيم أفضل الممارسات OBPR في إدارة رئيس الوزراء، وكلما كان الـ RIS يقدم معلومات كافية تساعد الـ OBPR على فهم طبيعة السياسة محل النقاش، يجب على الـ OBPR أن تقدم ردها خلال خمسة أيام عمل مؤكدة، إذا كان هناك احتياج أم لا لتقديم الـ RIS، ونوعه إذا كان مطلوباً. وهناك ثلاثة أنواع من الـ RIS: استمارة طويلة، واستمارة عادية، واستمارة قصيرة. وفي كل الحالات يجب على الهيئة أن تتحمل التكاليف التنظيمية (وتشمل تكاليف التعويضات) بغضّ النظر عن نوع الـ RIS المنطبق عليها. (انظر: الدليل، الهامش 33 السابق، صفحة 11)

[54] الصفحة 13، "مراجعة تعديلات تشريع الاتصالات والتشريع الآخر (المساعدة والنفاذ) – مشروع القانون 2018- التسليم رقم 18- التسليم التكميلي 6: رد إدارة الشؤون الداخلية على الأسئلة عن الإنذارات" الإدارة الأسترالية للشؤون الداخلية، نوفمبر 2018، https://www.aph.gov.au/DocumentStore.ashx?id=13d6d87f-a64e-4e7c-8cc1-83d939e9fe1d&subId=660956

(فيما بعد، مراجعة الـ DHS لقانون TOLA)

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

حقيقية (على سبيل المثال في تحسين الأمن القومي أو إنفاذ القانون)[55] أو عن الأضرار الاقتصادية المحتملة التي قد يسببها قانون TOLA إذا تسبب في الإضرار بالنواحي الاقتصادية للشركات الأسترالية أو تهديد الثقة الرقمية.[56]

وفي الفصول اللاحقة من التقرير نشرح سبب حيوية التشفير في دعم الأمن الرقمي، بالنظر إلى أهمية المعلومات الرقمية للاقتصاد الأسترالي والعالمي ، وكيف أن تهديد التشفير يهدد بحدوث أضرار اقتصادية جسيمة. وندرس الآليات المختلفة التي يتسبب من خلالها قانون TOLA في تهديد الثقة الرقمية والإضرار بالاقتصاد الأسترالي.

الاعتبارات التكنولوجية

أُشركت هيئات الاستخبارات وإنفاذ القانون لاختبار فرضية التأثير السلبي للمساعي التشريعية والقانونية الأخرى لتقويض التشفير على الاعتبارات الاقتصادية، مثل الأعمال والابتكار والتجارة والاستثمار الداخلي. في حين أن هذا التقرير هو تحليل اقتصادي، فإن تقويض التشفير (أو كما يصفه قانون TOLA: "إزالة التشفير") يشمل التكنولوجيا. ولهذه الغاية، يبحث هذا القسم من التقرير الآثار التكنولوجية لإزالة التشفير أو تطويقه، ويوفر إطاراً لكيفية تأثير الاعتبارات التكنولوجية على القضايا الاقتصادية. وليس الهدفُ هنا تقديمَ تحليل فني متعمق، ولكن ببساطة توفير سياق للتحليل الاقتصادي.

ومن المعترف به على نطاق واسع أن التشفير القوي أمر ضروري لكثير من الأنشطة المهمة في مجتمعنا، مثل التجارة والحرية وحرية التعبير والأمن القومي.[57] وقد يسمح التشفير القوي للمجرمين بالتواصل دون أن يُلاحظوا أو يُفهموا، وتؤكد هيئات الاستخبارات وإنفاذ القانون أن هذا التشفير يعوق قدرتهم على تنفيذ مهامهم. وسَعَت هيئات الاستخبارات وإنفاذ القانون إلى فرض قوانين من شأنها أن تلزم مقدمي خدمات الاتصالات المحدودة الذين يقدمون منتجات وخدمات مشفرة بالمساعدة في توفير وصول غير مشفر إلى الاتصالات المستهدفة، بناءً على أمر أو إشعار قانوني. وغالباً ما يشار إلى هذا النوع من الوصول القانوني لطرف ثالث بأنه وصول استثنائي[58] إلى المحتوى المشفر.

---

[55] القول بأن هناك جرائم بشعة (الإرهاب والاتجار بالبشر، ... إلخ) وفرض تهديد أمني على الأمن القومي والسلامة، أمرٌ صحيح، ولكنه غير كافٍ لتوضيح تقييم التأثير لقانون TOLA، وكيف سيتناول القانون هذه الأنواع من الجرائم وغيرها، التي ربما يجب على القانون التطرق لها.

[56] "طلب حرية المعلومات" نسخة من الاستمارة القصيرة قُدمت لإدارة الشؤون الداخلية يوم 1 تشرين الأول/ أكتوبر 2020. وفي 1 آذار/ مارس 2021 صرحت إدارة الشؤون الداخلية أن هذا الطلب كان وثيقة إعفاء، ولن يُطرَح.

[57] اجتماع المائدة المستديرة لجمعية الإنترنت - تشاتام هاوس بشأن التشفير والوصول القانوني، تشرين الأول/ أكتوبر 2017: https://www.internetsociety.org/resources/doc/2018/internet-society-chatham-house-roundtable-on-encryption-and-lawful-access.

[58] تشير متطلبات الوصول الاستثنائية إلى بعض وسائل السماح لفرض القانون، من خلال القدرة على الوصول القانوني إلى محتوى الاتصالات والبيانات المشفرة في شكل غير مشفر. انظر: 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, United Kingdom +44 7554 065 718

وبين الخبراء التقنيين إجماعٌ قوي على أن مثل هذه التدخلات، حتى بالطريقة الأكثر استهدافاً، تزيد المخاطر، ولها تأثير سلبي على تآكل الثقة في الخدمات المشفرة.[59] وقد أشار خبراء الأمن السيبراني البارزون، في تحليل لأساليب الوصول الاستثنائية التي تُناقَش في الاتحاد الأوروبي، إلى أن كل طريقة وصول استثنائية ستؤدي إلى ظهور ثغرات أمنية يمكن لطرف ثالث (على سبيل المثال: جهة فاعلة سيئة) استغلالها للتأثير على جميع المستخدمين.[60] وقد تؤدي إمكانية الوصول الاستثنائي إلى إضعاف الثقة، والتقليل من استخدام التشفير والخدمات التي تعتمد عليها، مثل التجارة أو التمويل الإلكترونيين.

ونتناول فيما يلي مخاوف محددة تتعلق بالسماح بالوصول إلى البيانات المشفرة كما هو مقترح في قانون TOLA.[61] ونتناول أولاً بغير تفصيل الأسئلة التالية:

- ما التشفير؟ وكيف يُستخدَم؟ وما قيمته؟
- كيف يمكن إتاحة الوصول إلى البيانات المشفرة؟ وكيف يُعرَّف ذلك في القانون؟
- ما العواقب التقنية المحتملة لقانون TOLA؟

ولتلخيص هذا القسم، نصِفُ التحديات التي تواجه تحقيق تدخل مستهدف على خدمة التشفير، ونوضح كيف يمكن تطبيق مثل هذه التدخلات بشكل ضار يتجاوز الهدف، على الرغم من النيات الحسنة؛ إما لهيئات الاستخبارات وإنفاذ القانون LEIAs، أو لمقدمي خدمات الاتصالات المحددة DCPs، ونجد أن اللغة الغامضة والمتطلبات والالتزامات المطبقة على نطاق واسع في القانون تزيد المخاوف بشأن القدرة على تحقيق تدخل مستهدف. في حين أنه من الصعب تحديد تأثير جهود إزالة التشفير أو تقويضه، فإننا نرى زيادة في المخاطر واحتمال انخفاض الثقة في هذه الأنظمة المشفرة. ويمكن أن يقوض قانون TOLA ويقلص ثقة الجمهور في العديد من الخدمات المشفرة التي نستخدمها جميعاً حالياً كلَّ يوم. ويمثل مجرد تصور ضعف التشفير أو تهديد الهيئات الحكومية التي لديها القدرة على جمع المعلومات تقويضاً للثقة.

4.1 ما التشفير؟

للتشفير تعريفات عديدة، ولكن التعريف البسيط والشامل إلى حدٍّ ما هو: "أي إجراء مستخدم في التشفير لتحويل نص عادي إلى نص مشفر لمنع أي شخص دون المستلم فهمَ المقصود من قراءة تلك البيانات."[62] وبالطبع، في سياق القضية المطروحة، يمكن أن تعني كلمة "نص" أي

[59] Keys Under Doormats: فرض عدم الأمان من خلال مطالبة الحكومة بالوصول إلى جميع البيانات والاتصالات https://www.csail.mit.edu/research/keys-under-doormats، والأكاديمية الوطنية للعلوم. "فك تشفير نقاش التشفير: إطار عمل لصانعي القرار" (2018) https://www.nap.edu/read/25010

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

61 استُخلِصت هذه النتائج من تحليل القانون المقترح، ومراجعة الصحافة التجارية والمنشورات الأكاديمية، والتعليقات المقدمة، بوصفها جزءاً من السجل العام، فضلاً عن المقابلات مع عدد من مقدمي الاتصالات الذين يقدمون خدمات مشفرة.

[62] NIST SP 800-101 ، REV 1. https://doi.org/10.6028/NIST.SP.800-101r1، تحت التشفير، تمت زيارته 11/2020

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

نوع من أنواع الاتصالات، مثل الصوت، والصور، والشخصيات، والفيديو، والدردشة، والمواقع الإلكترونية وغيرها.[63] والغرض من التشفير توفيرُ وسيلةٍ لمنع أولئك الذين يعترضون اتصالاً مشفراً من فهم محتواه. وتُستخدَم لوغاريتمات تشفير مع رسالة نصية غير مشفرة بالإضافة إلى "مفتاح" لإنتاج نص مشفر. وتعمل لوغاريتمات فك التشفير المستخدمة عند الاستلام على عكس هذه العملية لإعادة إنتاج رسالة غير مشفرة، وهو ما يعني أن المرسل إليه المقصود بالرسالة المشفرة يجب أن يكون لديه المفتاح لقراءة تلك الرسالة. ويمكننا التفكير في التشفير بوصفه نظاماً يتضمن عناصر عديدة تعمل معاً عبر الإنترنت. ولا يقتصر التشفير على العناصر الرياضية المتماثلة في البرنامج فحسب، بل يمثل أيضاً مجموعة واسعة من اللوغاريتمات والوظائف المهمة، مثل التبادل الآمن للمفاتيح. ومن المفترض أنه لا ينبغي أن يمتلك المفاتيحَ أيُّ شخص سوى المرسِل والمرسَل إليه المقصود.[64]

إن السرية التي يوفرها التشفير توازي فقط قوة تنفيذها. ويمكن اعتبار التشفير القوي بمنزلة خزينة بنك قوية، فكلاهما يجعل الوصول إلى ما بداخلهما غير عملي، إذ سيستغرق الأمر الكثير من الوقت والمال والموارد و/ أو الخبرة لفك التشفير تماماً، كما في حال اقتحام قبو البنك. وإذا كانت لوغاريتمات التشفير ضعيفة، يمكن استرداد الرسالة غير المشفرة بسهولة إلى حد ما عن طريق المعترض. وتشبه اللوغاريتمات الضعيفة قفلاً بسيطاً على الخزينة، ولكن لا فائدة للقفل القوي على الخزينة إذا أمكن فك المفصلات ورفع الباب. ويجب أن تساهم جميع أجزاء نظام التشفير في قوته. ومع زيادة التشفير القوي، يصبح فك التشفير صعباً للغاية، بل أقرب إلى المستحيل. ومن المهم أيضاً ضمان توزيع المفاتيح الخاصة على المرسَل إليهم المقصودين فقط، وليس أي جهات خارجية أخرى تستطيع استخدامها للوصول إلى البيانات المشفرة. وللمقارنة أيضاً، تُفتح أقوى الخزائن إذا تمكنت من الوصول إلى المفاتيح.

وجدير بالذكر أيضاً أن التشفير يمكن تنفيذه في عدة نقاط في الشبكة، ومن قِبَل مجموعة متنوعة من الكيانات. وفي الواقع، أصبح من السهل الآن للغاية للمستخدمين تنفيذ خدماتهم القوية المشفرة من الطرف إلى الطرف دون الاستفادة من خدمة تجارية. وكما سنناقش لاحقاً، ترتب على ذلك آثار على هيئات الاستخبارات وإنفاذ القانون.

4.2 كيف يُستخدَم التشفير؟ وما قيمته؟

يحتوي التشفير على مجموعة كبيرة ومتنوعة من التطبيقات. ويُستخدَم في المقام الأول لحماية البيانات (أي الحفاظ على سرية البيانات وحمايتها من التلاعب بها)، التي تُخزَّن ("البيانات

[63] قد تنشأ أيضاً مخاوف تتعلق بالأمان والخصوصية، وترتبط بالبيانات الوصفية للاتصالات الآمنة، على الرغم من أن هذا المحتوى قد لا يكون محمياً من خلال التشفير. ويتضمن ذلك معلومات عن مصدر الاتصالات ووجهتها، والتطبيقات المستخدمة، ووقت حدوث الاتصالات، وغير ذلك. وينشأ العديد من المخاوف نفسها لحماية البيانات الوصفية، كتأمين محتوى الاتصالات، ومن ثَم فإن هذه المعلومات محمية قانوناً، وتتطلب مذكرة من الوكالات الحكومية للحصول على محتواها.

[64] على الرغم من أهمية تفاصيل التبادل الرئيسي، والتشفير المتماثل وغير المتماثل، والقضايا ذات الصلة، فهي خارج نطاق هذا التقرير. وللحصول على شرح مفصل لموضوع التشفير، اطلع على: https://www.internetsociety.org/issues/encryption/

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

الثابتة") أو التي تُرسَل ("البيانات المتحركة"). وبالطبع، يريد المستخدمون حماية بياناتهم أثناء الحركة أو أثناء عدم النشاط. وللتشفير مجموعة واسعة من الاستخدامات، تشمل – على سبيل المثال: حماية المعاملات المالية، وسجلات الرعاية الصحية، والتخزين الآمِن للملفات، وتشفير القرص، وإغلاق الجهاز، والتحقق من بيانات الاعتماد للوصول إلى الشبكات الخاصة الافتراضية، وتصفح الويب الآمِن، والرسائل الخاصة أو المجهولة، وأمن الحوسبة السحابية، وغير ذلك الكثير.[65] ومن خلال توفير هذه الحماية، يؤدي التشفير دوراً مهماً في تمكين أجزاء مهمة من اقتصادنا، من خلال ضمان الثقة في التجارة الإلكترونية، والتمويل الإلكتروني، والصحة الإلكترونية، والتعلم الإلكتروني، وتخزين المعلومات الآمِن، والاتصالات الخاصة الآمنة، ومن خلال ضمان حرياتنا المدنية، مثل الخصوصية وحرية التعبير وحرية تكوين الجمعيات.

بينما حاولت بعض الأبحاث (كما هو موضح في قسم التحليل الاقتصادي من هذا التقرير) تعيين قيمة نقدية للتشفير، لكنها مهمة صعبة نظراً للطريقة التي يتداخل به التشفير في حياتنا المعاصرة، والطرق التي لا حصر لها التي نعتمد عليها في حياتنا اليومية، والآثار التي لا تُحصَى من الأدوار التي يؤديها التشفير الآن في حياتنا.[66] وكما هو موضح سابقاً، يوفر التشفير اللبِنة الأساسية للثقة على الإنترنت، التي أتاحت النمو الهائل للاتصالات، والتجارة، والخدمات المالية والصحية عبر الشبكة والعالم. وخلال جائحة كورونا، أتاح التشفير لشركات عديدة مرونة العمل من المنزل، وهو ما سمح للتجارة بالاستمرار، على الرغم من قيود الجائحة والوباء.

وتكمن قيمة التشفير في تأمين تلك الخدمات وتوفير أساس للثقة. ولا تتوفر هذه الثقة من دون تشفير قوي، ويضر ذلك النقص في الثقة بالخدمات المذكورة سابقاً. وتُعَد الثقة عبر التشفير الأساسَ لجميع هذه الأنشطة على الإنترنت، ومن دونها قد لا يكون لدى الأفراد والكيانات استعدادٌ للمشاركة في كل هذه الأنشطة عبر الإنترنت. وفي الواقع، مع استمرار تحوُّل مجتمعنا إلى اقتصاد المعلومات والبيانات، تظهر الحاجة لمزيد من التشفير وليس أقل، بل إن تقويض قوتها يقودنا إلى الاتجاه الخاطئ.

[65] الأكاديمية الوطنية للعلوم. "فك تشفير نقاش التشفير: إطار عمل لصانعي القرار" (https://www.nap.edu/read/25010201)

[66] انظر المناقشة في القسم الاقتصادي من هذه الورقة. ويُقدر الاستثمار في الأمن السيبراني بمئات المليارات من الدولارات الأمريكية. انظر: دي وجون سكوت (2018) "الآثار الاقتصادية للتشفير المتقدم، 1996-2017"، المُعد للمعهد الوطني للمعايير والتكنولوجيا، NIST GCR 18-017، متاح على: https: // doi.org/10.6028/NIST.GCR.18-017، وقد نُشر في صورة مقال في مجلة: ليبتش، دي بي، فيريس س، وسكوت، جيه، تي، (2019). الآثار الاقتصادية لمعيار التشفير المتقدم، 1996-2017. حوليات سياسة العلوم والتكنولوجيا، 3 (2) ، 257-142. 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, United Kingdom +44 7554 065 718

وصرحت شركة Apple أيضاً بأنه: "تحدث كل يوم أكثر من تريليون معاملة عبر الإنترنت بأمانٍ نتيجةً للاتصالات المشفرة.[67] "ومن المتعارف عليه أن أفضل طريقة لتعزيز الأمن السيبراني الدعوةُ لاعتماد أوسع لتشفير رقمي قوي من الطرف إلى الطرف.[68]

4.3 كيف يمكن توفير وصول استثنائي؟

يمكن للمجرمين استخدام ميزات التشفير نفسها التي تجعله جزءاً مهماً من الإنترنت لإخفاء الأنشطة غير القانونية، عبر مجموعة واسعة من التقنيات والتطبيقات. ويعوق ذلك قدرةَ هيئات الاستخبارات وإنفاذ القانون على سهولة اعتراض وعرض محتوى اتصالات المستهدفين في التحقيقات. ويسعى الوصول الاستثنائي إلى توفير وسيلة لهيئات الاستخبارات وإنفاذ القانون للحصول على نص رسالة غير مشفرة من محتوى الاتصالات المشفرة.

وعامةً، يمكننا التفكير في الوصول الاستثنائي على النحو التالي:

- إزالة التشفير أو التوثيق.

---

[67] الصفحة 1، "مراجعة قانون الاتصالات السلكية واللاسلكية وتعديل التشريعات الأخرى (المساعدة والوصول) لعام 2018 التقديم 53، شركة أبل، متاح على:
https://www.aph.gov.au/DocumentStore.ashx؟id=ecd6be12- ab84-43de-be61-1599e1db2a74 & subId = 661073.

[68] هناك العديد من البيانات الرسمية من صانعي السياسات في الدول في جميع أنحاء العالم عن قيمة الأمن السيبراني. على سبيل المثال:

- أقر المدعي العام ويليام بار ضمنياً أنه لا طريقة لتوفير وصول الحكومة إلى البيانات المشفرة دون خلق نقاط ضعف يمكن للجهات الفاعلة الخبيثة استغلالها، بحجة أن الخطر "مقبول لأننا نتحدث عن منتجات وخدمات استهلاكية، مثل المراسلة، الهواتف الذكية، والبريد الإلكتروني، وتطبيقات الصوت والبيانات، ولا نتحدث عن حماية رموز الإطلاق النووية للأمة." (راجع" حديث المدعي العام الأمريكي ويليام بار أن على الأمريكيين قبول المخاطر الأمنية للتشفير في الأبواب الخلفية" ، TechCrunch، 23 تموز/ يوليو 2019 ، متاح على: https://techcrunch.com/2019/07/23/william-barr-consumers-security-risks-backdoors/?guccounter=1).
- قال آش كارتر، وزير الدفاع الأمريكي الأسبق، بأنه "لا جدوى من شراء كل هذه الطائرات، والسفن والدبابات ووجود جنود وبحارة وطيارين ومشاة البحرية إذا لم أتمكن من الاتصال بهم... لذا فإن أمن البيانات ضرورةٌ مطلقة لنا... لذلك نحن نساند الأمان القوي للبيانات، بما في ذلك التشفير القوي... بلا شك". (انظر ملاحظات الوزير كارتر في محادثة" فايرسايد "مع تيد شلاين في سان فرانسيسكو، "نسخة مكتوبة، وزارة الدفاع الأمريكية، 2 آذار/ مارس 2016، متاح على: https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/684858/remarks-by-secretary-carter-in-a-fireside-chat-with-ted-schlein-in-san-francisc/;
- يقول روبرت هانيجان، المدير السابق لمكاتب الاتصالات الحكومية البريطانية في المملكة المتحدة: "التشفير شيء جيد للغاية، فهو يحافظ على سلامتنا وأماننا جميعاً... إن البناء في الأبواب الخلفية يمثل تهديداً للجميع، وليس من الجيد إضعاف الأمن حتى يتمكن الجميع من التعامل مع أقلية"(اقرأ: رئيس المخابرات البريطانية السابق يحذر من خطورة خطة أمبر راد لتمرير قانون جديد لتشفير الهواتف الذكية"، ذي إندبندنت، 10 تموز/ يوليو 2017، متاح على:-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
- اختتمت اللجنة الدائمة المعنية بالسلامة العامة والأمن القومي التابعة لمجلس العموم الكندي تقريرها لعام 2019 بشأن "الأمن السيبراني في القطاع المالي كمسألة أمن قومي" بالموافقة على "أنه من المهم، لأسباب تتعلق بالأمن والخصوصية، أن يحصل كل كندي على تشفير قوي" والتوصية بأن "ترفض حكومة كندا مناهج الوصول القانوني الذي من شأنه إضعاف الأمن السيبراني (راجع: "الأمن السيبراني في القطاع المالي كمشكلة أمنية وطنية"، مجلس العموم الكندي، حزيران/ يونيو 2019، متاح على: https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP10589448/securp38/securp38-e.pdf)
- وفقاً للمفوضية الأوروبية: "يُعد التشفير القوي الأساسَ لأنظمة تحديد الهوية الرقمية الآمنة التي تؤدي دوراً رئيسياً في الأمن السيبراني الفعال؛ وهي تحافظ كذلك على أمان الملكية الفكرية للأفراد، وتمكن من حماية الحقوق الأساسية، مثل حرية التعبير وحماية البيانات الشخصية، وتضمن تجارة آمنة عبر الإنترنت. (راجع الصفحتين 9-10 في "المرونة والردع والدفاع: بناء أمن إلكتروني قوي للاتحاد الأوروبي"، "المفوضية الأوروبية، بروكسل، 13 أيلول/ سبتمبر 2017، متاح على: https://ec.europa.eu/transparency/regdoc/rep/10101/2017/EN/JOIN-2017-450-F1-EN-MAIN-PART-1.PDF).

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

- عرض نقاط الضعف والثغرات.
- أو عرض أجهزة أو برامج لتوفير الوصول إلى المحتوى الذي فُك تشفيره.

ويمكن تحقيق ذلك من خلال مناهج مثل الضمان الرئيسي، وتغيير إدارة المفاتيح، وإضافة نقطة ضعف في التشفير أو الأساليب أو البروتوكولات، أو تطبيقات خدمة التشفير، أو ببساطة إيقاف تشغيل التشفير.[69]

وفي أستراليا، يسمح قانون TOLA لهيئات الاستخبارات وإنفاذ القانون بفرض التزامات قانونية على مقدمي خدمات الاتصالات المحددة، ويطلب منهم المساعدة في توفير وصول تلك الهيئات إلى الخدمات المشفرة وبياناتها. وما لا يوضحه هذا القانون هو كيف يمكن توفير هذا الوصول. ولن نحاول مناقشة الأساليب التقنية مناقشةً شاملةً لتوفير الوصول إلى البيانات المشفرة (يقع هذا خارج نطاق هذا التقرير)؛ وبدلاً من ذلك، سندرس ببساطة ونناقش الآثار التكنولوجية العالية المستوى لقانون TOLA.[70]

ويوفر الضمان الرئيسي، إذ يحتفظ بمجموعة إضافية من مفاتيح فك التشفير طرفٌ ثالث "موثوق به" "كضمان"، التي تقدمها لهيئات الاستخبارات وإنفاذ القانون عندما يكون ذلك مناسباً من الناحية القانونية، نوعاً واحداً من الوصول للأطراف الثلاثة المصرح لهم (على سبيل المثال: هيئات الاستخبارات وإنفاذ القانون). ومع ذلك، بسبب المخاوف بشأن من يمكنه الوصول إلى هذه المفاتيح (على سبيل المثال: يمكن سرقتها أو إساءة استخدامها أو فقدها أو مشاركتها)، ولأن أساليب الضمان الرئيسي لا تحتاج قانون TOLA، فإننا لا نناقش هذا النهج هنا إلا لملاحظة أن المجتمع الفني كان ولا يزال يعارض هذا النهج[71].

[69] يمكن أن تتضمن الوسائل التقنية لتوفير الوصول إلى المحتوى المشفر مجموعة واسعة من الأساليب (بعضها خارج نطاق TOLA)، مثل: الاستفادة من نقاط الضعف التي اكتُشفت، وعرض نقاط الضعف، وهجمات أوسع باستخدام أدوات مثل راصد لوحة المفاتيح أو أدوات التطفل، وإزالة ضوابط الأمان من نظام أو برنامج أو جهاز معين، وتعطيل خدمات التشفير أو تخفيضها، واعتراض جلسات التشفير بين المتصفح والخادم، وتبادل المفاتيح، ومفتاح الضمان، أو غيرها من الأساليب الممكنة. ومرة أخرى، إن المناقشة الأكثر شمولاً تقع خارج نطاق هذا التقرير.

[70] لدى أستراليا بالفعل قوانين قائمة توفر الوصول القانوني إلى البيانات، التي من شأنها أن تقدم لهيئات الاستخبارات وإنفاذ القانون مساراً قانونياً للحصول على البيانات المشفرة من عدد كبير من مقدمي الخدمات. وكما هو مذكور في الفصل القانوني، يبدو أن TOLA يعمل على توسيع القانون الحالي إلى الحد الذي يشير فيه صراحة إلى إزالة التشفير، وتوسيع هذه السلطة إلى مقدمي خدمات الاتصالات المحددة DCPs من غير شركات النقل، ومقدمي خدمات النقل، ومشغلي المرافق وشبكات الاتصالات والخدمات التي لا تعد خدمات اتصالات سلكية ولاسلكية بشكل صارم، والتي كان العديد منها بالفعل (قبل TOLA) خاضعاً للتشريعات الشاملة لمجتمع الاستخبارات الوطنية. وتشمل التشريعات السابقة قانون الاتصالات السلكية واللاسلكية (الاعتراض والوصول) لعام 1979 (TIA) والتشريعات ذات الصلة اللاحقة التي أعقبت هجمات 11 أيلول/ سبتمبر الإرهابية في عام 2001، ومنذ ذلك الوقت أقر البرلمان الأسترالي أكثر من 124 قانوناً لتعديل الإطار التشريعي لمجتمع الاستخبارات الوطني.

[71] انظر: أبلسون، هـ. ر. أندرسون، س. بيلوفين، جيه بينوليه، إم. بليز، دابليو. ديفي، جيه جيلمور، إم جرين، إس. لانداو، بي. نيومان، آر. ريفست، جيه. شيلر، ب. شينير، إم سبكتر، إم سبيكتر ، ود. ويتزنر (2015)، "المفاتيح المتاحة: التفويض بعدم الأمان من خلال مطالبة الحكومة بالوصول إلى جميع البيانات والاتصالات،" Journal of Cybersecurity، 1 (1)، الصفحات 69-79، وللحصول على نسخة ورقة العمل الموسعة، انظر التقرير الفني (MIT-CSAIL-TR-2015/026)، 6 تموز/ يوليو 2015، متاح على: https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf.

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

وهناك طريقة أخرى لتنفيذ مثل هذا الوصول، وهي دمج نقطة ضعف "الباب الخلفي"[72] في آلية التشفير الأساسية أو البرامج ذات الصلة. وتكمن المشكلة هنا في أن هذه العملية، طبقاً للتصميم، تشكل ضعفاً أو ثغرة أمنية، ويُقوَّض التشفير نتيجةً مثل هذا التلاعب. وأيضاً تتعارض إضافة نقاط الضعف ببساطة مع القاعدة المطبقة بصرامة لبناء التشفير القوي وتقييمه، فضلاً عن عملية اكتشاف نقاط الضعف والإعلام بها وتصحيحها. فهي لا تضعف التنفيذ الفعلي للتشفير فحسب، بل تقوض الثقة في مفهوم التشفير بوصفه أداةً تدعم الكثير مما نفعله بصفتنا مجتمعاً عبر الإنترنت.[73]

4.4 كيف يُعرَّف هذا النوع من الوصول للمعلومات؟

كما سنناقش فيما بعد، تطرح اللغة الحالية المستخدمة في قانون TOLA عدداً من الأسئلة والمخاوف بشأن التنفيذ. والرسالة الواضحة، التي سمعناها من جميع الشركات التي أجرينا مقابلات معها، هي أنها ببساطة لا تعرف ما يمكن توقعه، على الرغم من أنه من المألوف أن تكون جوانب اللغة التشريعية واسعة النطاق والتطبيق عن قصد. ونحن نحدد عدم الوضوح، وننظر في عواقبه.

ومن أول الأشياء المُلاحظة عند قراءة قانون TOLA أنه يشرح بشكل أكثر استفاضة ما لا يمكن أن يتطلبه الإشعار بدلاً من متطلباته. وليس من المستغرب أن هذا النهج هو إحدى طرق تضييق النطاق بطريقة تجعله أكثر قبولاً ويصعب الاختلاف معه. ومع ذلك، عند قراءة هذه اللغة يصبح من الصعب فهم المعنى، ولا يمكن للقارئ العادي التأكد من التعريفات والالتزامات.

فعلى سبيل المثال، ينص قانون TOLA على أنه "يجب ألَّا يُطلَب من مقدم الاتصالات المعين أو يُفرَض عليه تنفيذ أو بناء ثغرة أمنية نظامية أو ضعف نظامي، وغير ذلك." وينص كذلك على أن الإشعارات يجب ألَّا يكون لها تأثير "(أ) طلب أو اشتراط أن ينفِّذ مقدم اتصالات معين أو يبني ثغرة أمنية نظامية، أو ثغرة منهجية، في شكل من أشكال الحماية الإلكترونية؛ (ب) أو منع مقدم اتصالات معين من تصحيح ضعف نظامي، أو ثغرة منهجية، في شكل من أشكال الحماية الإلكترونية." ويضيف القانون أن الإشعارات لا يمكن أن تطلب من مقدم الخدمة "تنفيذ أو بناء قدرة جديدة لفك التشفير"، أو "جعل الأساليب المنهجية للمصادقة أو التشفير أقل فعالية"، أو تقديم ثغرة أو ضعف "انتقائي" من شأنه "تعريض أمن أي معلومات يحتفظ بها أي شخص

[72] كما ذكرنا سابقاً، يُشار إلى إحدى طرق الحصول على وصول بديل إلى محتوى الاتصالات المشفرة بأنها "باب خلفي"، تماماً كما يسمح الباب الخلفي للمنزل ببديل لدخول المبنى. وبالطبع، لا يريد معظمنا باباً خلفياً به نقطة ضعف معروفة في منزلنا (أي ضعف الأمان)، ولن يرغب معظمنا في تقديم مفاتيح الأبواب للحكومة (أي الضمان الرئيسي).

[73] على سبيل المثال: راجع الباب الخلفي لجونيير الخاص بمولد DUAL-EC-DRBG للأرقام العشوائية: https://dl.acm.org/doi/pdf/10.1145/2976749.2978395.

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

آخر للخطر، "أو تخلق" خطراً مادياً يتمثل في إمكانية وصول طرف ثالث غير مصرح له إلى المعلومات الآمنة."[74]

وقد أُضيفت التعريفات التالية إلى التشريع[75]:

الثغرة النظامية: تعني ثغرة تؤثر على فئة كاملة من التكنولوجيا، ولكنها لا تتضمن ثغرة انتقائية لواحدة أو أكثر من التقنيات المستهدفة المرتبطة بشخص معين. ولهذا الغرض، ليس من المهم تحديد هوية الشخص.

الضعف المنهجي: يعني ضعفاً يؤثر على فئة كاملة من التكنولوجيا، ولكنه لا يشمل نقطة ضعف انتقائية لواحدة أو أكثر من التقنيات المستهدفة المرتبطة بشخص معين. ولهذا الغرض، ليس من المهم تحديد هوية الشخص.

وبينما تحاول هذه التعريفات تقليل المخاطر على المستخدمين غير المستهدفين، لا تزال الرؤية غير واضحة، وهناك تداعيات للنتائج المحتملة. وتوضيح المقصود بالتكنولوجيا المستهدفة هو الخطوة الأولى. وقد يكون من المفيد أيضاً فهم أنه لا يمكن عامةً استخدامُ الثغرات المنتقاة على التقنيات المستهدفة على المستوى النظامي، وهي نقطة لاحظها الخبراء الفنيون باعتبارها مشكلة متأصلة في هذا النهج.[76] ويوجد احتمال كبير لتسريب أو اكتشاف النهج المتبع لتنفيذ ثغرة مستهدفة (أو ربما التنفيذ الفعلي لهذه الثغرة) واستغلاله من قبل الآخرين. وفي هذه المرحلة، قد يُطبَّق على هدف واحد أو أكثر من الأهداف الأخرى.

وفي حين توجد بعض الطرق الأساسية لتوفير الوصول إلى أشياء، مثل الاتصالات الصوتية للهاتف المحمول، وبعض الأجهزة المقفلة، فإن العديد من خدمات الإنترنت الحالية يستخدم تشفيراً قوياً من الطرف إلى الطرف، وهو ما قد يحد قدرة مقدم الخدمة على المساعدة في توفير وصول استثنائي (هذا ما يعترف به قانون TOLA).[77] وعلاوة على ذلك، أصبح من السهل الآن تنفيذ أو الحصول على خدمة اتصالات قوية من الطرف إلى الطرف دون مساعدة مقدم الخدمة، لذلك لن يكون لدى مقدم الخدمة القدرة على الكشف عن المحتوى إذا طلبت منه ذلك هيئاتُ الاستخبارات وإنفاذ القانون.

وفي واقع الأمر، يمكن تنزيل البرامج المفتوحة المصدر وتنفيذها لهذا النوع فقط من الوظائف، وهو ما يزيد صعوبةَ إدخال ثغرة أمنية دون اكتشافها. ومن المحتمل ألَّا يتمكن أي مقدم (حتى

---

[74] لهذه الاقتباسات وللاقتباسات السابقة في هذه الفقرة، راجع صفحتَي 85-84 من قانون TOLA، *supra* Note 2.

[75] صفحة 12 من من قانون TOLA، *supra* Note 2.

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

[77] تقلل الشركات التي تقدم خدمات لإنهاء أحد طرفي القناة المشفرة معايير منخفضة لاعتراض الاتصالات. ولديهم حق الوصول إلى المحتوى غير المشفر. وفي مثل هذه الحالات، فإن الاستجابة لطلب الباب الخلفي يجب أن تفرض الحد الأدنى من التكاليف المباشرة.

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

منشئ البرامج المفتوحة المصدر - بافتراض أن قانون TOLA يمكنه حتى الوصول القانوني إلى هذا المقدم) تزويد الوكالات الحكومية بالمعلومات التي يطلبونها من هذا الوصول.[78] ومن المهم هنا أنه لا يمكن عملياً منع الأشخاص من استخدام تشفير قوي من الطرف إلى الطرف، إذا كان لديهم الدافع لفعل ذلك. ومن غير الواقعي توقُّع أن اختراع لوغاريتمات التشفير أو عدم نشرها كأنه لم يكن، مثلما لا يُعقَل توقُّع إلغاء برنامج التشفير المفتوح المصدر.

4.5 ما تبعات TOLA؟

ناقشت دراساتٌ فنية واقتصادية وتجارية عديدة المخاوفَ المتعلقة بتوفير وصول استثنائي إلى التشفير.[79] وتتراوح هذه المخاوف بين الإشارة إلى الطرق التي يمكن أن يجري من خلالها إضعاف التشفير، والمشكلات التي يطرحها تآكل الثقة، والاهتمامات الأوسع للإنترنت المنقسم. وقد قوبل الوصول الاستثنائي إلى التشفير مراراً وتكراراً بمقاومة قوية من الخبراء الفنيين على مدى العقود الثلاثة الماضية، ولم تظهر الجهود الأخيرة لدعم الوصول الاستثنائي مساراً يتغلب على المخاوف الفنية، وهذا يشمل النهج المقترح في قانون TOLA. وفي هذا القسم، نحاول تقديم منظور بشأن تحديات الوصول الاستثنائي وعواقبه، وبشكل أكثر تحديداً الصعوبات التي يطرحها تنفيذ هذا القانون. وفي الجزء المتبقي من هذا القسم، نتطرق لمشاكل مثل: إضعاف التشفير، واستهداف غير واضح، وتطوير الأساليب والاحتفاظ بها، وإعادة الاستخدام، والتصعيد، والتسريب والمشاركة، وعملية والتزامات غير مؤكدة.

إضعاف التشفير

وينص قانون TOLA على أنه "لا يمكن مطالبة مقدم الاتصالات بما يلي: بناء أو تنفيذ ضعف نظامي أو ثغرة نظامية في شكل من أشكال الحماية الإلكترونية، أو منع مقدم اتصالات معين من تصحيح ضعف نظامي أو ثغرة نظامية في شكل من أشكال الحماية الإلكترونية."[80] وهنا، كان

[78] على سبيل المثال، قد يكون الفاعلون السيئون، الذين يعرفون أنهم أهداف محتملة لهيئات إنفاذ القانون أو هيئات الاستخبارات، أكثر عرضة لاستخدام طبقات إضافية من الحماية الأمنية المتاحة على نطاق واسع، وهو ما يجعل الوصول المدعوم من قبل TOLA غير فعال.

[79] الأكاديمية الوطنية للعلوم (2018)، "فك تشفير نقاش التشفير: إطار لصناع القرار"، متاح على: https://www.nap.edu/read/25010 ، بيلوفين إس، إم بلايز، دي يونيه، إس لاندواو وار ريفست (2018)، تحليل بروتوكول CLEAR في إطار الأكاديميات الوطنية، CUCS-003-10، 10 أيار/ مايو 2018 ، متاح على: https://mice.cs.columbia.edu/getTechreport.php?techreportID=1637، بيلوفين إس، إم بليز، إس كلارك، وإس لاندو (2014)، "القرصنة القانونية: استخدام الثغرات الأمنية الموجودة للتنصت على الإنترنت،" Northwestern Journal of Technology and Intellectual Property، مجلد 12، نسخة رقم 1، أبيلسون، أتش، إل اندرسون، إس بيلوفين، جيه بينولاه، إم بلايز، دابليو ديفي، جيه جيلمور، إم جرين، إس لاندوا، بي نيومان، آر ريفست (2015)، Keys under doormats: فرض انعدام الأمن من خلال طلب وصول الحكومة إلى جميع البيانات والاتصالات، Journal of Cybersecurity، 1 (1)، من صفحة 79:69، متاح على: https://academic.oup.com/cybersecurity/article-pdf/1/1/69/7002861/tyv009.pdf، والتقرير الفني MIT-CSAIL-TR-2015-026، (6 تموز/ يوليو، 2015) على: https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf;علي ام (2016) ، "فك التشفير المستتر الخاص بالحكومة يضر بعملي وعملك"، Harvard Business Review، 15 أيلول/ سبتمبر، 2016، متاح على: https://hbr.org/2016/09/backdoor-government-decryption-hurts-my-business-and-yours.

[80] صفحات TOLA XX، الهامش 2 السابق.

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

المشرعون يتخذون خطوات لمنع إنشاء نقاط ضعف منهجية. ومع ذلك، فإن عدم مطالبة مقدم الخدمة ببناء أو تنفيذ ضعف منهجي أو ثغرة منهجية لا يمنعه من فعل ذلك.

وبدلاً من القول بأن مقدم الاتصالات المحدد لن يُمنع من تصحيح ضعف أو ثغرة، يجب أن تنص اللغة على أن مقدم الاتصالات المحدد ملزم[81] باتباع أفضل الممارسات في هذا المجال، فيما يتعلق بالتصحيح الفوري للثغرات الأمنية ونقاط الضعف المعروفة.

ويكمن الخطر في أن قانون TOLA قد يخلق حوافز للشركات للاحتفاظ (على سبيل المثال: عدم الكشف) بالثغرات المعروفة. وفعل ذلك يضع الجمهور الأوسع في خطر أكبر، ويوجد اهتمام عام مفرط في الإبلاغ عن الثغرات وإصلاحها وتصحيحها بأسرع ما يمكن، لا سيما للحد من مخاطر وتأثير هجمات الثغرة الأمنية "هجوم ساعة الصفر" "zero day".

وعلى نحو مماثل، غالباً ما يعرض مؤيدو بعض الأساليب مثل الفحص من جانب العميل ومقترح المملكة المتحدة "Ghost Proposal" تلك الأساليب على أنها تستخدم القدرات الحالية، بدلاً من إحداث ثغرات أمنية أو ثغرات جديدة.[82] وفي الواقع، إن هذه التقنيات تحدث بالفعل ثغرات جديدة. فعلى سبيل المثال، يوفر مقترح المملكة المتحدة "Ghost Proposal" آلية للتطويق الفعال لعملية التشفير من خلال السماح لطرف ثالث بالانضمام إلى جلسة دون علم المشاركين المقصودين. وتصبح هذه الآلية عملية قابلة للتطبيق على نطاق واسع نظراً لإمكانية تكرارها من مقدم خدمة الاتصالات المحددة عبر قاعدة المستخدمين بأكملها.

استهداف غير واضح

في حين أن تقييد الطلب/ الإشعار على هدف معين من أجل الحد من التعرض هو النهج الصحيح، لا تزال إمكانية تحقيق الاستهداف دون كشف المستخدمين غير المستهدفين غير واضحة. ويبدو أن مسؤولية اتخاذ هذا القرار تقع على عاتق مقدم خدمة الاتصالات المحددة، وليس مضموناً أن يفعل ذلك بشكل صحيح. ومن غير الواضح أيضاً كيف سينفذ مقدم خدمة الاتصالات المحددة الإزالة المستهدفة أو تقويض التشفير (هل التحديثات مطلوبة، وكيف

[81] هناك دائماً فرصة لحدوث ثغرة، ولكن تعتمد المسؤولية فيما يتعلق بنقاط الضعف غير المعروفة لمقدم الخدمة على كيفية تعيين معيار الواجب الائتماني أو مسؤولية العناية الواجبة، ولكن من المفترض عادةً أنها لن تشكل مسؤولية غير محدودة.

[82] انظر: كلاس، جيه، (2019)، "حيلة المستخدم الخفي لفك التشفير لن تعمل"، ACLU Blog Poast، 23 تموز/ يوليو 2019، متاح على: https://www.aclu.org/blog/privacy-technology/ghost-user-ploy-break-encryption-wont-work. للحصول على معلومات أساسية عن اقتراح Ghost الذي قُدِّم لأول مرة في المملكة المتحدة، راجع ليفي، أي و سي روبينسون (2018)، "مبادئ مناقشة الوصول الاستثنائي الأكثر استنارة،" مدونة LawFare، 29 تشرين الثاني/ نوفمبر 2018 ، متاح على: https: //www.lawfareblog.com/principles-more-informed-exceptional-access-debate.

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

تُستهدَفه ولا تُسرَّب). ويثير ذلك تساؤلاً وهو: أين تُطبَّق طريقة الوصول الاستثنائية في النظام؟ وكيف تُقدَّم؟

تطوير الأساليب والاحتفاظ بها

بينما يحاول قانون TOLA حماية التشفير القوي بذِكر إنه يجب عدم مطالبة أو إلزام مقدمي الخدمة بإحداث ثغرات أمنية أو نقاط ضعف نظامية، فهو لا يمنعهم من فعل ذلك. وقد يثير البعض نقطة أن الشركة ليست مستعدة أو تميل إلى تنفيذ مثل هذه الثغرات النظامية، فإن حظرها من شأنه أن يسمح بثقة أعلى للعملاء في التشفير. وبالنظر إلى أن قانون TOLA يسمح لبعض هيئات الاستخبارات وإنفاذ القانون بطلب أو بوجوب إحداث ثغرات أمنية أو نقاط ضعف انتقائية، فكيف يُتحكَّم في مثل هذه الثغرة الأمنية؟ وما طريقة منع حدوث مثل هذه الثغرة الأمنية في المستقبل؟

إعادة الاستخدام

في حين أن تقييد الالتزام بإحداث ثغرات أمنية أو نقاط ضعف مستهدفة فقط قد يبدو أنه التوجه الصحيح من حيث المبدأ، فإن مجرد إنشاء آلية وصول استثنائية، بغضّ النظر عن مدى استهدافها، يفتح الطريق على نطاق أوسع لسوء استخدام النظام وللأطراف السيئة. ويمكن أن يؤدي تدخل معين إلى استخدامات غير مقصودة، وهي ليست جزءاً من طلب أو إشعار قانون TOLA، وهو ما يؤدي إلى فتح باب خلفي قابل للتطبيق على نطاق واسع.

بالإضافة إلى ذلك، فإن التدخل يعني أن طريق الدخول أصبح الآن معروفاً. وقد تتسبب معرفة الطريقة (أو ما هو أسوأ مثل: أدوات البرامج أو التنفيذ) في إصدار غير مقصود أو عن علم لآخرين غير مصرح لهم بذلك. ويؤدي عدم التأكد من هوية من طُلب منه تدخل الوصول الاستثنائي إلى تقليل الثقة عبر سلسلة القيمة.

التصعيد

إن أحد التحديات الأساسية لإلزام مقدمي الخدمة بإنشاء وصول مستهدف هو عدم وجود ضمان بعدم تطبيقهم له على نطاق أوسع ليصبح نظامياً، جزئياً أو كلياً. وغالباً ما تكون الخطوة

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

الأولى عند تطوير هجوم منهجي على نظام ما هي تحديد هجوم محدود، ثم تحديد كيفية تطبيقه على نطاق أوسع. ومن ثَم، فإن مطالبة مقدمي الخدمات بمحاولة إنشاء تدخلات هادفة هي الخطوة الأولى نحو خلق ثغرات منهجية. وعلاوة على ذلك، من المرجح أن يكون التدخل المستهدف، إذا لزم تكرار الأمر، أسهل في الاستخدام وأكثر آلية، ومن ثَم يقارب التدخل النظامي.

ومن المرجح أن يصبح التدخل المستهدف نظامياً فور اكتشاف وجود الضعف أو إنشائه أو مشاركته. وحتى إمكانية وجود الضعف قد تشجع أيضاً الفاعلين السيئين على البحث عنه. ويمكن أن تتطور الثغرة المستهدفة أو الضعف إلى ثغرة نظامية ببساطة عن طريق تكرار أو تضخيم الثغرة الأمنية عبر قاعدة مستخدمين (من خلال التحديثات أو الفيروسات أو الطرق الأخرى.)

التسريب والمشاركة

قد تُسرَّب التدخلات المستهدفة، وتصبح متاحة لمجتمع أوسع، ومن ذلك أن تصبح في متناول الفاعلين السيئين الذين قد يستخدمونها لتهديد الجمهور.[83] بالإضافة إلى ذلك، قد لا تُصحَّح الثغرات "المكتشفة"، بل يُحتفظ بها. وفورَ معرفة التدخلات، من الضروري أن يعمل مقدم الخدمة من خلال عمليات الإخطار والتصحيح المعروفة في المجتمعات الأمنية، ومع ذلك لا يتطلب قانون TOLA من مقدمي الخدمة فعل ذلك. ومن المنطقي أن نقول إنه بعد ظهور ثغرة أو ضعف، فستكون مسألة وقت فقط حتى تُكتشَف، أو تُشارَك، أو تُسرَّب، أو تُسرَق، أو تُجرَى هندسة عكسية لها.

عملية والتزامات غير مؤكدة

بموجب قانون TOLA، قد يُطلب من مقدمي خدمة الاتصالات المحددة الاحتفاظ بالثغرات الأمنية غير المقصودة في أنظمتهم للاستخدام المستقبلي، وهو ما قد يصنع حالةً من عدم اليقين لهؤلاء المقدمين بشأن متى ينبغي عليهم المشاركة في الكشف عن الثغرات الأمنية، وكيف. ويُرسل الكشف الواضح عن الثغرات الأمنية إشارة قوية إلى أن التشفير القوي سيُحافَظ عليه، الأمر الذي يزيد ثقة المستخدمين -الكيانات التجارية والمستخدمين الفرديين- على حدٍّ سواء. ويوجد أيضاً حالة من عدم اليقين بشأن ما قد يعني طلب أو إشعار قانون TOLA من المشركة؛ وبشكل أكثر تحديداً، لأي مدى يلتزم مقدمو الخدمة بالمساعدة في عملية اعتراض الاتصالات أو فك تشفيرها. ويعني عدم اليقين بشأن قانون TOLA عدم تأكد المشركات من الأساليب المطلوبة للوفاء بالطلب أو الإنذار الصادر بمقتضى هذا القانون، وهذا يعني مواجهة مسؤولي الأمن داخل

[83] أشارت جمعية الإنترنت في ورقة CALEA II الخاصة بها إلى كيفية حدوث مثل هذه التسريبات. https://cdt.org/wp-content/uploads/pdfs/CALEAII-techreport.pdf. وراجع على EternalBlue https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/ .

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

المشركة صعوبات عند التعامل مع قرارات بشأن تبنّي التكنولوجيا، وتوظيف العاملين في الأمن، وحتى نتيجة الشراكة معشركات أخرى أو مشاركة البيانات. ووجود نهج مدروس ومصمم يتميز بالشفافية له نفعٌ سيلقي بظلاله على هذا المجال.

ومن الصعب (أو على الأقل يجب أن يكون صعباً)[84] كسر التشفير القوي بناءً على التصميم، وليس من الواضح كيف سيتعامل كل مقدم خدمات الاتصالات المحددة مع طلب الوصول. وذلك التأكيد على عدم الوضوح يستند إلى المناقشات التي أجرتها هيئات الاستخبارات وإنفاذ القانون مع مجموعة متنوعة من مقدمي خدمات الاتصالات المحددة الرئيسيين. وبناءً على المقابلات التي أجريناها، فإن الشركات ليست متأكدة من التزاماتها، ومن غير الواضح لها الأساليب المطلوبة للوفاء بالطلب أو الإنذار الصادر بمقتضى قانون TOLA.

وعلاوة على ذلك، يستلزم الأمر من فاعلين آخرين في النظام الإيكولوجي (على سبيل المثال: مقدمو خدمات الاتصالات المحددة المختلفون) اتباع طرق مختلفة لإزالة التشفير أو تطويقه. ووجدنا في المقابلات التي أجريناها أن فئات مختلفة من مقدمي الخدمة لديهم وجهات نظر مختلفة بشأن مدى صعوبة أو ضرر إزالة التشفير أو تطويقه. ووجدنا في محادثتنا مع شركات الاتصالات التقليدية (مثل مقدمي خدمة الهاتف السابقين) أن وجهة نظرهم أقل انتقاداً فيما يخص تنفيذ طلبات قانون TOLA، خلافاً لوجهة نظر مقدمي خدمة الويب والتطبيق ومقدمي خدمة الإنترنت الآخرين.

وإيجازاً، يمكن لقانون TOLA تقويض وإضعاف ثقة الجمهور في العديد من الخدمات المشفرة التي نستخدمها جميعاً الآن يومياً. فمجرد تصوُّر ضعف التشفير أو التهديد الناتج عن قدرة الهيئات الحكومية على جمع المعلومات يقوض الثقة عبر أنظمة بأكملها.

وقد يتجنب المستهلكون، سواء أكانوا كيانات تجارية أم أفراداً، إدارةَ الأعمال في بيئة ثقة ضعيفة. كذلك يجب على الشركات اتخاذ قرارات عما إذا كانت تريد التعامل مع الصعوبات القانونية والتشغيلية واللوجستية، التي قد تواجهها أثناء ممارسة الأعمال التجارية في أستراليا (أثار هذه النقطةَ العديدُ من الشركات الكبرى خلال مقابلاتنا). وأعرب العديد من شركات التكنولوجيا في أستراليا عن مخاوفها بشأن قانون TOLA.

فعلى سبيل المثال، في عام 2020 م، صرح باتريك تشانغ، رئيس السياسات والشؤون الحكومية في أتلاسيان، أن "استمرار نجاح ونمو الابتكار التكنولوجي والتصنيع في أستراليا سيعتمد اعتماداً كبيراً على الأمن الفعلي والمتصوَّر للتقنيات التي تدعم الاقتصاد الرقمي ونظامه البيئي."[85] وهذه

[84] يتيح استخدام أساليب مثل الـ Ghosting إضافة طرف ثالث إلى جلسة آمنة بصمت، ويمكن للمرء أن يجادل بأن هذا ليس بالأمر الصعب، ولذلك نضيف هذا التوصيف.

[85] "قوانين التشفير تلحق الضرر المحتمل: أتلاسيان"، InnovationAus، 24 حزيران/ يونيو 2020، متاح على: https://www.innovationaus.com/encryption-laws-damage-potential-atlassian/

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

الادعاءات بالضرر ليست مجرد تخمينات، فقد صرحت شركة فولت سيستمز، وهي مقدم خدمات سحابية أسترالية، أنها "متأثرة مادياً وسلباً" من قانون TOLA.[86]

وفقاً لذلك، قد يكون من الأسهل ببساطة البحث عن خدمات في بلد آخر لتجنُّب عدد لا يُحصَى من التحديات وعدم اليقين الاقتصادي، إذ صرح مجلس هندسة الإنترنت بقوله: "قد يتسبب هذا الخطر في انتقال بعض مقدمي البنية التحتية، أو تقليل الخدمة، أو حتى حظر الخدمة للمستخدمين الأستراليين. ويُعد تفكك الإنترنت بهذا الشكل أحد اهتماماتنا الأساسية حالياً، لأنه يقلل قيمة الإنترنت العالمي المتصل بشكل كبير."[87]

الإطار الاقتصادي

يهدف هذا التقرير أساساً إلى تقييم جميع الأدلة المتاحة للآثار الاقتصادية لقانون TOLA. وقد كان من المتوقع أن يُبذَل مثل هذا الجهد قبل إقرار هذا القانون، لكن كما أوضحنا لم يحدث ذلك. ويظل الأمر الأكثر إثارةً للدهشة لنا هو ملاحظة أنه لا توجد دراسات لتقييم الآثار الاقتصادية للتشريعات الشبيهة بهذا القانون التي توجد في أي مكان، من خلال مراجعتنا للأدبيات المنشورة، أو في سياق بحثنا الأساسي الذي يتضمن مقابلات متعمقة مع مقدمي خدمات الاتصالات المحددة المتنوعين والمتعددي الجنسيات (سوف يُناقَش ذلك مناقشةً مفصلةً في الفصل السادس). وعلى الرغم من مساهمة المؤيدين والمنتقدين للوائح الشبيهة بقانون TOLA في مجموعة كبيرة من المؤلفات الأكاديمية، وتقديمهم لتعليقات في اجتماعات متعلقة بهذا القانون (كما لوحظ بالفعل) وفي اجتماعات مماثلة متعلقة بتشريعات أخرى، مثل قانون سلطات التحقيق في المملكة المتحدة (2016 م)[88]، هناك ندرة ملحوظة في محاولات تحديد التكاليف الاقتصادية أو المنافع التي يمكن توقعها في كل هذه المواد.

وفي عالم مثالي، يتطلع الفرد إلى دراسة تحدد جميع التكاليف والفوائد المحتملة لقانون TOLA، وترجمها إلى مصطلحات نقدية، ثم تجمعها للوصول إلى تقدير صافي الفوائد الاقتصادية المتوقعة. فإذا وُجد مثل هذا التقدير، فقد يساعد في تقييم احتمال تجاوز صافي منافع قانون

[86] "النطاق الواسع لقانون الأمن القومي الأسترالي الجديد يتضح"، ZDNet، 6 حزيران/ يونيو 2019، متاح على: https://www.zdnet.com/article/huge-scope-of-australias-new-national-security-laws-reveals-itself/)
و"قوانين التشفير تخلق هجرة جماعية للبيانات من أستراليا"، ZDNet، 5 تموز/ يوليو 2019، متاح على: https://www.zdnet.com/article/encryption-laws-are-creating-an-exodus-of-data-from-australia-vault/

[87] تعليقات مجلس هندسة الإنترنت (IAB) على قانون المساعدة والوصول الأسترالي، 9 أيلول/ سبتمبر 2018، متاح على: https://www.iab.org/wp-content/IAB-uploads/2018/09/IAB-Comments-on-Australian-Assistance-and-Access-Bill-2018.pdf

[88] انظر الهامش 27 السابق.

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

TOLA لصافي تكاليفه. وبطبيعة الحال، لن يكون التقدير النقدي للتأثير الاقتصادي الصافي الكلي وحده هو كل ما سيضعه صانعو السياسات في الاعتبار من أجل تقييم تأثير هذا القانون. ومن الصعب بطبيعة الحال ترجمة بعض الآثار إلى مصطلحات نقدية (مثل الأمن القومي، ومنع الجريمة، أو ملاحقة مرتكبيها)، كما يمثل وضع توزيع الآثار الاقتصادية اعتباراً مهماً (سواء فيما يتعلق بتخصيص التكاليف والمنافع، أو طرق تحقيقها بمرور الوقت).

نحن لا نعيش في عالم مثالي، ولا يمكن لهذا التقرير أن يقدم تقديراً نقدياً كمياً لتأثير قانون TOLA. وبدلاً من ذلك، نفحص الآليات المختلفة التي من خلالها قد يؤدي هذا القانون إلى تأثيرات اقتصادية. ويحدد هذا التحليل بسهولة العديد من الآليات التي يمكن أن من خلالها أن يتسبب هذا القانون في تكاليف مباشرة وغير مباشرة لشركات تطوير البرامج، والمؤسسات الأخرى، والمستهلكين في المجالات الاقتصادية. ولا تقتصر التكاليف ذات الصلة على التكاليف المباشرة التي تتحملها الشركات الناشئة التي قد تتلقى إنذارات هذا القانون، أو حتى التكاليف غير المباشرة للشركات في قطاع تكنولوجيا المعلومات والاتصالات، ولكنها تشمل التكاليف غير المباشرة للشركات والمستهلكين الآخرين على نطاق أوسع. وعلاوة على ذلك، من المتوقع أن تتراكم التكاليف بمرور الوقت، إذ تُستخدَم السلطة الحكومية الجديدة التي أنشأها القانون.

ويقودنا تحليلنا إلى استنتاج أن لدى قانون TOLA القدرة على إحداث ضرر اقتصادي كبير على الاقتصاد الأسترالي، وتداعيات سلبية من شأنها أن تضخم هذا الضرر على المستوى العالمي.

ونوضح سبب صعوبة تحديد عناصر التكلفة والمنفعة، حتى مع توفر بيانات أفضل، مع ملاحظة الانعدام شبه الكامل للبيانات ذات الصلة. وعلاوة على ذلك، نوضح لماذا يُعد القياس الكمي - جزئياً على الأقل- للتكاليف التي من المرجح أن يتسبب فيها قانون TOLA تحدياً أكثر سلاسة من تحديد منافعه.

ويقودنا تحليلنا كذلك إلى استنتاج أن تهديد قانون TOLA للثقة عبر الإنترنت هو أكثر مصدر محتمل للتكلفة المتعلقة بالقانون. وكما نوضح، فحتى التأثير الضئيل على الثقة يمكن أن يؤدي إلى أضرار اقتصادية موزعة على نطاق واسع تؤدي إلى آثار اقتصادية سلبية بما يوازي مليارات الدولارات. وبالمقارنة مع تلك التكاليف غير المباشرة التي سوف تتراكم بمرور الوقت، فإن التكاليف المباشرة التي تتحمَّلها الشركات، التي قد تتضرر أعمالها الفردية من تنفيذ هذا القانون، من المرجح أن تكون أصغر كثيراً في الإجمال، ولكن لا تزال تكلفتها كبيرة للشركات المتضررة ومن الناحية النقدية الإجمالية. فعلى سبيل المثال، شرحت إحدى الشركات المتعددة الجنسيات التي قابلناها كيف أدى قانون TOLA بالفعل إلى خسارة الشركة ما يزيد على مليار دولار أسترالي في الإيرادات، وأفاد العديد من المشاركين في الاستطلاع أنهم تكبدوا بالفعل خسائر في الإيرادات

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

بنسبة مئوية ثنائية الرقم. ولسوء الحظ، لا توفر تلك المعلومات للبيانات الفردية أساساً موثوقاً به لاستخلاص تقدير للتكاليف الإجمالية على مستوى الاقتصاد.

5.1 إطار فهم التأثيرات الاقتصادية لقانون TOLA

إن الإطار المناسب لإجراء مثل هذا التقييم هو مقارنة ما حدث (أو من المحتمل أن يحدث) في العالم إذا طُبِّق قانون TOLA، مقارنةً بعالم افتراضي "عالم لو لم يكن هناك" "but-for world"، حيث لا يُطبَّق فيه.[89] ويثير ذلك العديد من التحديات النظرية والتجريبية المعقدة لأسباب متعددة ، منها الحاجة إلى توسيع نطاق الجهد من خلال معالجة الأسئلة التالية:

1- ما الآثار الاقتصادية التي يجب وضعها في الاعتبار؟
2- هل ينبغي التركيز على التأثير على أستراليا أو العالم؟
3- كيف نوازن بين التركيز على تكاليف قانون TOLA في مقابل منافعه؟
4- هل تحليل الآثار طويل المدى أم قصير المدى؟
5- كيف يتسم عالم "لو لم يكن هناك" قانون TOLA؟
6- كيف تُجمَع بيانات عن تأثير قانون TOLA؟

وسوف تُتناول كل من هذه التحديات في الأقسام الفرعية التالية.

5.1.1 ما الآثار الاقتصادية التي يجب وضعها في الاعتبار؟

يعتمد تقييم الآثار الاقتصادية للتشريعات على القدرة على تقييم كيفية تغيير الشركات والمستهلكين المتأثرين بقانون TOLA لسلوكهم، سواء كان تغييراً مباشراً أم غير مباشر، نتيجةً له، وهو أمر يمثل تحدياً، لأن السلوك يعتمد على التوقعات. ومن الناحية المثالية، نود تحديد التأثيرات القابلة للقياس على إجمالي الفائض، وهو مجموع فائض المنتج والمستهلك من الناحية النقدية (بالدولار الأسترالي). ولا يمكن ملاحظة الآثار النقدية لقانون TOLA على فائض المنتج والمستهلك مباشرةً، ويجب تقديرها من مجموعات البيانات النقدية وغيرها من البيانات المتعلقة بالنتائج. ويمكن تفسير أنواع التأثيرات السلوكية والمرتبطة بالنتائج على نطاق واسع لتشمل التأثير المحتمل للقانون على إيرادات الأعمال والاستثمار والخطط الإستراتيجية. فعلى سبيل المثال، يمكن تقدير فائض المنتج عن طريق البيانات المتنوعة المتعلقة بالنتائج، مثل البيانات المتعلقة بإيرادات الأعمال وتكاليف التشغيل والاستثمارات، التي يمكن تقديرها من

[89] ملاحظة: من المحتمل أن يكون اعتماد قانون TOLA قد أثر على السلوك والنتائج حتى قبل اعتماده في كانون الأول/ ديسمبر 2018. وعلاوة على ذلك، فاستمرار عدم اليقين بالإصلاحات التنظيمية أو التشريعية المستقبلية والخلافات بشأن التفسير القانوني للقانون وماهيته واستخدامه المستقبلي يساهم في تشويه التحدي المتمثل في تحديد واضح مقارن لمرحلة ما قبل القانون وما بعده، ومع وجوده أو من دونه، مجموعة أدوات لتقييم الآثار الاقتصادية. وكما سنناقش لاحقاً، فإن أحد الأسباب التي قد تجعلنا نفشل في ملاحظة التأثيرات القابلة للقياس على السلوك بسبب القانون هو أنها لم تُطبَّق بالكامل بعدُ بسبب المخاوف من التحديات المستمرة التي تواجه قانون TOLA.

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

بيانات مبيعات الوحدات وسعر الوحدة وبيانات التكلفة. وإرجاع هذه التأثيرات إلى عامل فردي مثل تأثير قانون TOLA يحتاج إلى بيانات إضافية لإثباته.

ويُعد تقدير فائض المستهلك أمراً أكثر صعوبة، ولكنه يشمل تقدير المدى الذي يتجاوز فيه طلبُ المستهلك شبه الهامشي الأسعارَ المدفوعة (أي مدى تجاوز الاستعداد لدفع السعر)[90]. وعلاوة على ذلك، يعتمد فائض المستهلك أيضاً على اختيار المنتج (الانتقاء) والجودة[91].

وتشمل الاستجاباتُ السلوكية التغيراتِ في ممارسات التوظيف في الشركات، وسلوك الاستثمار، ونشاط الابتكار، وجميعها مرتبطة بعضها ببعض. فعلى سبيل المثال، تعتمد الاستثمارات في القدرات التجارية على التوقعات المتعلقة بالآفاق المستقبلية للشركة، التي تعتمد على الميزة التنافسية للشركة، وعلى استثمارات الشركة في البحث والتطوير، والاستثمارات الإستراتيجية المتنوعة (على سبيل المثال، في صورة هويتها التجارية، والأمن السيبراني، والملكية الفكرية، ... إلخ). وكما سنوضح لاحقاً، من المتوقع أن تكون إحدى الاستجابات السلوكية المحتملة تقليلَ الشركات استثماراتها في البحث والتطوير، وتقديم المنتجات الجديدة في أستراليا، التي من المتوقع أن تتأثر سلباً بقانون TOLA، سواء كان التأثر مباشراً أم غير مباشر. وبقدر ما يحدث، فإن تقدير التأثير الاقتصادي سيعتمد على حساب صافي الفوائد المستقبلية المتوقعة من الاستثمارات التي أعيقت، أو تحسين اختيار المنتج والتسعير الذي كان سيتحقق لولا ذلك. وهذا بطبيعته أكثر صعوبة في القياس، بدلاً من قياس ما حدث بالفعل.

ومن ثَم، فإن التأثيرات السلوكية المتعلقة بالنتائج تعتمد على اتجاهات وتوقعات العمل التجاري. ومن المحتمل أن تصل التأثيرات إلى مستوى الاقتصاد كله، وحتى على المستوى العالمي، ومن ثَم، تتجاوز تلك التأثيراتِ المنسوبة مباشرة إلى الشركات التي تتلقى طلبات قانون TOLA أو إشعاراته. وفي الواقع، من المتوقع أن تكون هذه التأثيرات غير المباشرة أكبر كثيراً في المجمل من التأثيرات المباشرة. ومع ذلك، وعلى الرغم من صعوبة تقييم الآثار الاقتصادية المباشرة، فإن تقدير الآثار غير المباشرة يُعد أكثر صعوبة.

5.1.2 هل ينبغي التركيز على التأثير على أستراليا أم على العالَم؟

[90] لا يُلاحَظ الاستعداد للدفع المباشر، ولكن يمكن الاستدلال عليه من استبيانات المستهلكين، ومن خلال سلوك التفضيل المكشوف في السوق، (أي وظيفة الطلب التقديرية في الصناعة).

[91] يتخذ المستهلكون عادةً خياراتهم للشراء من بين عدة شركات، وتقدم كل منها مستويات متعددة من المنتجات (على سبيل المثال، بقسط، أو بتخفيض)، ويختار المستهلكون المنتج الذي يقدم أفضل مقايضة للجودة في مقابل السعر. ويفضل المستهلكون دائماً الأسعار الأقل للحصول على الجودة نفسها للسلعة. ومع ذلك، ونظراً لاختلاف طلب المستهلكين للجودة ومميزات المنتج الأخرى، فإن وجود خيارات متعددة يزيد احتمالية أن يجد المستهلكون سلعاً تتناسب بشكل وثيق مع أذواقهم الخاصة. بالإضافة إلى ذلك، كلما زاد عدد الشركات التي يجري الاختيار من بينها، زادت المنافسة، التي قد تؤدي (أو قد لا تؤدي) إلى اختيار أوسع لمستويات الجودة اعتماداً على طبيعة المنتج والديناميكيات التنافسية، ولكن عموماً ستؤدي إلى انخفاض الأسعار. ومع ذلك، حتى مع وجود شركة واحدة فإن مجموعة المنتجات المعروضة مصممة لزيادة فائض المنتج إلى الحد الأقصى، وهو ما يؤدي إلى مواجهة الشركات التحدي المتمثل في تحديد تسعير فئة المنتج لتمييز السعر على النحو الأمثل: أي تحديد السعر بحيث يتجه بعض المستهلكين إلى القرار العقلاني لمقايضة الجودة المضافة بالسعر الأعلى. وخلافاً لذلك، يختار المستهلكون السلع الأقل سعراً والأقل جودة، وتكون فئة الجودة العليا غير عملية في السوق.

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

بينما ينصبُّ تركيزنا على الاقتصاد الأسترالي، فإننا مهتمون أيضاً بتحديد الآثار غير المباشرة المحتملة على نطاق أوسع. وتُعد سوق تكنولوجيا المعلومات والاتصالات والمنتجات والخدمات سوقاً عالميةً، وقد تؤثر التشريعات في أستراليا على احتمالية وجود تشريعات مماثلة في دول أخرى تعمل على تقوية التأثير الاقتصادي لقانون TOLA أو إضعافه داخل أستراليا بمرور الوقت.

ويعتبر البعض أن القلق بشأن قدرة هيئات الاستخبارات وإنفاذ القانون على الوصول إلى المعلومات، التي تتخذ شكلاً رقمياً بشكل متزايد، يمثل تهديداً خطيراً لفعالية خدمات تطبيق القانون والأمن على الصعيد الدولي، سواء كانت هذه المعلومات "متحركة" (مكالمات هاتفية، أو رسائل، أو عمليات نقل الملفات، أو تبادل الهوية أو بيانات الاعتماد)، أم "ثابتة" (مخزنة في صورة ملفات رقمية، أو برامج على الأجهزة أو خوادم الملفات في السحابة) التي تحظى بالحماية أيضاً بشكل متزايد بأدوات الأمن السيبراني، مثل تقنيات التشفير من الطرف إلى الطرف، التي يعتبرها البعض تهديداً حقيقياً لكفاءة فرض القانون وخدمات الأمن على المستوى الدولي.

واقترح واضعو السياسات في بلدان متعددة مبادرات تشريعية وناقشوها، وهي التي من شأنها أن تمنح هيئات الاستخبارات وإنفاذ القانون صلاحيات إضافية للحصول على وصول استثنائي إلى البيانات الرقمية.[92] وكما أوضحنا سابقاً، وعلى الرغم من أن قانون TOLA يتبع اعتماد المملكة المتحدة السابق للسلطات الحكومية الموسعة للحصول على مساعدة الصناعة في تطويق التشفير، فمن المرجح أن تؤثر الدروس المستفادة في أستراليا على الدول الأخرى هل ستحذو حذو أستراليا أم لا. وهذا أمر مثير للقلق، لأن الافتقار إلى الأدلة التجريبية للأضرار الاقتصادية الكبيرة قد يُفهَم خطأً على أنه دليل على عدم وجود مثل هذه الأضرار، وهو ما قد يشجع البلدان الأخرى على تبني تشريعات مماثلة لقانون TOLA، الأمر الذي يؤدي إلى تضخم تكاليف هذا القانون.

5.1.3 كيف نوازن بين التركيز على تكاليف قانون TOLA في مقابل منافعه؟

يتطلب تقييم الأثر النقدي الإجمالي لقانون TOLA مراعاة كل من التكاليف، التي من المحتمل أن يحدثها القانون، بالإضافة إلى المنافع الذي قد يقدمها. في حين أنه من السهل نسبياً تحديد آليات متعددة يمكن من خلالها أن يؤثر هذا القانون تأثيراً مباشراً على سلوك الشركات، ومن ثَم

[92] على سبيل المثال، كان لدى المملكة المتحدة تشريعات سارية تُمكّن هيئات إنفاذ القانون وهيئات استخبارات الأمن القومي من الوصول القانوني إلى المعلومات المشفرة منذ أوائل العقد الأول من القرن الحادي والعشرين، التي توسعت عبر قانون سلطات التحقيق في المملكة المتحدة (2016) (انظر الهامش 27 السابق). وفي الآونة الأخيرة، في الولايات المتحدة ، قدم السناتور الجمهوري ليندسي جراهام إلى مجلس الشيوخ قانون 4051 - قانون الوصول القانوني إلى البيانات المشفرة (LAEDA) في حزيران/ يونيو 2020 (انظر: https://www.congress.gov/bill/116th-congress/senate-bill / 4051). وفي تشرين الأول/ أكتوبر 2020، أصدر تحالف "العيون الخمس" الاستخباراتي بين أستراليا وكندا ونيوزيلندا والمملكة المتحدة والولايات المتحدة ("العيون الخمسة" الأصلية) والهند واليابان بياناً مشتركاً يدعو إلى إمكانات أقوى لتمكين الوصول القانوني إلى البيانات المشفرة (انظر:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/925601/20.10.11_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, United Kingdom +44 7554 065 718

المستهلكين، بطرق تؤدي إلى زيادة التكاليف، لكن الأكثر صعوبة تتبُّع الآلية التي سيؤدي بها القانون إلى زيادة المنافع.

وفي الأقسام اللاحقة، نحدد الآليات المختلفة التي قد يؤدي قانون TOLA من خلالها إلى زيادة التكاليف. وفي الجزء المتبقي من هذا القسم، نشرح سبب كون تقدير المنافع مسألة أكثر صعوبة.

ومن ناحية التكلفة والمزايا، تتداخل القيود المفروضة على الإفصاح، التي تعد جزءاً من قانون TOLA، مع جمع البيانات التفصيلية عن كيفية تغيير استخدام هذا القانون للسلوك. بل إن فجوات البيانات أكثر شدة، ومع ذلك، يُعد تتبُّع آثار السببية أكثر صعوبة في جانب المنفعة منه في التكلفة. وكانت المنفعةُ الرئيسية المتصورة لإقرار قانون TOLA معالجةَ التحدي الملحوظ الذي يطرحه الاستخدام المتزايد للتشفير على متابعة هيئات الاستخبارات وإنفاذ القانون لمهام إنفاذ القانون والأمن القومي. ومن المفترض أن تحسن القدرات الموسعة التي تحقَّقت بهذا القانون فعاليةَ هيئات الاستخبارات وإنفاذ القانون وكفاءتها. وهذا الافتقار للشفافية يجعل من الصعب التأكد من كيفية تغيير هذا القانون، أو احتمال تغييره لسلوك هيئات الاستخبارات وإنفاذ القانون (ذات الصلة بـ"عالَم لو لم يكن هناك").

ومع ذلك، حتى قبل التعمق في حل أوجه القصور تلك في البيانات، من الممكن التفكير نوعياً في كيفية تأثير قانون TOLA على فعالية هيئات الاستخبارات وإنفاذ القانون. وهناك العديد من الأسباب المعقولة التي تشير إلى احتمال قلة المنافع التي ستعود على هيئات الاستخبارات وإنفاذ القانون. وتشمل هذه الحقائق أولاً أن التقنيات متاحة على نطاق واسع لأي شخص (مثل المجرمين) لإدخال طبقات إضافية من أمن البيانات، ومنها التشفير. وثانياً: في العديد من الدول تشريعات واسعة النطاق بالفعل تنص على الوصول القانوني إلى البيانات.

وتوحي النقطة الأولى بأن المستهدفين، ذوي الدوافع المناسبة الراغبين في تأمين بياناتهم، يستطيعون فعل ذلك حتى لو اعتُمِد قانون TOLA، وذلك من خلال استخدام تشفير قوي لكل من البيانات المتحركة (مثل الرسائل من الطرف إلى الطرف)، والثابتة (مثل المخزنة على جهاز)، والاستفادة من تقنيات أخرى (مثل أشكال مختلفة من المراوغة كالتوجيه البصلي) لجعل أي جهود لتقديم المساعدة يبذلها مقدمو خدمات الاتصالات المحدود غير فعالة. ويعرف المجرمون أنهم يلعبون دائماً لعبة القط والفأر مع تطبيق القانون. ومن ثَم، يكون لديهم حافز إضافي للاستفادة من التقنيات التي تستخدم طبقات إضافية من الأمان.

وحتى إذا رفُضت النقطة الأولى، فإن النقطة الثانية تسلط الضوء على اعتماد المنافع الإضافية لقانون TOLA على مدى إنشاء القانون لإمكانات جديدة توسِّع قدرات إنفاذ القانون للوصول إلى بيانات الأهداف المشروعة. ومع ذلك، نظراً لوجود عدم وضوح بشأن كيفية استخدام هذا القانون، فإن حجم هذه المنافع الإضافية غير مؤكد.

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

وعلى أي حال، فمن الضروري تحليل السياسات القائمة على الأدلة اللازمة لتقدير تكاليف ومنافع قانون TOLA بشكل أكثر دقة، إذا كان من المتوقع أن تكون تقديرات التكاليف والمنافع قريبة نسبياً من حيث الحجم. وإذا كان هناك دعم (أو دليل) على ضآلة التكاليف الإجمالية، ولكن الفوائد الإجمالية كبيرة (أو العكس)، فإن وجود تقديرات دقيقة للأثر الاقتصادي يصبح أمراً أقل أهمية[93].

ونظراً لعدم إجراء تحليل فعلي مفصل للأثر الاقتصادي (أو إتاحته للجمهور) حتى الآن، يمكن الاستنتاج بشكل معقول أن المنافع ستفوق التكاليف إذا استُنتج إما (1) أن التكاليف المحتملة ضئيلة في حين أن المنافع كبيرة؛ (2) أو أن التكاليف والمنافع المحتملة في أدنى مستوياتها، ولكن المنافع المحتملة أكبر.[94] ويشير ذلك إلى أن الحالة الأولى غير مرجحة، لكن الحالة الثانية لا تزال بحاجة إلى معالجة. ومن ثَم، فإن التركيز على حجم التكاليف المحتملة نقطةُ انطلاقٍ معقولة.

5.1.4 هل تحليل الآثار طويل المدى أم قصير المدى؟

من المهم معرفة هل يمكن قياس أي آثار قصيرة المدى ناتجة عن قانون TOLA منذ تطبيقه قبل عامين فقط. ومع ذلك، من المحتمل أن يظهر التأثير الكامل للقانون بمرور الوقت، ولدينا مزيد من الوقت مستقبلاً لمعرفة تكاليف هذا القانون. ومن ثَم، من المتوقع أن تظهر أهم الآثار الاقتصادية للقانون في المستقبل. فعلى سبيل المثال، ستكون التأثيرات المتوقعة أكبر، إذا ظل النطاق الكامل للقانون سارياً، وزاد عدد الطلبات والإنذارات الصادرة بموجب هذا القانون إلى ما بعد المستوى المنخفض الذي شوهد خلال العامين الأولين، وتوسع أكثر ليشمل استخدام إنذارات القدرة الفنية التي تتطلب من مقدمي الخدمة تعديل أنظمتهم أو تقنياتهم[95].

5.1.5 بِمَ يتسم عالم "لو لم يكن هناك" قانون TOLA؟

نستخدم حالة ما قبل قانون TOLA معياراً لنا لعالم "لو لم يكن هناك" قانون TOLA، مع إدراك أنه في عالم من دون هذا القانون قد تحدث أشياء أخرى قد تكون قابلة للتنبؤ (على سبيل المثال: إصدار مختلف من القانون، أو معدل اعتماد مختلف لتكنولوجيا التشفير). ويطرح تحديد سيناريو مناسب لـ"لو لم يكن هناك" مشكلة خاصة في حالة تقييم الأثر الاقتصادي للاستثمارات في أمن المعلومات (على سبيل المثال: "InfoSec"، كما في حال جدران الحماية، ومراقبة الأمان المحسَّنة، وتقنيات التشفير). وذلك لأن العائد على الاستثمار يعتمد على تكلفة الأضرار التي جرى تجنُّبها، وأي تقدير من هذا القبيل يعتمد على احتمالية وقوع تلك الأضرار في غياب

[93] هناك أربع حالات محتملة لـ(التكاليف/ المنافع) على النحو التالي: (كبيرة، كبيرة)، (كبيرة، صغيرة)، (صغيرة، كبيرة)، (صغيرة، صغيرة).

[94] نحن هنا نتجاهل الحالات التي يُعتقد أن تكاليفها كبيرة، لأن ذلك من شأنه ألّا يرجح دعم مرور قانون TOLA من خلال تقييم الأثر الاقتصادي.

[95] حتى الآن ، يُستخدَم قانون TOLA استخداماً قليلاً. فقد أصدر، حتى الآن، أقل من 50 إشعاراً من تقرير التقييم الثالث (ولم يُصدَر إشعار TAN أو TCN) (انظر الهامش 32 السابق).

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

استثمار- InfoSec ، وهو أمر احتمالي وغير مؤكد بطبيعته[96]. وسيكون شرح السيناريو المفصل لـ "لو لم يكن هناك" قانون TOLA جزءاً من تقييم توازن التأثيرات الاقتصادية لهذا القانون.

5.1.6 كيف تُجمع بيانات عن تأثير قانون TOLA؟

أصبحت تحديات تقدير التأثير الاقتصادي لقانون TOLA أكثر صعوبة بسبب متطلبات عدم الإفصاح التي ينص عليها القانون. وتمنع تلك المتطلبات متلقي إنذارات هذا القانون من الإبلاغ عن تفاصيل أو نتائج لأي إعلام تلقَّوْه. وهي أيضاً تمنع هيئات الاستخبارات وإنفاذ القانون من الكشف عن كيفية استخدامهم لهذا القانون، الأمر الذي يجعل من الصعب للغاية عزل التأثيرات الخاصة بالقانون عن العديد من التأثيرات الأخرى ذات الصلة بالاقتصاد أو نتائج الشركة (على سبيل المثال: الإيرادات، والاستثمار في الأمن السيبراني، وغير ذلك)، التي قد تؤثر على سلوك الشركة. فعلى سبيل المثال، إذا عدَّلت الشركات تسويق العلامة التجارية، أو الإعلان عن المنتجات، أو ممارسات دعم العملاء، فلا يتضح هل تفعل الشركات ذلك نتيجةً لتلقي إنذار قانون TOLA، تحسباً لكيفية تأثير هذا القانون على أسواقها، أم تفعل ذلك لبعض الأسباب غير ذات الصلة على الإطلاق.

يؤخر الإبلاغ عن إنذارات قانون TOLA وتُقدَّم على المستوى الإجمالي فقط. ويُبلَغ عن إجمالي عدد الإنذارات الصادرة، ولكن لا يُبلَغ عن أنواع الشركات التي تلقت تلك الإنذارات. ويُسمح لمقدمي خدمات الاتصالات المحدودة بإجراء إفصاحات إحصائية فيما يتعلق بالعدد الإجمالي للإنذارات المُستلمة خلال الأشهر الستة السابقة، وهل الإنذارات طوعية TARs أم إلزامية (TANs أو TCNs)، ولكن لا يمكن للشركات أن توضح أي من هيئات الاستخبارات وإنفاذ القانون قد أصدرت تلك الإنذارات، أو أن تفصح عن مزيد من التفاصيل.

وقد يسعى مقدمو خدمات الاتصالات المحددة للحصول على إذن للسماح لهم بالكشف عن معلومات عن المساعدة.[97] ومن غير المؤكد هل سيسعى مقدمو خدمات الاتصالات المحددة إلى الحصول على مثل هذا الإذن، وهل سيُمنَحون إياه. فعلى سبيل المثال، أي مقدم لخدمات الاتصالات المحددة، يُحَث على تقديم المساعدة -التي تهدد بالفعل، أو قد يُنظَر إليها على أنها تهدد، الأمن الرقمي لمنتجات أو خدمات مقدم خدمات الاتصالات المحددة- قد لا يرغب في الكشف عن أي إجراء من هذا القبيل، خوفاً من التأثير السلبي الذي قد يحدث لعلامته التجارية.

[96] في معظم الاستثمارات، يلاحظ المستخدم الفوائد المتدفقة من استخدام القدرات التي يتيحها الاستثمار (على سبيل المثال: يمكن للسيارة والسفر الذي يمكن تحقيقه بالسيارة أن يسمحا باستهلاك الاستثمار طوال الأميال المستخدمة). ومع استثمارات الأمن السيبراني، تُستمد الفائدة من الأضرار التي لم تتحقق (على سبيل المثال: انخفاض معدل الاحتيال أو التكاليف المُتكبدة في حالة خرق البيانات). ومثل التأمين ضد الحريق، فأتمنى، أنا المستهلك، أن أتمكن من استرداد جميع مدفوعات التأمين السابقة التي دفعتها في السنوات التي لم أشهد فيها حريقاً.

[97] انظر المادة 186 (2) من قانون TIA، الهامش 6 السابق (17)-317ZF(13) من TOLA، هامش 2 السابق. وراجع أيضاً "المساعدة والوصول: الخرافات الشائعة والمفاهيم الخاطئة"، الهامش 130 اللاحق.

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

وعلى الرغم من أن الشفافية الكاملة فيما يتعلق بكيفية استخدام هيئات الاستخبارات وإنفاذ القانون لقانون TOLA من المحتمل أن تضر بفعالية أنشطة هيئات الاستخبارات وإنفاذ القانون المدعومة من هذا القانون، وقد تشكل مخاطر إضافية على الأمن السيبراني،[98] فإن الحظر شبه الكامل لأي بيانات عن كيفية استخدام هذا القانون يجعل أي تقييم دقيق لتأثيراته الاقتصادية شبه مستحيل.[99]

وعلاوة على ذلك، فإن الثغرات الموجودة في البيانات المتعلقة بقانون TOLA، إلى جانب قواعد الملاذ الآمن، وأحكام السداد التي تسمح لمقدمي خدمات الاتصالات المحددة بتقديم التماس لاسترداد التكاليف المتعلقة بالمساعدة، والغموض فيما قد تطلبه أو تفرضه هيئات الاستخبارات وإنفاذ القانون، قد يكون له نتيجة سلبية قد تزيد الأضرارَ الاقتصادية المتوقعة من قانون TOLA. ومن المرجح أن تكون هذه الأضرار مرتبطة بتأثيرات غير مباشرة. والسبب في ذلك هو أن خصائص هذا القانون تقلل تحفيز مقدمي خدمات الاتصالات المحددة على مقاومة الامتثال لطلبات هيئات الاستخبارات وإنفاذ القانون، حتى لو مثلت هذه الطلبات تهديداً للأمن الرقمي.

ومن غير المرجح معاقبة المتعاونين من مقدمي خدمات الاتصالات المحددة بسبب تعاونهم مع عملائهم أو الكيانات الأخرى التي تتعامل معهم، نظراً لأنهم لا يستطيعون معرفة هل تلقى مقدم خدمات الاتصالات المحددة إنذاراً، وكيف استجاب له. وتضيف السرية المحيطة باستخدام قانون TOLA إلى حالة عدم اليقين في الأعمال، التي تواجه جميع الكيانات التي قد تتأثر بهذا القانون، وهو ما يؤدي إلى نشر تلك التأثيرات على نطاق أوسع، إذ يُترك الأطراف المهتمة لافتراض أن أياً من مقدمي خدمات الاتصالات المحددة، أو جميع مقدمي خدمات الاتصالات المحددة، قد يتعين عليهم الامتثال لطلبات أو متطلبات قانون TOLA.

وأخيراً، فإن الإشراف على قانون TOLA أكثر صعوبة في ظل افتقار الوصول نفسه إلى البيانات المتعلقة بهذا القانون، الذي يمنع من تقدير آثاره الاقتصادية.[100] وقد يؤدي التصور المتزايد بأن الرقابة على هذا القانون غير كافية للمخاطر المتوقعة نتيجة انتهاكات هيئات الاستخبارات وإنفاذ

[98] على سبيل المثال: ستشمل الشفافية الكاملة معلومات عن أي من مقدمي خدمات الاتصالات المحدودة حصل على إشعارات قانون TOLA، وما طلبات أو متطلبات تلك الإشعارات من مقدمي خدمات الاتصالات المحدودة، وما فعله مقدمو خدمات الاتصالات المحدودة في المقابل، وأي من هيئات الاستخبارات وإنفاذ القانون قد أصدرت القانون، وما الذي فعلته تلك الهيئات نتيجةً للمساعدة التي حصلت عليها من مقدمي خدمات الاتصالات المحدودة. ومن الواضح أن هذا المستوى من الإفصاح العام سينبّه إلى أهداف أخرى محل اهتمام هيئات الاستخبارات وإنفاذ القانون (مثل المجرمين المحتملين)، وتمكنهم من اتخاذ إجراءات مراوغة لمواجهة جهود التحقيق في تلك الهيئات. وقد يكشف الإفصاح الكامل أيضاً عن تفاصيل عن قدرات أمان هذه الهيئات أو مقدمي خدمات الاتصالات المحدودة، التي قد يستغلها الآخرون، وهو ما يؤدي إلى مخاطر إضافية للأمن السيبراني.

[99] لتقدير الأثر الاقتصادي لقانون TOLA، يجب أوّلًا يكون الإفصاح كاملاً أو عاماً. وقد تسهّل البيانات المتعددة والأكثر تفصيلاً الحصولَ على تقديرات أفضل، ولكن حتى البيانات التقريبية نسبياً عن أنواع المساعدة المطلوبة و/ أو المفروضة و/ أو المقدمة من شأنها التغلب على فجوات البيانات بشكل كبير. بالإضافة إلى ذلك، قد يُكشَف عن هذه البيانات بموجب أوامر وقائية تقيد الإبلاغ عن البيانات التفصيلية المستخدمة لتقدير الآثار الاقتصادية الإجمالية من قبل المحللين أو الباحثين المكلفين باستنتاج التقديرات. وتحديد الحد الأدنى من الإفصاح، الذي قد يسهل التقديرات المقبولة للتأثيرات الاقتصادية، هو أمر خارج نطاق هذا التقرير، ومع ذلك، فإننا نعتقد أنه يمكن تمكين الوصول المحمي إلى البيانات ذات الصلة، الذي من شأنه تسهيل تقدير الآثار الاقتصادية، مع الحفاظ على فعالية مساعدة قانون TOLA لهيئات الاستخبارات وإنفاذ القانون.

[100] في الواقع، فإن تقدير الأثر الاقتصادي لقانون TOLA جزءٌ من الرقابة اللازمة لحماية أستراليا والبلدان الأخرى من آثار التشريعات المضلّلة.

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

القانون التي تهدد الأمن الرقمي، ومن ثَم الثقة الرقمية، وهو ما يؤدي إلى تفاقم أي تأثير اقتصادي ضار قد يكون متعلقاً بالقانون.

5.2 النقاش النوعي المتعلق بالتأثيرات الاقتصادية

كما أشرنا سابقاً، فإن الآثار الاقتصادية لقانون TOLA مباشرة وغير مباشرة، وهي تتشكل وتتغير بمرور الوقت، ولها تأثير منتشر خارج أستراليا. وبعض من هذه التأثيرات ربما تكون أكثر وضوحاً ويمكن تحديدها وقياسها أكثر من غيرها. فعلى سبيل المثال، فإن تقييم الآثار المباشرة للقانون بالتركيز أولاً على شركات الأعمال الملزمة في إطار التشريع بالاستجابة لطلبات هذا القانون وإنذاراته، وعلى المنتجات والخدمات التي تقدمها هذه الشركات، والتي تستفيد من البيانات المشفرة، سواء في حالة الحركة أو الثبات، من المحتمل أن تكون فرصة جيدة للتعرف على التأثيرات الاقتصادية للقانون، التي يمكن قياسها، وهي تلك التأثيرات المرتبطة بالسلوك أو الناتج.

بالإضافة إلى ذلك، فإن الفهم الأفضل للآثار المباشرة من شأنه أن يساهم في فهم طبيعة الآثار غير المباشرة المحتملة. وكذلك، فمن الأفضل التركيز أولاً على محاولة التعرف، في ظل التجربة السابقة، هل لقانون TOLA تأثيرات يمكن قياسها قبل الشروع في تقييم الآثار المستقبلية، حتى وإن كان من المتوقع أن تحدث كل الآثار الاقتصادية للقانون في المستقبل. وهذا المنطق في التفكير يمثل الأسلوب الطبيعي لمناقشة التوقعات مناقشة نوعية، لمناقشة التوقعات الخاصة بأنواع التأثيرات التي يمكن ملاحظتها.

أولاً: ترجع طلبات قانون TOLA وإنذاراته مباشرةً لمقدمي الخدمات المحددة التي تتسع لتشمل أي شركة تقدم خدمات أو منتجات تكنولوجيا الاتصالات والمعلومات، والتي تستخدم البيانات المشفرة في أستراليا (سواء كان مقر هذه الشركات في أستراليا أم خارجها).[101] ولحتى هذا التقييم يمثل "سلسلة إمداد"[102] مركبة تشمل شركات الإنتاج أو التوزيع التي تعد مسؤولة مسؤوليةً جماعية عن توصيل خدمات ومنتجات البيانات المشفرة، لكي يستخدمها (يستهلكها) المستخدم النهائي، الذي يشمل أيضاً أعمال أخرى تستخدم البيانات المشفرة في أعمالهم اليومية (مثل البنوك والمستشفيات ومعظم الشركات في عالمنا اليوم، ولكن بدرجات متفاوتة من

[101] هذا التحديد للإطار الخاص بالقانون يستبعد اعتبار الشركات أو المستخدمين النهائيين، الذين قد يكونون هم مَن يشترون خدمات تكنولوجيا الاتصالات والمعلومات التي تستخدم البيانات المشفرة (مثل المستشفيات والبنوك، وغيرها من المستخدمين النهائيين). لكن لما كان المستخدمون النهائيون هم نقطة الطلب النهائية لاستخدام خدمات البيانات المشفرة، فإن تأثير قانون TOLA على السلوك والنتائج التي يرونها (مثل الأثمان التي يدفعونها، واختيار المنتجات التي يمكنهم الاختيار منها، أو بشكل مساوٍ لذلك جودة هذه المنتجات) كل ذلك مرتبط بتقييم التأثير الاقتصادي الإجمالي لقانون TOLA.

[102] قد تُستخدَم مصطلحات سلسلة الإمداد، أو سلسلة القيمة، أو سلسلة الإنتاج بالتبادل. وهذه المصطلحات تعكس مفهوم أن إنتاج معظم السلع والخدمات يمكن تنظيمه في سلسلة من المهام أو المراحل التي تتدفق من موارد خام، ثم مراحل متوسطة من الإنتاج، وصولاً إلى المبيعات النهائية للمستخدم النهائي. وفي أبسط صورها، يمكن اعتبار ذلك تدفقاً خطياً للمراحل التي يمكن تنظيمها في صورة حلقات من شركات الإنتاج والتوزيع، وبعض الشركات يمكن دمجها رأسياً في مراحل متعددة. والشركات التي تعمل في المرحلة نفسها تُعد منافِسة أفقية، أما الشركات التي تعمل في مراحل مختلفة فهي منافِسة رأسية. ومن ثَم، فإن المنافَسة تكون على الطلب النهائي الذي يوفر تدفقاً للأرباح يدعم نشاط سلسلة القيمة. لكن معظم عمليات الإنتاج، خاصة التي تتعلق بمنتجات وخدمات تكنولوجيا الاتصالات والمعلومات، لا تناسب هذا النموذج بوضوح. فهناك العديد من العمليات المتوازية وحلقات النتائج المركبة. ويمكن للشركات أن تكون كيانات متنافسة أفقية ورأسية.

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

الأهمية للعمليات التي يجرونها)، وأيضاً مستهلكو السوق الكبيرة (مثل مستخدمي خدمات النطاق العريض للاتصالات الثابتة والمحمولة في المنازل).

وتشمل سلسلة الإنتاج منتجي تقنيات وأجهزة التشفير وخدماته، مثل الشركات التي تُصنِّع أجهزة الشبكات، وتشارك في صياغة المعايير الدولية، وتمتلك براءات الاختراع أو العلامات التجارية لتكنولوجيات الأمن، ... إلخ. وهذه الشركات، التي تُسمَّى بشركات صناعة تأمين المعلومات InfoSec -وهي تسمية غير دقيقة- تبيع منتجات الأجهزة والبرمجيات التي تُستخدم لتوثيق الاعتمادات الرقمية، وتُجري فلترة الحركة الرقمية وتحجبها انتقائياً (مثل جدران الحماية)، وتقدم مجموعة من الخدمات الأخرى (مثل أدوات مراقبة حركة الأمن السيبراني)، التي يشتريها ويستخدمها مقدمو خدمات الاتصالات الذين يُوزِّعون الخدمات، مثل مقدمي خدمات الإنترنت كشركات Telstra وTPG، أو مقدمي الخدمات السحابية، أو خدمات الحواف التي تقدم تطبيقات وخدمات محتوى، مثل فيسبوك وجوجل ونيتفليكس. وتشمل أيضاً صناع أجهزة المستخدم النهائي والمطورين وتجار تطبيقات البرمجيات والخدمات التي تستخدم هذه الأجهزة، بدءاً من الهواتف الذكية للألواح وأجهزة إنترنت الأشياء.

ويُعد تعقُّب علاقات الأعمال بينشركات تكنولوجيا الاتصالات والمعلومات أمراً معقداً، وذلك لأنشركات تكنولوجيا الاتصالات والمعلومات تبيع لشركات أخرى عاملة في مجال تكنولوجيا الاتصالات والمعلومات،وكذلك للمستخدمين النهائيين (مثلشركات الأعمال ومستهلكي السوق الكبيرة الذين يشغِّلون الشبكات الداخلية وشبكات البيانات الخاصة). بالإضافة إلى ذلك، فإن كثيراً منشركات تكنولوجيا الاتصالات والمعلومات يعمل على مستويات مختلفة داخل سلسلة الإمداد، وربما يبيع بشكل متوازٍ ما لديه من مكونات وتكنولوجيا لتلك الشركات التي يتنافس معها في أسواق التوزيع (مثلاً: تشتريشركة آبل مكونات من سامسونج، وترخِّص التكنولوجيا، وكلتاهما تبيع هواتف ذكية).

ولتحليل التأثير الاقتصادي لقانون TOLA، يمكن أن يكون التركيز على سلسلة قيمة تكنولوجيا الاتصالات والمعلومات كليةً، التي تُوفِّر المنتجات والخدمات التي تستخدم التشفير والبيانات المشفرة، وتُعد سلسلة القيمة الكلية بمنزلة "صندوق أسود"، يوفر مجموعة من المنتجات والخدمات التي تستخدم البيانات المشفرة، وتركز على كيفية تأثير هذا القانون على العرض والطلب لهذه المنتجات والخدمات. وعلى المستوى النظري، وفي إطار تزايد الاقتصاد الرقمي، الذي قد يزداد ليشمل اقتصاد السلع والخدمات كليةً، ولما كان كل شيء في الاقتصاد الحديث يستخدم تكنولوجيا الاتصالات والمعلومات استخداماً مباشراً أو غير مباشر، فإن أهمية التشفير تتزايد، وتُعد أهم أفضل الممارسات التي تضمن "موثوقية" منتجات وخدمات الاتصالات وتكنولوجيا المعلومات، أو حمايتها من المخاطر السيبرانية، التي تشمل الحماية من انتهاك البيانات التي يمكن أن تهدد الخصوصية، أو تمثل أي أشكال أخرى من الخسارة الاقتصادية (مثل الاحتيال والهجمات للحصول على فدية، وتدمير القيم، وفقدان السلامة الشخصية،... إلخ).

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

ومن هذا المنظور، فإن قانون TOLA يمكن اعتباره قانوناً ينطوي على تكلفة لتأمين البيانات، ومن ثَم، يشكل تهديداً للـ"ثقة" في المنتجات والخدمات الرقمية، وهي أمر مطلوب من أجل استخدام الإنترنت وشبكات البيانات الأخرى الخاصة بالتجارة الكترونية، التي ستشمل، كما ذكرنا آنفاً، الاقتصاد كله. وبتحليل اقتصادي بسيط، فإن التكلفة الزائدة لتوفير خدمات الاتصالات وتكنولوجيا المعلومات "الموثوق بها" سوف ترفع تكلفة العرض، وتخفض "استعداد المستخدم النهائي للدفع". وسيؤدي ذلك إلى زيادة العرض المجمع وانخفاض الطلب، وهو ما سيسفر عن توازن أعلى للسعر عند المستوى الأدنى من الطلب المجمع، في مرحلة ما بعد قانون TOLA.

ويمكن أن ترتفع الأسعار، وأن يقل الطلب المجمع، الأمر الذي سيؤدي إلى ما يطلق عليه الاقتصاديون " خسارة الوزن الثقيل"، والمرتبطة بفرض هذا القانون.

ولو توقَّف الأمر عند هذا التحليل البسيط للآثار المترتبة على قانون TOLA، لما كان اعتماد هذه السياسة أمراً غير مقبول، فهناك عوامل تزيد الأمر تعقيداً، ومنها الحقيقة التي لُمحنا إليها سابقاً، وهي أننا نتجاهل السبل الممكنة التي تمكن هذا القانون من زيادة الثقة، عن طريق تمكين إنفاذ القانون ليكون أفضل في منع الجريمة، ويؤدي إلى زيادة في الطلب المجمع، وهو الأمر الذي يمكن أن يعوِّض أي خطر يسببه قانون TOLA بسبب فقدان الخصوصية، أو بسبب تحمُّل أي تكاليف من الشركات نتيجة القيود التي يفرضها القانون على استخدام التقنيات المشفرة.

ومما يزيد الأمر تعقيداً عند تحليل قانون TOLA هو أن الآثار المترتبة عليه ليست واحدة في كل قطاعات الاقتصاد، ولا في كل مراحل سلسلة الإمداد الخاصة بتكنولوجيا الاتصالات والمعلومات، ولا بالخدمات والمنتجات التي تستخدم التشفير، ومن ثَم، للطلب النهائي للمنتجات والخدمات. وإحدى وسائل التطرق لهذا التحدي تطبيقُ إطارِ العمل المذكور تطبيقاً منفصلاً في كل قطاع من القطاعات ومراحل إنتاج تكنولوجيا الاتصالات والمعلومات، أو الأسواق الخاصة بالمنتجات والخدمات، وذلك على المستوى النظري، ثم تشكيل التفاعلات بين هذه التحليلات المختلفة، التي يُعد جزءٌ منها مرتبطاً بالاقتصاد، وجزء آخر مرتبطاً بالتوازن، وذلك لحساب كل التأثيرات الأخرى. وهذه التحليلات يمكن إجراؤها ربما من خلال نموذج مفصل لكل مدخلات الاقتصاد ومخرجاتها، أو سلسلة إمداد قطاع الاتصالات وتكنولوجيا المعلومات، التي تتبع المشتريات والمبيعات التي تجريها الشركات أو مجموعة من الشركات (أو الصناعات أو قطاعات الصناعة)، ثم حساب تأثير قانون TOLA على الأسعار وكميات هذه التعاملات. ومن المبادئ العامة، فكلما كان النموذج أكثر تفصيلاً، وكلما كانت البيانات وأدوات وضع النماذج والتوقع الخاصة بتنفيذ النموذج أفضل، كلماكانت الصورة أفضل فيما يتعلق بكلٍّ من التأثيرات المجمعة والموزعة لهذا القانون.

ويتيح هذا النموذج الاقتصادي المثالي دراسة كيف يتغير سلوك أعمال الاتصالات وتكنولوجيا المعلومات والمستخدمين النهائيين والمستهلكين من الأفراد، استجابةً لقانون TOLA، وما

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

يمارسه من تأثير مباشر على الشركات، ثم نتيجةً لردود أفعال الشركات الأخرى وهكذا. وهذه الاستجابات المباشرة وغير المباشرة للشركات قد تنتج في نهاية الأمر توازناً يشابه الذي كان قبل صدور القانون (في عالم "لو لم يكن هناك") لمعرفة هل المنافع الكلية المجمعة التي تحققت للاقتصاد الأسترالي أو العالمي أكثر في ظل قانون TOLA أم أقل، وأيضاً كيف تُوزَّع هذه المنافع المجمعة الكلية.

ومن المؤسف أن هذا النموذج المثالي لا يمكن تنفيذه، لأنه لا يوجد أي من العناصر المطلوبة. فقبل النظر في الأدوات الاقتصادية المتاحة وطرق صياغة هذا النموذج المثالي، يكفي أن نشير إلى أن الغياب شبه الكامل للبيانات ذات الصلة يُعد في ذاته عقبةً كافية لتقدير التأثير الاقتصادي لقانون TOLA. فلا بيانات كافية لأي تحديد، حتى وإن كان غير واضح المعالم، ومن ثَم لا يمكن قياس التأثيرات السلوكية للشركات في سلسلة إمداد تكنولوجيا الاتصالات والمعلومات التي تتأثر بالقانون.

ويرى مؤيدو قانون TOLA أن أي تأثير اقتصادي غير مرغوب فيه للقانون هو تأثير بسيط، وذلك لأن:

- مقدمي خدمات الاتصالات المحددة هم فقط الذين يتلقون إنذارات؛
- قانون TOLA يتيح استعادة التكاليف المعقولة التي تتحملها الشركات استجابةً للإنذارات.
- قانون TOLA يمنع هيئات الاستخبارات وإنفاذ القانون من مطالبة مقدمي الاتصالات المحددة من فعل أي شيء يتسبب في إلحاق ضرر منظم بأمن المنتجات والخدمات الخاصة بها. [103]

وتذهب وجهة النظر تلك إلى أن القليل من الشركات فقط سيتأثر بقانون TOLA، وأن التأثير على الموثوقية (الجودة) وعلى السعر (التكلفة) لمنتجات هذه الشركات وخدماتها سيكون بسيطاً جداً، ومن ثَم لن يكون هناك أي تأثيرات اقتصادية ضارة ذات قيمة من ناحية التوزيع، أو أضرار مجمعة نتيجة لهذا القانون.

ومن ناحية أخرى، فإن معارضي تشريعات الوصول الاستثنائي، مثل قانون TOLA، التي تشمل معظم المجتمع الفني العالمي وصناعة تكنولوجيا الاتصالات والمعلومات يعارضون هذين الادعاءَين. والدليل على ذلك ما جاء في تقرير Carnegie الصادر عام 2019 م، الذي أكد النتائجَ نفسها التي جرى التوصل إليها من قبلُ في تقرير أصدره مجموعة من الخبراء، الذين توصلوا إلى

[103] يتميز الضرر المنظم للأمن الرقمي عن الخفض المقصود للأمن الرقمي للشخص أو الأشخاص المستهدفين، الذين يكونون الهدف الذي يجري التركيز عليه في طلبات قانون TOLA.

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

أنه لا يوجد أسلوب معروف لتمكين هذا الشكل من الوصول للبيانات المشفرة الذي يتوقعه قانون TOLA دون خلق نوع من الثغرات الأمنية.[104]

وفي محاولة وضع إطار لتحليل التأثيرات الضارة المتوقعة نتيجة قانون TOLA، سيكون للثغرات الأمنية الناتجة عن القانون -ومن ثَم تمكين الوصول المستهدف للبيانات المشفرة، وهو ما يسهله القانون- أثر ضار على الثقة في الأمن السيبراني.[105] وهذا التأثير الضار على الثقة يمكن أن يكون نتيجة عدة عوامل.

أولاً، إن احتمالية أن يؤدي قانون TOLA إلى وصول هيئات الاستخبارات وإنفاذ القانون للبيانات التي يعتبرها المستخدم آمِنةً تعني أن المستخدم سيواجه انخفاضاً في الأمن السيبراني. ثانياً، لما كان هذا القانون يخلق نوعاً من عدم الثقة في البيانات التي تُستهدَف، فإن ذلك يعني بالضرورة زيادة الخطر السيبراني للجميع.[106] ثالثاً، إن تقبل وجهة النظر التي يطرحها تقرير Carnegie أنه لا يوجد أسلوب معروف لتمكين الوصول المستهدف دون حدوث ثغرات أمنية، فإن تطبيق قانون TOLA سيقلل من الأمن السيبراني لأي نظام أو خدمة يمكن أن تؤدي إلى وجود ثغرات أمنية. وهذه العوامل تشير إلى إحداث هذا القانون لخطر زائد على الأمن السيبراني.

حتى في حالة القدرة على التحكم في الثغرة الأمنية، فإن التعليقات التي أُرسلت خلال مدة التشاور العام بشأن قانون TOLA قبل إقراره في كانون الأول/ ديسمبر 2018 م تلقي الضوء على الطرق المتعددة التي أدى إقرار القانون من خلالها إلى زيادة عدم الثقة في قدرات الحكومة على التأثير على الأمن السيبراني.[107] ومن ثم، فحتى في حالة الإقرار بأن التهديد الحقيقي للأمن السيبراني، أو أن الزيادة في الخطر السيبراني أمر بسيط، فإن احتمالية حدوث آثار غير مرغوب فيها يضر بالثقة، ويمكن أن تؤدي إلى آثار اقتصادية كبيرة ضارة لا يقف تأثيرها على شركات الاتصالات وتكنولوجيا المعلومات أو مقدمي خدمات الاتصالات المحددة فحسب.

ومن ثم، فإن إحدى سُبل التطرق لقانون TOLA النظرُ فيما يحدثه التأثير الاقتصادي لانخفاض الثقة في الأمن السيبراني على الاقتصاد. فإن انخفاض الثقة يمكن أن يؤدي إلى خفض الطلب

---

[104] انظر: "تحريك حوار سياسة التشفير قدماً" مجموعة عمل التشفير، وقف Carneige للأمن الدولي، أيلول/ سبتمبر 2019، https://carnegieendowment.org/files/EWG__Encryption_Policy.pdf. وهذا التقرير يلخص النتيجة التي توصلت لها مجموعة عمل التشفير، التي أسست مؤسسة Carenige لتقديم الإرشاد لكبار المسؤولين داخل مجتمع الأمن السيبراني بشأن كيفية التعامل مع تشريع النفاذ. والنتيجة الإجمالية كانت أنه لا يوجد (حتى الآن) أي وسيلة لتمكين الوصول القانوني دون إحداث ثغرات أمنية في النظام.

[105] نستخدم "الثقة" هنا للإشارة نظرياً إلى وجهات نظر أصحاب المصلحة (العملاء والشركات وصناع السياسات، ... إلخ) فيما يتعلق بالأمن السيبراني، التي لا تتوافق توافقاً كاملاً مع الوضع الحقيقي للأمن السيبراني.

[106] يمكن القول بأنه لما كان المجرمون فقط هم مَن يجب أن يكونوا هدف طلبات النفاذ القانونية، فإن احتمالية أن يصبح المواطنون الشرفاء أيضاً أهدافاً لا يجب تجاهلها، إلا أن ذلك يعتمد على تقبُّل فكرة أن القوى التي يمنحها قانون TOLA لن تُستخدَم بالخطأ أو عن عمد، وكلا الافتراضين يثير شكوكاً لا يجب تجاهلها.

[107] تلقَّت الإدارة الأسترالية للشؤون الداخلية 343 تعليقاً قُدِّم خلال مدة التشاور العامة (انظر: https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/the-assistance-and-access-bill-2018). ومن المخاوف الشائعة التي ذكرها المعلقون غياب الوضوح فيما يتعلق بحدود القوى التي يتيحها قانون TOLA وفعالية الحماية والرقابة، وغياب الشفافية، وغياب أي تحليل تجريبي للتأثير الاقتصادي للقانون. وكل هذه المخاوف وما يتبعها من تحديات تسهم في زيادة عدم الوضوح بشأن التأثير المحتمل للقانون على الأمن السيبراني.

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

والنشاط في الاقتصاد الرقمي، وهو ما يؤدي إلى خفض أو تأخير (الأمر الذي يقلل القيمة الاقتصادية للقيم الحالية) نمو وابتكار إنتاجية تكنولوجيا الاتصالات والمعلومات.[108]

وإحدى طُرق قياس القيمة الاقتصادية لزيادة خطر الأمن السيبراني أو انخفاض الثقة على الاقتصاد كليةً صياغةُ سيناريوهات متوقعة لما يمكن حدوثه تحت مختلف مستويات الثقة. ومن الأمثلة الجيدة على ذلك الأمر التحليل الذي أجرته مجموعة تأمين زيورخ عام 2015 م[109] التي استخدمات نموذجاً للاقتصاد الكلي لتوقُّع منافع نمو الاقتصاد العالمي تحت مجموعة من السيناريوهات التي تختلف باختلاف مستويات الثقة في الإنترنت الآمن.

وطبقاً لسيناريو الثقة العالية، فإن الجريمة الإلكترونية لا تمثل تهديداً للتجارة الإلكترونية، والنمو الاقتصادي يجري بشكل أسرع. لكن طبقاً لأسوأ السيناريوهات، فإن الجريمة الإلكترونية تدمر الثقة في الأنشطة الاقتصادية على الإنترنت، ومن ثَم، يكون نمو التجارة الإلكترونية بطيئاً، وتكون الحالة الأساسية وسَطاً بين الحالتين. وتشير هذه الدراسة إلى وجود فجوة بين توقعات أفضل الحالات وأسوئها حتى عام 2030 م يصل إلى 120 تريليون دولار أمريكي، يشمل 6% تغير في الناتج المحلي الإجمالي العالمي المتراكم، وذلك يشير إلى التهديد الحقيقي الذي تمثله الجريمة الإلكترونية على الاقتصاد العالمي. ويكون النمو الأبطأ نتيجةَ انخفاض الطلب على الاشتراك في التجارة الإلكترونية، وما ينتج عنه من انخفاض في الحوافز التي تشجع شركات الإمداد على الاستثمار في ذلك المجال.

وبالتطبيق بشكل أكثر قرباً على الوضع في أستراليا، قدر تقرير AustCyber الصادر في تموز/ يوليو 2020 م أن النشاط الرقمي "يساهم بـ426 مليار دولار أسترالي في الاقتصاد الأسترالي، ويحقق تريليون دولار أسترالي في الناتج الإجمالي الاقتصادي، وهو ما يعني وظيفة بين كل 6 وظائف".[110] ووفق تقديرات هذا التقرير، فإن أي إضطراب أو تدخل رقمي يستمر أربعةَ أسابيع نتيجة أي هجوم سيبراني واسع الانتشار يمكن أن يتسبَّب في خسائر تصل إلى 1.5 % من إجمالي الناتج المحلي السنوي الأسترالي."[111] ويُعد ذلك تقديراً للآثار المبلشرة للهجوم الناجح، وأي زيادة في الخطر الإلكتروني تعني أن هذه النتيجة من المحتمل أن تحدث.

---

[108] هناك الكثير من الأعمال الاقتصادية المهمة التي توضح أن الاستثمار في تكنولوجيا الاتصالات والمعلومات يمكن أن يحقق عوائد كبيرة، وأن يساهم في نمو الإنتاجية الاقتصادية. وتلخيصاً لذلك، انظر: ليهر دابليو وشارفات إيه (2017) "محركات تكنولوجيا الاتصالات والمعلومات للتنمية المستدامة" في إيه شارافات ودابليو ليهر (eds)، النمو الاقتصادي المتمركز على تكنولوجيا الاتصالات والمعلومات، جنيف، سويسرا: الاتحاد الدولي للاتصالات، https://www.itu.int/dms_pub/itu-d/opb/gen/D-GEN-ICT_SDGS.01-2017-PDF-E.pdf أو البنك الدولي (2016) تقرير التنمية العالمية 2016 والمقسمات الرقمية http://www.worldbank.org/en/publication/wdr2016

[109] انظر: زيورخ (2015) مخاطرة Nexus: هل يمكن تفاديها بالخطر السيبراني؟ المنافع الاقتصادية وتكلفة المستقبل السيبراني البديل" تقرير أعده مجلس الأطلنطي ومجموعة تأمين زيورخ (Zurich)، أيلول/ سبتمبر 2015، http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf

[110] انظر: تقرير AustCyber (2020) "تقرير الثقة الرقمية لأستراليا": https://www.austcyber.com/resource/digitaltrustreport2020. تقرير تموز/ يوليو 2020، 52 صفحة. ووفقاً لتقديرات التقرير، فإن النشاط الرقمي يدعم 22% من الاقتصاد الأسترالي، وهو ما يمثل 6% من إجمالي الناتج القومي مباشرةً. وتشمل القطاعات: 317 مليار دولار للنشاط الرقمي: 16 مليار دولار للأمن السيبراني، و335 مليار دولار للبيع بالتجزئة على الإنترنت، و2.7 مليار دولار للصحة الرقمية، و 0.7مليار دولار للطاقة الشمسية، و 3.9مليارات دولار للفضاء، ... إلخ. (صفحة 11).

[111] المرجع السابق، صفحة 5. ويقدر التقرير أنه يمكن خسارة 30 مليار دولار أسترالي و163 ألف وظيفة نتيجةً للهجوم الواسع الانتشار.

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

وما تشير إليه هاتان الدراستان هو أن احتمالية وقوع آثار كبيرة غير مرغوب فيها ورادة، ومن ثَم فمن المهم دعم الثقة في الأمن الرقمي. ومع الأسف، لا يعرض التقريران أي توجه مفيد لكيفية تحديد الكمِّ الذي سيزيد به الخطر السيبراني نتيجة قانون TOLA، إلا أنهما يؤكدان ضخامة هذه التأثيرات واتساع نطاقها لتشمل الاقتصاد كله. [112]

ومن الممكن أيضاً النظر في احتمال حدوث آثار ضارة إقليمية، أو أضرار خاصة بقطاع ما نتيجة تهديد الثقة. فعلى سبيل المثال، من المتوقع لقطاعات الاتصالات وتكنولوجيا المعلومات الأسترالية أن تعاني من صدمة أكبر مرتبطة بقانون TOLA في المستقبل القريب، والمرتبطة بالثقة الأقل في المنتجات والخدمات، مقارنةً بقطاعات تكنولوجيا الاتصالات والمعلومات في دول أخرى، التي لا تتأثر تأثراً مباشراً. ويمكن لذلك الوضع أن يؤثر تأثيراً ضاراً على التنافس الدولي لقطاع الاتصالات وتكنولوجيا المعلومات الأسترالي. ويمكن أيضاً النظر لأكثر من المستوى القومي لدراسة الأقسام الفرعية لقطاعات الاتصالات وتكنولوجيا المعلومات وباقي القطاعات، التي تعتمد بشكل متجانس على استخدام البيانات المشفرة بمستويات مختلفة، والتي يمكن أن تتأثر نتيجة قانون TOLA.

وعلى مستوى الشركات، من المتوقع أن يؤدي قانون TOLA إلى إحراز آثار مباشرة أو غير مباشرة. فعلى سبيل المثال، قد يقلل انخفاضُ الطلب المجمع على منتجات الشركة نتيجة انخفاض الثقة في السوق نصيبَ كل الشركات. بالإضافة إلى ذلك، فإن فقدان الشركات لدرجة أعلى من الثقة قد يقلل نصيب الشركة في السوق من الطلب المجمع المنخفض. وآثار انخفاض أمن البيانات تتراوح بين كونها آثاراً بسيطة (مثل خسارة بعض المبيعات لبعض المنتجات) وآثاراً جسيمة (مثل التهديد الوجودي لمستقبل عمل الشركة في حالة أن يؤدي قانون TOLA إلى أن يفقد المشاركون في السوق الثقة في التزام الشركة بالشفافية وتأمين بيانات المستهلك).

وهذه النتيجة الأخيرة تمثل قلقاً كبيراً للشركات التي تقوم نماذج الأعمال الخاصة بها على برمجيات المصدر المفتوح، وعلى الخدمات والمنتجات المتاحة في الأسواق ومنتجات السوق الكبيرة وخدماتها (أي الخدمات والمنتجات التي لا تُعدَّل على أساس رغبات المستهلك).

ويلزم الالتزام بالمصدر المفتوح بوصفه مكوناً أساسياً لمنصة العمل الشركة بمستوى من الشفافية لا يتماشى مع القيود التي يفرضها قانون TOLA، والتي تقيِّد قدرة الشركات على الإفصاح عن التغييرات المقدمة للعروض، أو عن الأكواد التي ربما كان الإفصاح عنها مطلوباً عند الاستجابة لإنذار القانون.

[112] قد يكون التأثير كبيراً إذا تسبب في اختراق واحد للبيانات ذي تأثير كبير، أو إذا تسبب في عدد من الاختراقات الأخرى التي قد تكون صغيرة، ولكنها كبيرة في تأثيرها، أو إذا كان هناك مزيج من الاثنين. والنقطة المهمة هنا هي أن ثغرات الأمن السيبراني قد تنتج أنواعاً مختلفة من الضرر التي تختلف في شدتها وفي نطاقها. وفي غياب نموذج للتهديد، واحتمالية نجاح تهديدات أخرى، فمن غير المعقول أن نتوقع الضرر المتوقع حدوثه.

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

ولتقييم التأثير الاقتصادي لقانون TOLA، يكون على الشركة أن تتوقَّع احتمالية تلقيها لطلب أو إنذار بمقتضى هذا القانون، وهو ما قد يؤثر على العمليات الخاصة بها، ودراسة كيفية حدوث هذا التأثير، وما فرص الاستجابات. وذلك يتماثل مع طريقة تقييم الشركات للمخاطر السيبرانية، وتحديد أفضل الإستراتيجيات للاستثمار في منتجات وخدمات أمن المعلومات InfoSec، مثل جدران الحماية وخدمات مراقبة حركة البيانات، وغير ذلك من المصادر الداخلية للأمن السيبراني، ومنها التأمين الإلكتروني CyberIns الذي يتناول أي خطر سيبراني متبقٍّ، ولا يمكن التطرق له ومواجهته من خلال العمليات المعدلة للأمن السيبراني.[113] وفي الأقسام الفرعية اللاحقة من التقرير نلقي الضوء على بعض أساليب المواجهة التي تتبعها الشركات في مواجهة التأثيرات الضارة لقانون TOLA.

5.3 ازدياد عدم الثقة في الأعمال

يزيد قانون TOLA انعدامَ الثقة التنظيمية كما أشرنا قبل ذلك، وكذلك، تؤدي زيادة عدم الثقة الفنية والسوقية والتنظيمية إلى زيادة الخطر الذي يواجه الاستثمارات بشكل لا يمكن علاجه فيما بعد، ويضر بهذه الاستثمارات. ويصعب عامةً قياس تأثير انعدام الثقة في الأعمال، ولا يكون هذا القياس عملياً عندما يتعلق الأمر بتشريع محدد مثل قانون TOLA.

لكن الدراستين الوحيدتين اللتين أُجرِيَتا لتقييم التأثير الاقتصادي لقانون TOLA تشيران إلى أهمية أي تشريع يؤثر على انعدام الثقة التنظيمية والمرتبط بتشفير التكنولوجيا. وقد أجرى هاتين الدراستين المعهدُ القومي الأمريكي للمعايير والتقنية NIST عامي 2001 و2018 م.

ففي دراسة تأثير التشفير التى أجراها المعهد 2001 م [114]سعى الباحثون لتقييم المساهمة الاقتصادية لمعيار تشفير البيانات DES في الاقتصاد الأمريكي. وتوصلت الدراستان إلى أن جهود المعهد القومي الأمريكي للمعايير والتقنية قد أسرعت من استخدام معيار تشفير البيانات DES

[113] اتخاذ قرارات للاستثمار بشأن أمن المعلومات والتأمين السيبراني InfoSEc/CyberINs أمرٌ يشمل الكثير من المعلومات، ومن ثَم هو أمر مكلّف. أرورا وآل (2004) هيوبارد وسيرسن (2016) وجونز (2005) جوردون ولووب (2002). واقترح آخرون أدوات ووسائل نظرية لاتخاذ القرار للمساعدة في تقدير التكاليف السيبرانية وإستراتيجيات منافع الأمن السيبراني البديل للمساعدة في صنع القرار الاستثماري. انظر: أرورا أيه ودي هال وسي بياتو ودي رامسي وار تيلانج (2004) "قياس قيمة المخاطرة لحلول أمن تكنولوجيا المعلومات" خبراء تكنولوجيا المعلومات 42-35 (6) 6، هوبارد دي دابليو وار سيرسن (2016). وكيف يمكن قياس أي شيء يتعلق بخطر الأمن السيبراني. جزن ويلي وأبناؤه: نيويورك 2016 وجوردون إل أيه ولوب إم بي (2002). واقتصاديات استثمار أمن المعلومات. وتحويلات ACM لأمن الأنظمة والمعلومات 457-438 (4) 5 TISSEC. ولفهم بعض من التحديات المرتبطة بتقييم التأثير الاقتصادي للجريمة السيبرانية، انظر: ولف جوزفين ووليام ليهر (2017) "درجات الجهل بشأن تكلفة اختراق البيانات: ما الذي يمكن أن يفعله صناع السياسات وما لا يستطيعون فعله بشأن غياب البيانات التجريبية الجيدة"، مؤتمر البحث الخامس والأربعون بشأن الاتصالات والمعلومات وسياسة الإنترنت (TPRC45)، أيلول/ سبتمبر 2017، الإسكندرية VA متاح على: SSRN https://ssrn.com/abstract=2943867

[114] انظر: ليش دي وأم شينورث (2001) " التأثيرات الاقتصادية لبرنامج معيار تشفير البيانات DES التابع للمعهد القومي للمعايير والتقنية". دراسة أعدها للمجموعة مكتب برنامج التخطيط الإستراتيجي والتحليل الاقتصادي التابع للمعهد القومي للمعايير والتقنية NIST، تشرين الأول/ أكتوبر 2001 https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=918355 (فيما بعد دراسة تأثير التشفير للمعهد القومي للمعايير والتقنية 2001).

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

لسنوات عديدة، وهو ما أسفر عن صافي عوائد تتراوح بين 345 مليون دولار أمريكي و1190 مليون دولار أمريكي وذلك نتيجة انخفاض تكاليف إدارة بيانات البنك من قبل طرف ثالث.[115]

وفي الدراسة اللاحقة التي أجراها المعهد عام 2018 م، كان التركيز على التأثير الاقتصادي لمعيار التشفير المتقدم AES، الذي كان للمعهد أيضاً دور في دعمه.[116] وقد اعتمدت الدراسة الأخيرة على استبيان لاستخلاص التقديرات بشأن كيفية مساعدة معيار التشفير المتقدم AES على خفض التكاليف التي تتحملها الشركة النشطة في استخدام تقنيات التشفير بسبب وجود معيار حكومي. وافترضت تلك الدراسة وضعاً معيناً، حيث يكون التحرك نحو صياغة معيار AES بطيئاً.

وفي هذه الحالة، استفاد الباحثون من قدرتهم على وضع نموذج تحسينات الأداء التي يوفرها معيار AES، مقارنةً بالمعيار الذي جاء بديلاً له. وقدَّرت الدراسة التي أجراها المعهد القومي الأمريكي للمعايير والتقنية عام 2018 م أن المعدل الداخلي للدخل من استثمار المعهد القومي للمعايير والتقنية في دعم وترويج معيار التشفير المتطور زاد بنسبة 81% عن تكلفة رأس المال الخاصة بالمعهد، التي تصل إلى 7% (وفقاً للقواعد الحكومية)، وأن مجمع صافي العوائد على الاقتصاد زاد على 250 مليون دولار أمريكي بعد حساب كل الآثار المباشرة وغير المباشرة لانتشار المعيار.

وتوصلت كلتا الدراستين إلى أن الاستثمار في إسراع انتشار قدرات التشفير يعود بمكاسب كبيرة على الاقتصاد، ومن ثَم يمكن اعتبار أن التأخير في استخدام تقنيات التشفير المتطورة (من خلال تبطيء الاستخدام أو الاستخدام الذي يميل إلى تشفير آمن أقل) بسبب قانون TOLA يمكن أن يكون له آثار سلبية كبيرة. وأيضاً في كلتا الحالتين يمكن أن نتفهم جهود المعهد القومي الأمريكي للمعايير والتقنية في دعم تقبل معيار الصناعة من أجل خفض انعدام الثقة في الأعمال.

.

5.4 تدمير هوية الأعمال

تصوغ الشركاتُ هُوياتها من خلال الإعلان، ومن خلال السمعة الجيدة عن طريق مقارنة منتجاتها في السوق، وتنافس بعروضها عروض الشركات الأخرى. وكلما كانت هوية الشركة أفضل، كان من الأسهل على الشركة أن تبيع منتجاتها وتحصل على عوائد من المبيعات، وأن تدافع عن نفسها

[115] هدف الدراسة توضيحُ مساهمة المعهد القومي للمعايير والتقنية NIST في النمو الاقتصادي. وتوثق دراسة الحالة دور المعهد القومي للمعايير والتقنية في الترويج ودعم الاستخدم المبكر لمعيار التشفير للصناعة. ومعيار تشفير البيانات أُقِرَّ في 1977، وبحثت الدراسة سلوك الاستخدام من 1977 إلى 1982. وقد حاول الباحثون مبدئياً تجميع بيانات الاستبيان ليقيسوا مباشرةً التأثيرات، وقد باءت تلك المحاولة بالفشل. وكان البديل الذي استخدموه حساب التأثير اعتماداً على نتائج محددة معتمدة على التكاليف التي تجنبتها بنوك البيع بالتجزئة في الولايات المتحدة، التي تمكنت من التحول للمعاملات الإلكترونية (تكلفة أقل) بشكل أسرع مما كان عليه الوضع. وقد قدَّروا تكلفة تجنب المعاملات الإلكترونية، كما أدركوا ذلك عبر الوقت (في العالم الحقيقي)، وقارنوا هذه النتائج بسيناريوهات (لو لم يكن لهذا الأمر) (المنافع التي أُجلت مدةً تتراوح بين 3 و6 سنوات)، وأجروا حساب NPV لكل السيناريوهات لتقدير صافي التأثير لمجهودات المعهد القومي للمعايير والتقنية.

[116] انظر: ليش دي وجون سكوت (2018) التأثيرات الاقتصادية على معيار التشفير المتطور 1996-2017، تقرير أُعِد للمعهد القومي للمعايير والتقنية NIST GCR 18-017 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, United Kingdom +44 7554 065 718

أمام المنافسين، أو أن تحقق الاستجابة لتغييرات السوق غير المرغوب فيها، وزادت جاذبية الشركة لدى المستثمرين. وفي حالة ثبات باقي العوامل، فإن صورة الهوية الفُضلى ترتبط بارتفاع المبيعات عبر الوقت، ومن ثَم تحقيق قيمة سوقية أعلى (تعكس تقييم السوق لانخفاض أرباح الشركة). وذلك يُعد من الأصول غير الملموسة التي لا يمكن قياسها مباشرةً، إلا أن تقييمها ممكن من خلال مقارنتها بالتغيير في مؤشرات أخرى يمكن قياسها، مثل المبيعات والأرباح والقيمة السوقية أو الاستبيانات التى تتعرف على آراء المستثمرين أو العملاء ووجهات نظرهم.

ويمكن أن يتسبب أي تهديد للثقة في الشركة في تدمير هويتها، وهو ما يؤثر على المبيعات وقيمة الأعمال. وعلى الرغم من أن العملاء وشركاء العمل والمستثمرين والعاملين داخل الشركة يمكنهم أن يجروا تقييماً نوعياً لقانون TOLA وهل يمكن أن يتسبب في تأثير قوي على هوية الشركة أم لا، فإن هذا التأثير لا يمكن تحديده كمِّياً تحديداً مباشراً.

ووفقاً لبعض تفسيرات قانون TOLA، يمكن اعتبار التأثير الضار المحتمل للقانون تهديداً لوجود بعض الشركات التي تعتمد هويتها اعتماداً كبيراً على التزامها بالأمن السيبراني و/ أو بنماذج الأعمال التي تعتمد على برمجيات المصدر المفتوح. فعلى سبيل المثال، ربما تجد الشركات العاملة في مجال الأمن السيبراني، وخاصة تكنولوجيا التشفير، أن منتجها الأساسي يتضرر من تمكين جديد يهدد الخدمة. ويمكن أيضاً أن يتسبب ذلك في الإضرار بنموذج العمل لشركة قائمة على الالتزام ببرمجية المصدر المفتوح المتميز بالشفافية، التي لا تفرق بين المستخدمين النهائيين.

والحاجة إلى تعديل الشفرة لهدف ما، ثم العجز عن الإفصاح عن هذه التعديلات لباقي العملاء (نتيجة متطلبات عدم الإفصاح التي ينص عليها قانون TOLA) لا تتماشى مع المكون الرئيسي لنموذج الأعمال. وفي حالة أخرى، فإن الشركة التي تبني نموذج عملها عن طريق تملُّك الشفرة التي يمكن أن تضر بأحد الأصول الأساسية، إذا تسبب قانون TOLA في إجبار الشركة على الإفصاح عن تلك الشفرة، التي يمكن أن تكون عرضة للتشفير.

5.4 المبيعات المفقودة

على الرغم من أنه لا يمكن إتمام قياس نقدي للتأثير المباشر على هوية العمل، فإن التأثير على المبيعات يمكن قياسه. فيمكن لشركة ما أن تتبع حدثاً معيناً قد يتسبب في إلحاق الضرر بالسلوك الشرائي لعملاء معينين، أو تجاه منتجات محددة. وربما تلاحظ شركة ما أن العملاء يشترون عروض الشركة بصورة أقل، بسبب قلقهم من تهديد قانون TOLA لأمن البيانات.

وتعكس هذه المبيعات المفقودة استهلاكاً أقل للمشترين (مثلاً تعكس انخفاضاً في الطلب المجمع في عالم تزيد فيه نسب عدم الثقة)، أو تحوُّل المبيعات للمنافس. وهذا المنافس ربما

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

كانشركة أخرى في السوق نفسها (أستراليا)، أوشركة خارج البلاد. وهذه التغييرات في السلوك الشرائي للمستهلك، ومن ثم في مبيعات الشركة، يمكن أن تنطبق على مجموعات محددة من المنتجات بنسب متفاوتة. وغالباً ما تتواصل الشركة مباشرةً مع العملاء الفعليين أو المحتملين للتعرف على ما يهتمون به، وسبب شرائهم لما يريدون شراءه. وربما تصل الشركات أيضاً إلى الاستنتاج نفسه من دراسة مشتريات العملاء، أو من استبيانات تجريها أطراف ثالثة تسعى إلى تقدير القيمة التي يراها العملاء في مختلف الخدمات المرتبطة بالأمن.

وعلى الرغم من أن بيانات المبيعات، عامةً، هي واحدة من مصادر الآثار المباشرة التي يمكن ملاحظتها، فإن ربط التغيير في المبيعات بتشريع محدد مثل قانون TOLA دائماً ما يكون أمراً صعباً، وهذا لعدة أسباب: أولاً، هناك الكثير من العوامل التي تؤثر على سلوك العملاء، وقد يصعب فصل تأثير هذه العوامل. ثانياً، عند توقع هذه التأثيرات في المستقبل، يجب أيضاً الأخذ في الاعتبار صعوبة توقُّع أحداث مستقبلية غير مؤكدة. ثالثاً، العملاء لا يكونون دائماً صادقين في شرح السبب الذي يدفعهم لشراء المشتريات. فربما لا يريدون مشاركة المعلومات لأنهم لا يريدون أن يتسببوا في إحراج المورد، أو لأنهم ينتابهم القلق من الإفصاح عن الكثير من المعلومات. وبغضّ النظر عن سبب انخفاض المبيعات، فإن هذا الانخفاض يُترجَم إلى أرباح منخفضة (على فرض أن الشركات سوف تتجنب المبيعات التدريجية التي لا تحقق أرباحاً كافية لتغطية التكاليف التدريجية)[117]؛ وانخفاض الأرباح المستقبلية يعني انخفاض القيمة الاقتصادية للشركة.

وعلى الرغم من صعوبة التفكير في كيفية تقييم المبيعات المفقودة، فإن هناك عدداً من الأسباب التي تبرر خطورة تأثر المبيعات. فعلى سبيل المثال، في تموز/ يوليو 2020 م، أصدرت محكمة العدل الأوروبية قراراً كان يتوقعه الكثيرون، يقضي بإيقاف تبادُل بيانات العملاء بين الشركات العاملة في الولايات المتحدة الأمريكية وأوروبا، إذا تسبب هذا التبادل في انتهاك القواعد الأوروبية للخصوصية، وهو ما شكل تهديداً للشركات التي تمارس هذا النشاط، التي أصبح عليها إما أن تعمل على زيادة حماية البيانات، وإما أن توقف عمليات التبادل تلك.[118]

ويمكن اعتبار قانون TOLA قانوناً يهدد القدرة على الإيفاء بالمعايير الأكثر تشدداً لحماية البيانات، وهي تلك المعايير التي يقرها الاتحاد الأوروبي، التي تشكل -بالتبعية- تهديداً لقدرة الأعمال على تبادل البيانات بين أستراليا والاتحاد الأوروبي. بالإضافة إلى ذلك، فإن هذا القانون يُعَد مؤشراً على مزيد من التوسع في صلاحيات الحكومية في أستراليا، أو في أي مكان آخر لفرض الوصول إلى البيانات السرية، وهو ما قد يؤدي إلى مزيد من الاضطراب في تدفق البيانات.[119]

[117] نتجاهل هنا الإستراتيجيات القصيرة المدى مثل مبيعات الخسارة loss leader، أو عمليات الأعمال خلال الفترات المؤقتة للانكماش.

[118] انظر: قرارات Shrems II: دراسة تحويل البيانات بين الولايات المتحدة الأمريكية والاتحاد الأوروبي "iapp Privacy Tracker" https://iapp.org/news/a/the-schrems-ii-decision-eu-us-data-transfers-in-question/.

[119] على سبيل المثال، نيوزيلندا لديها قرار كفاية من الاتحاد الأوروبي، وربما يؤدي قانون TOLA إلى التأثير على قرارات الكيانات النيوزيلاندية بهدف استغلال خدمات الضيافة، أو غيرها من الخدمات التي تقدمها الشركات الأسترالية التي ينطبق عليها هذا القانون. (انظر: "قرارات الكفاية " الاتحاد

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

كان تبادل البيانات الدولية أمراً مهماً لعمل الاقتصاد الرقمي العالمي، فإن توقف عمليات التبادل تلك قد يكون له أثر مدمر على التجارة الإلكترونية العالمية.

5.5 ازدياد تكاليف التشغيل بسبب قانون TOLA

قد تزداد التكاليف التي تتحملها الشركات بسبب قانون TOLA. أولاً، قد يكون هناك تكاليف مباشرة تتكبدها الشركة التي تتلقى طلباً أو إنذاراً بمقتضى هذا القانون. وهذه التكاليف تعتمد على إذا ما كان الإشعار اختيارياً/ تطوعياً (الطلبات التي تصدر بمقتضى قانون TOLA) أم إجبارياً (إنذارات بمقتضى قانون TOLA) وعلى المتطلبات الخاصة التي يشملها أي إنذار صادر بمقتضى هذا القانون.

ويضع قانون TOLA شروطاً تهدف إلى تقليل التكاليف المباشرة المرتبطة بإنذاراته من خلال (أ) تمكين المتلقي من تعويض تكاليف الاستجابة للإنذار، (ب) وتحديد مجال الطلبات التي تصدر بمقتضى القانون لتنطبق فقط على الطلبات التي لا تؤدي إلى حدوث أي "ثغرات أمنية". وبالنظر إلى صعوبة تقدير التكاليف الكاملة للاستجابة للطلبات، أو الإنذارات الصادرة بمقتضى القانون، التي تشمل آثاراً مباشرة وغير مباشرة، فمن المتوقع أن ينتاب مقدمي خدمات الاتصالات المحددة القلقُ بشأن الالتزام برد التكاليف الكاملة لتأثير قانون TOLA، أو حتى التكاليف المباشرة الناجمة عن الاستجابة للإنذار.

بالإضافة إلى ذلك، تجدر الإشارة إلى تاريخ الرقابة وكيف كانت أقل تأثيراً في تحديد حدود عمل الهيئات الحكومية للعمل بمقتضى السلطات الجديدة.[120] ونتيجةً لذلك، من الطبيعي أن يستمر قلق مقدمي خدمات الاتصالات المحددة وغيرها من الشركات المتأثرة بقانون TOLA من فعالية الرقابة في ضوء غياب الشفافية وعدم وضوح أجزاء التشريع والمشكلات الأخرى. وبعد تقدير التكاليف المباشرة الناتجة عن الاستجابة للإنذارات أو الطلبات الصادرة بمقتضى هذا القانون، قد تحتاج الشركة إلى قياس ذلك مقارنةً باحتمالية تلقي مثل هذا الطلب أو الإنذار. وكلما قلت احتمالية تلقي الشركة طلباً أو إنذاراً، قلّت التكلفة المباشرة المتوقعة التي قد تتكبدها الشركة نتيجةً لذلك.

الأوروبي https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

120 انظر: أدبيات الاقتصاد الموسع في الاختيار العام والاقتصادات التنظيمية بشأن الزحف الاقتصادي الذي يعود إلى "ثروات الأمم" لآدم سميث، وأيضاً أعمال جورج جيه ستيجلر "نظرية التنظيم الاقتصادي" ودورية Science Bell Journal of Economics and Management، عدد 2 رقم 1 (ربيع 1971) صفحات 3-21 وبيلتزمان سي (1976) "نحو نظرية أكثر عموماً للتنظيم" دورية Journal of Law and Economics، العدد 19، صفحات 211-48 . وانظر: أيضاً النظرية الاقتصادية للبيروقراطية، التي تتضمن الهيئات التنظيمية، ومنها رسالة تعظيم الموازنة، لويليام نيسكانن "البيروقراطية والاقتصادات العامة" شيلتنهتام، المملكة المتحدة البريطانية: إدارد إيلجر، 1994 الذي يقود الزحف الاقتصادي. وانظر أيضاً: هيلم، دايتر. (2) 169 ودال بو اي (2006) " الأسر التنظيمي: مراجعة" Oxford Review of Economic Policy مراجعة السياسة الاقتصادية، 22 (2) صفحات 25-203 . وبشأن إدراك الحكومة للمشكلة، انظر: تقرير مكتب رئاسة الوزراء – قوة عمل التنظيم الأفضل ومجموعة عمل الزحف التنظيمي-2004: "تجنب الزحف التنظيمي"، الذي يعرف الزحف التنظيمي بأنه عملية يمكن من خلالها صياغة أو فرض التنظيم بأسلوب غير شفاف، ولا يتماشى مع المبادئ الخمسة للتنظيم: التناسب، والمسؤولية، والتناسق، الشفافية، والاستهداف.

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

بالإضافة إلى ذلك، وعلى الرغم من أن الالتزام بالطلبات التي تصدر بمقتضى قانون TOLA لا تُعد إلزامية، فإن بعض الشركات ترى في هذه الطلبات غير الإجبارية مقدمة لإنذار إجباري. ولذلك فإن اعتبار الطلبات الصادرة بمقتضى هذا القانون غيرَ ذات تأثير من وجهة النظر الاقتصادية وجهةُ نظرٍ غير مؤكدة.

ثانياً، فإن الشركات التي ربما لم تتلقَّ مطلقاً أي إشعار بمقتضى قانون TOLA قد تواجه تهديداً لتشويه صورة الهوية الخاصة بها، أو تشويه علاقات العملاء، وهو ما قد يضطر الشركة إلى تحمل تكاليف إضافية. وربما دفعهم ذلك إلى تحسين الهوية من خلال الإعلان والتسويق المباشر لتعويض المخاطر المحتملة من تشويه صورة الهوية الخاصة بهم. وقد يتطلب الأمر أيضاً إنفاق موارد إضافية للتعامل مع مخاوف العملاء المتعلقة بتأثير قانون TOLA على أمن بياناتهم.

ثالثاً، قد ينتاب الشركاتِ مخاوفُ بشأن أمن الخدمات والمنتجات التي يقدمها مورِّدوها، أو أمن العمليات الداخلية للشركة داخل أستراليا التي تُهدَّد بسبب قانون TOLA. وقد تضطر الشركات إلى إعادة تقييم علاقات الموردين وفرص العمل مع جهات ثالثة (مثل خدمات الحوسبة لإدارة بيانات العملاء أو البيانات السرية للشركة) في ضوء القلق الزائد بشأن هشاشة البيانات بسبب الاستجابة السلوكية للشركاء من التجار والموردين لهذا القانون.

وقد يسفر ذلك عن تحويل بعض الشركات لعلاقاتها وتجارتها إلى خارج البلاد لتجنُّب قانون TOLA. وهذا التعديل على علاقات الموردين أو تحويل العمليات الداخلية للشركة من أستراليا إلى الخارج قد يسفر عن تكبُّد تكاليف ترجع مبلشرةً إلى هذا القانون، قد تؤدي أيضاً إلى انتشار تأثيرات غير مرغوب فيها في باقي قطاعات الأعمال الرقمية في أستراليا، الأمر الذي يزيد الآثار غير المبلشرة للقانون.

رابعاً، قد تحول الشركات من إستراتيجيات الأمن السيبراني الخاصة بهم نتيجة القيود المفروضة عليهم بسبب قانون TOLA. وقد ينعكس ذلك في هيئة تكاليف متزايدة مرتبطة بتأمين المعلومات InfoSec أو التأمين السيبراني CyberIns، وذلك لتعويض المخاطر السيبرانية المتزايدة والمرتبطة بهذا القانون. وإحدى الطرق التي تقيِّم بها الشركات المخاطر السيبرانية هي تقدير التهديد الذي قد يحدث نتيجة أنواع مختلفة من الهجوم. ومن أكثر التهديدات صعوبةً في التناول تلك التهديدات الداخلية أو الجرائم الإلكترونية التي يرتكبها موظفون غير جديرين بالثقة. فمِن أكثر المصادر المعروفة لانتهاك البيانات الموظفون الساخطون أو الفاسدون الذين تدفعهم الرغبة في الانتقام أو تحقيق المكاسب غير القانونية، وذلك بتجاهلهم لدفاعات الأمن

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

الداخلية لاستخراج البيانات.[121] ولا تتمكن أفضل جدران الحماية في العالم من أن توقف موظفاً ما من أن يحمِّل بيانات سرية معه، سواء على وحدة تخزين خارجية، أو على هيئة ملفات ورقية.

ويمكن اعتبار قانون TOLA عاملاً من عوامل زيادة التهديدات الداخلية، لأنه يزج بسلطة الدولة داخل الشركة، وهو ما قد يدفع موظفاً آخر لتجاهل بروتوكولات الأمن الخاصة بالشركة. ويزيد أمرَ هذا التهديد غيابُ الشفافية والقيود المفروضة على المعلومات التي يمكن لمتلقي انذار TOLA أن يشاركها مع طرف ثالث (مثل المستشار القانوني)، أو مع موظفين آخرين داخل الشركة.

ولتقييم التأثير المحتمل لقانون TOLA على تكاليف التشغيل ورأس المال الخاص بأمن المعلومات InfoSec وعلى التأمين السيبراني CyberIns للشركة، من المهم أن نعرف كيف تستخدم الشركة التشفير للبيانات المتحركة والثابتة، وما احتمالات تعديل إستراتيجيات أمن البيانات والتأمين السيبراني لمواجهة هذا القانون. بالإضافة إلى تقسيم تحديات أمن البيانات إلى تحديات مرتبطة بالبيانات المتحركة (مثل خدمات الاتصالات الإلكترونية، مثل الهواتف والبريد الإلكتروني وخدمات الدردشة وإرسال الرسائل والنفاذ عن بُعد للأطراف، ... إلخ) في مقابل البيانات الثابتة (مثل الملفات السرية للبيانات وكلمات الدخول، ... إلخ). ومن المهم أيضاً أن نعلم كيف تستخدم الشركة التشفير داخلياً في علاقتها مثلاً بشركات سلسلة الإمداد، مثل شركات الإنتاج والعملاء.

وفي كل من الحالات الست، هناك اعتبارات واحتمالات اقتصادية مختلفة ترتبط بكل حالة (ربما يتطلب الأمر مزيداً من الحالات لدراسة المنتجات والأسواق المختلفة ومختلف قطاعات العملاء).[122]

خامساً، وفي إطار رد الفعل للجهود القومية المتزايدة لحماية بيانات العملاء من الرقابة الأجنبية، ربما تضطر الشركات الرقمية إلى الاستثمار في مزيد من توطين البيانات. فعلى سبيل المثال، بعد توقُّف العمل بالاتفاق السابق الذي ينص على توفير ملاذ آمِن لاستبدال البيانات الدولية داخل دول الاتحاد الأوروبي بعد قرار Schrems I الصادر عام 2015 م، استثمرت شركة ميكروسوفت في حلول توطين البيانات في ألمانيا، وهو القرار الذي جرى التخلي عنه فيما بعدُ عام 2016 م بعد إقرار الاتفاق الجديد بين جهات الصناعة والخاص بمشاركة الملاذ الآمن.[123]

---

[121] على الرغم من عدم وجود إحصاءات موثوق بها بشأن نسبة البيانات التي يمكن اختراقها بسبب تهديدات داخلية، فمن المقبول داخل مجتمع الأمن أن الموظفين الذين فشلوا في اتباع إجراءات الأمن عن عمد أم لا يمثلون مصدراً أساسياً لاختراق البيانات، ولكن لما كان معظم حالات اختراق البيانات لا يُبلغ عنها، وكانت الإحصاءات الخاصة بالحالات التي أُبلغ عنها غير كاملة، فمن غير المعروف مقدار النسبة الداخلية. فوفقاً لأحد الاستبيانات فإن "66% من المنظمات ترى أن الهجمات الضارة أو حالات اختراق البيانات تكون داخلية أكثر منها خارجية". (انظر: https://techjury.net/blog/insider-threat-statistics/#gref، آب/ أغسطس 2020).

[122] الحالات الست عن (بيانات ثابتة/ بيانات متحركة مستخدمة) في مقابل (علاقات داخلية/ علاقات مع الموردين/ العملاء).

[123] انظر: "سحابة ميكروسوفت بألمانيا تستخدم نموذج وصي البيانات" eWeek 22 أيلول/ سبتمبر 2016، متاح على: https://www.eweek.com/cloud/microsoft-cloud-germany-opens-using-data-trustee-model في مقال من عام 2016

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

وبالتخلي عن هذا الحل المؤقت، سمحت ميكروسوفت برفع تكلفة الخدمة المقدمة للعملاء وخفض كفاءتها، نتيجةَ إقرار حل توطين البيانات. ويحدث ذلك عن طريق تقييد قدرة الشركات المتعددة الجنسيات على تحقيق اقتصاديات الحجم والمجال. وترتفع تكلفة تحديث البرمجية (وتشمل توزيع تصحيحات البرمجيات) بسبب التكاليف الخاصة بخلق استجابات متباينة لكل سوق،وكذلك لحساب التكاليف الإضافية المرتبطة بإدارة عملية التحديث الأكثر تعقيداً.

5.6 انخفاض فرص النمو المستقبلي نتيجة قانون TOLA

أخيراً، قد يتسبب قانون TOLA في إعادة تفكير الشركات في خطط الاستثمار الاستراتيجية الخاصة بتطوير وطرح منتجات وخواص جديدة. وقد يؤدي ذلك إلى تغيير الشركات لخطط الطرح الخاص بها، أو لخطط التسعير لمجموعة من المنتجات والخواص التي يجري تعديلها. وقد يؤدي ذلك إلى أن تقرر الشركات عدم توفير منتجات معينة في أستراليا لحماية نفسها من تأثير قانون TOLA، بالإضافة إلى احتمال خفض المبيعات المستقبلية للشركة وانخفاض النمو (أو فائض المنتج)، وذلك يحرم المستهلك من المزايا الخاصة بالاختيار الموسع، ومن ثَم يقلل الفائض المتاح للمستهلك.

وقد يعني الاستثمار الأقل في المنتجات الجديدة والأكثر أمناً استثماراً أقل في قدرة العمل، ومن ذلك الاستثمار في البحث والتطوير. وهذه الاستثمارات قد تُؤجل أو تُلغى كاملةً، أو قد تتحول إلى خارج أستراليا. وفي كل الأحوال يصاب الاقتصاد الأسترالي بخسارة مبلشرة وغير مبلشرة.

5.7 التأثيرات الطويلة المدى والعالمية

على الرغم من أن قانون TOLA قد أُقِر عام 2018 م، فما زال بعد عامين من إقراره هدفاً للتحديات التي تجعل من مستقبله على المدى الطويل أمراً غير مؤكد. فلو أن هذا القانون بالفعل يمثل تهديداً للاستخدام الموسع وأمن خدمات التشفير، ومن ثَم للأمن الرقمي، ثم للثقة في التجارة الرقمية، فإن الانتشار الموسع لأي تشريع مماثل لهذا القانون سوف يزيد التأثيرَ غير المرغوب فيه. وعلى صعيد آخر، لو نجحت التحديات المستمرة التي تواجه هذا القانون، وما

عندما أعلنت ميكروسوفت عن ترتيبات جديدة و-https://mspoweruser.com/microsoft-is-discontinuing-the-german-data-trustee-model/ من عام 2018 عندما أعلنت ميكروسوفت أنها ستوقف أعمال توطين البيانات. وعلى الرغم من أن ميكروسوفت لا تحدد ما يعنيه تكلفه إقرار هذا النموذج ثم التخلي عنه، فمن المقبول توقُّع أن تصل تكلفة هذا المشروع إلى ملايين الدولارات. وطبقاً لأحدث قرارات Schrems II الذي أطاح بقرار الملاذ الآمن الذي كان مطبقاً عدة سنوات بعد صدور قرار Schrems I أكدت ميكروسوفت مرة أخرى التزامَها بحماية سرية بيانات عملائها. (انظر: "خطوات جديدة لحماية البيانات"، مدونة ميكروسوفت، 19 تشرين الثاني/ نوفمبر 2019، متاح على: https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/. وانظر: "Schrems I حماية البيانات باكر ماكينزي – كانون الأول/ ديسمبر 2019- متاح على: https://www.bakermckenzie.com/en/-/media/files/insight/publications/2019/12/schrems-ibackgroundv6.pdf ولخلفية عن قرار Shrems I وأصل القرار انظر: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN. ولقرار Schrems II الصادر تموز/ يوليو 2020، انظر: 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, United Kingdom +44 7554 065 718

يثار حول التهديد الذي يمثله للأمن الرقمي في تقليل احتمالية استخدام الإمكانات التي يتيحها القانون، فإن الآثار غير المرغوب فيها المذكورة من قبلُ يمكن أن تكون مؤقتة، بل يمكن تجنُّبها.

وفي هذه المرحلة، فمن المستحيل التنبؤ بأيٍّ من الاحتمالات يمكن حدوثه.

5.8 الملخص

تتمثل الآثار الاقتصادية المباشرة وغير المباشرة لقانون TOLA فيما يسفر عنه هذا القانون من خفضٍ للثقة في الأمن السيبراني. فالتكاليف المباشرة المرتبطة بالاستجابة للطلبات والإنذارات الصادرة بمقتضى هذا القانون ربما هي أصغر مصادر التكاليف وأقلها أهمية، لأن عدد متلقي إنذارات هذا القانون وطلباته من المحتمل أن يظل عدداً قليلاً.

لكن الآثار غير المباشرة سوف تتضمن تأثير قانون TOLA على كل قطاعات الاقتصاد، مع استجابة المتلقين المباشرين (الذين يشملون مقدمي خدمات الاتصالات المحددة) والشركات والعملاء الذين يتعاملون معهم للمخاطر السيبرانية المتزايدة التي يطرحها هذا القانون. وهذه التكاليف الإجمالية من المتوقع أن تزيد مع الوقت مع انتشار الآثار غير المباشرة بين دوائر قطاع تكنولوجيا الاتصالات والمعلومات في أستراليا، لتمتد إلى باقي القطاعات في الاقتصاد الأسترالي وإلى الاقتصادات العالمية، ثم العودة مرة أخرى إلى دوائر الرأي التي تضم النظام الإيكولوجي الاقتصادي العالمي المتشابك.

وتشير كل من دراسة زيورخ (2015 م) [124] والتقرير السيبراني الأسترالي AustCyber (2020 م) [125] إلى أن الأضرار غير المباشرة المحتملة التي تنتج عن تهديد الثقة الرقمية يمكن قياسها بمليارات الدولارات. وعلى الرغم من أن هذا التقدير لا يشير إلى حجم التكاليف المجمعة لقانون TOLA، فإنه يكفي لنستخلص أن حدوث أضرار على المستوى القومي والدولي احتمالٌ كبير.

وهناك دليل فرضي وتجريبي إلى حد ما يشير إلى أن تأثير قانون TOLA قد يؤدي إلى وقوع آثار غير مباشرة كبيرة. وتشير أيضاً المؤشرات الكمية الثابتة إلى أن التأثيرات المحتملة غير المرغوب فيها (في صافي التكاليف) لهذا القانون قد تكون كبيرة بالفعل. ولكن لا يوجد دليل قطعي يحدد قيمة هذه الآثار وحجمها.

وقد أجرينا مسحاً لأنواع البحث المختلفة المتاحة، فلم نجد أي دراسات أو بيانات كافية يمكن من خلالها تحديد التقديرات التجريبية. ولتناول مثل هذا التحدي، وفي إطار هذا المشروع، أجرينا بحثاً جديداً مبدئياً يجمع آراء شركات التكنولوجيا الأجنبية الكبيرة المتعددة الجنسيات، وعدد كبير من الشركات الأسترالية المتنوعة النشاط، بشأن الآثار المحتملة لقانون TOLA على

[124] انظر: الهامش 92 السابق.
[125] انظر: الهامش 93 السابق.

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

أعمالهم، وهل يرون أن هذه التأثيرات المشار إليها من قبلُ قد حدثت بالفعل، وفي هذه الحالة فما تقدير هذه التأثيرات بالدولار.

وتضمن هذا البحث عنصرين: أولاً، لقاءات مطولة عبر تقنية الفيديو كونفرانس مع الشركات الرائدة لمقدمي خدمات الاتصالات المتعددي الجنسيات، التي ينطبق عليها قانون TOLA. ثانياً، استبيان بدون اسم لعدد أكبر من مقدمي خدمات الاتصالات الذين ينطبق عليهم هذا القانون والشركات التي تتأثر أيضاً بالقانون داخل أستراليا. ويعرض الفصل التالي نتائج هذا العمل. وتلخيصاً، فإن هذا البحث يدعم النتيجة الرامية إلى أن صافي التأثير الاقتصادي لهذا القانون تأثير سلبي، وأنه يهدد بإحداث أضرار جوهرية في المستقبل.

4. نتائج البحث التجريبي

في إطار ما نُجريه من تحليل للتأثير الاقتصادي لقانون TOLA، أجرينا (1) مقابلات سرية موسعة عن طريق الفيديو كونفرانس مع تِسعٍ من الشركات الكبيرة التي تدير أعمالها في أستراليا، والتي تأثر نشاطها مباشرة بهذا القانون (يمكن اعتبار هذا الشركات مقدمي خدمات اتصالات محددة ينطبق عليها تلقي إنذارات بموجب قانون TOLA، (2) استبياناً بدون ذكر أسماء للشركات العاملة في أستراليا، التي ربما تتأثر تأثراً مباشراً أو غير مباشر بهذا القانون.

وكما سنشرح فيما بعدُ في ملخص هذا القسم، فإن نتائج المقابلات والاستبيان بدون ذكر أسماء تدعم (دعماً محدوداً) وتتسق كلياً مع تقييم التأثير الاقتصادي لقانون TOLA. وقد شملت الملاحظات والنتائج ما يلي:

1- من المتوقع أن يكون لهذا القانون آثار سلبية على الأعمال وعلى القاعدة العريضة من عملاء هذه الأعمال (أي لا يقتصر الأمر على الشركات العاملة في قطاع الاتصالات وتكنولوجيا المعلومات).
2- معظم الأضرار المتوقعة ستكون غير مباشرة وترتبط بالتهديد الذي يفرضه هذا القانون، ويضر بتصور العملاء وشركاء الصناعة عن الثقة الرقمية.
3- استمرار حالة عدم الوضوح فيما يتعلق بالقانون وآثاره.
4- محدودية الدليل العملي المباشر عن التكاليف الاقتصادية (أو المزايا)، لكننا نرجع ذلك إلى (أ) الضبابية التي تكتنف الأنشطة الخاصة بقانون TOLA نتيجة شروط عدم الإفصاح، (ب) والوقت المحدود منذ إقراره، واستمرار الجدال القائم بشأن تحديد استخدام هيئات الاستخبارات وإنفاذ القانون LEIA للسلطة التي يخولها لهم قانون TOLA، (ج) وتوقع أن تكون التأثيرات في الأغلب غير مباشرة ومستقبلية.

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

5- الدليل المباشر المحدود الذي لاحظناه يدعم النتيجة الرامية إلى أن المزايا التي تعود على الشركات مزايا بسيطة، بينما التكاليف التي تتحمَّلها الشركات كبيرة جداً. [126]
6- لا تمثل البيانات العملية المتاحة عينة كافية يمكن الاعتماد عليها لتقدير التأثير الاقتصادي المجمع لقانون TOLA.

وشملتشركات تكنولوجيا المعلومات التسع التي وقع عليها الاختيار لإجراء المقابلات الموسعة ستاً من الشركات العاملة في مجال التكنولوجيا، التي تصل عوائدها الإجمالية إلى أكثر من تريليون دولار أمريكي. [127]

أما الشركات الثلاث الأخرى، فتضمشركة أسترالية تعمل ناقلةً لتكنولوجيا الاتصالات، وشركتين أستراليتين تعملان في مجال تقديم الخدمات الإلكترونية، وواحدة من هاتين الشركتينشركة تصدير أسترالية، والثانية مستثمر أجنبي ومورد للخدمات المبتكرة لأستراليا.

وقد صمَّمتشركة أبحاث إستراتيجية (Clarity Strategic Research- Sydney) وأطلقت الاستبيان بدون ذكر أسماء، وذلك بتوجيه من الشركاء الاستشاريين للقانون والاقتصاد LECA. [128]

وأُطلق الاستبيان في شهر كانون الأول/ ديسمبر 2020 م، وشارك فيه 79شركة، وقد وُجه الاستبيان لذوي الخبرة في مجال تكنولوجيا المعلومات، وذلك على الرغم من أن التأثير الاقتصادي المتوقع لقانون TOLA، كماشرحنا آنفاً، يشمل الاقتصاد كله، كذلك من المتوقع أن تكون معظم هذه التأثيرات غير مباشرة.

ويرجع استهداف ذوي الخبرة في مجال تكنولوجيا المعلومات إلى أن خبراء تكنولوجيا المعلومات هم أكثر علماً بقانون TOLA وبالسياسات التي تؤثر على تكنولوجيا التشفير. وبالنظر إلى قصر المدة والموارد المحدودة المتاحة للاستبيان، قدَّمت هيئات التجارة الأسترالية المساعدة في تحديد متلقي الاستبيان، إذ وافقت هذه الهيئات على المساعدة في الوصول إلى 16000 من خبراء تكنولوجيا المعلومات. ومن هذه الهيئات الشبكة الأسترالية لنمو الأمن السيبراني AustCyber [129]وجمعية صناعة المعلومات الأسترالية AIIA [130]وتحالف الاتصالات ومتخصصو تكنولوجيا المعلومات بأستراليا ITPA. [131] [132]

[126] ركزت المقابلة والاستبيان على التأثيرات التي مر بها بالفعل المشاركون في الاستبيان.
[127] لتوفير بعض من السياق، فإن العائد الإجمالي يُقدر بحوالي ثلاثة أرباع الناتج المحلي الإجمالي الأسترالي.
[128] انظر: https://claritystrategicresearch.com.au/
[129] انظر: https://www.austcyber.com/
[130] انظر: https://www.aiia.com.au/
[131] انظر: https://www.commsalliance.com.au/
[132] انظر: 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, United Kingdom +44 7554 065 718

واعتمد الاستبيان على الأسلوب نفسه للاستبيانين السابقين. فالاستبيان الأول أطلقته AustCyber عام 2018 م عشية إقرار قانون TOLA، بينما أطلق تحالف الاتصالات ومتخصصو تكنولوجيا المعلومات بأستراليا الاستبيان الثاني في 2019 م، أي بعد مرور عام من سريان هذا القانون. ونتائج الاستبيان المذكورة هنا تعطي تصوراً عن آراء قطاع الصناعة وتجاربه بعد عامين من إقرار هذا القانون. ومن أهم نتائج هذا التحليل هو التماثل المميز بين توقعات المشاركين من قطاع الصناعة بشأن تأثيرات القانون، وما سجلوه بالفعل من تجارب وتوقعات مستقبلية. وكما سنشرح لاحقاً، فإن أغلبية من أجابوا الاستبيان قد توقعوا بالفعل تأثيرات اقتصادية سلبية لهذا القانون قبل إقراره، وهذه التوقعات تحققت بالفعل، وهناك توقع لحدوث أضرار سلبية أخرى في المستقبل.

وقبل مناقشة النتائج الواردة من المقابلات والاستبيان، دعونا نلخِّص نتائج الاستبيانين السابقين.

1.1. الشبكة الأسترالية لنمو الأمن السيبراني AustCyber (2018 م)

قبيل إقرار قانون TOLA في 2018 م، شاركت الشبكةُ الأسترالية لنمو الأمن السيبراني AustCyber المركزَ الدولي للسياسة السيبرانية التابع لمعهد السياسة الإستراتيجية الأسترالي ASPI لإجراء استبيان على الإنترنت بشأن الصناعة الأسترالية. وقد بدأ الاستبيان في تشرين الثاني/ نوفمبر 2018 م، ونُشرت النتائج في كانون الأول/ ديسمبر 2018 م.[133] وقد أُرسل الاستبيان إلى 512 شركة من شركات تكنولوجيا المعلومات العاملة في أستراليا، وأجابت 63 شركة فقط الاستبيان. ومن إجمالي الشركات التي أجابت الاستبيان أعربت 76% منها عن قلقها إزاء مشروع القانون و"بعض من القضايا المثارة التي تعبر عن مخاوف حقيقية دارت حول بعض الملاحظات وغياب الوضوح" بشأن ما يمكن أن يفرضه قانون TOLA على الشركات.[134] فعلى سبيل المثال، توقعت 57% من التي أجابت الاستبيان أن يكون للقانون أثر سلبي على أعمالهم في أستراليا، ومن هذه الشركات، توقعت 69% أن يستمر هذا التأثير عامين مقبلين.[135] كذلك توقعت 65% من التي أجابت الاستبيان، وعرفت أنفسها بأنها مصدِّرة خدمات، أن يكون للقانون أثر سلبي على صادرات الشركات.[136]

[133] انظر: معهد السياسة الإستراتيجية الأسترالي (2018) " استبيان الملاحظات: وجهات نظر الصناعة بشأن المضامين الاقتصادية لقانون المساعدة والنفاذ 2018" موّل AustCyber الاستبيان ونفذه معهد السياسة الإستراتيجية الأسترالي، 22 كانون الأول/ ديسمبر 2018، متاح على: https://www.austcyber.com/resources/perceptions-survey

[134] معهد السياسة الإستراتيجية الأسترالي (2018)، الهامش 7 السابق، صفحة 3.

[135] معهد السياسة الإستراتيجية الأسترالي (2018)، الهامش 7 السابق، صفحة 8. ويتوقع 7% فقط حدوث تأثير إيجابي، بينما يتوقع 22% بعدم حدوث أي تأثير، و14% كانت غير متأكدة.

[136] معهد السياسة الإستراتيجية الأسترالي (2018)، الهامش 7 السابق، صفحة 7. وقد ذكرت 51% من التي أجابت الاستبيان أنها تعمل مصدِّرة، منها 4% توقعت أن يكون لقانون TOLA تأثير إيجابي، بينما توقع 17% ألَّا يكون للقانون أي تأثير، و13% منها غير متأكدة من التأثير على صادرات الشركة.

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

وأخيرا حدَّدت 76% من التي أجابت الاستبيان، وكانت لديها مخاوف تجاه قانون TOLA قبيل إقراره، المخاوف التالية: [137]

جدول 6.1: المخاوف التي رصدها استبيان AustCyber	النسبة المئوية
غياب الوضوح بشأن التعريفات	%81
احتمالية النزاع بين القوانين الأسترالية والدول الأجنبية	%73
وجهة نظر أن منتجشركتك أقل أمناً	%71
تكلفة الالتزام بالإنذارات	%52
تآكل قدرة الشركة	%50
التأثير على عوائد الشركة	%46
انخفاض قدرة الشركة على جذب مستثمرين	%46
الخسارة المحتملة للملكية الفكرية	%44
عدم القدرة على فرض عقوبات عندما تكون الشركة قائمة في دول أخرى، ولكنها تقدم خدماتها في أستراليا	%40
تدمير العلامة التجارية للشركة	%40
التأثير على سلسلة الإمداد	%38
انخفاض قدرة الشركة على جذب مشترين جدد	%33
انخفاض الشفافية فيسبب الاحباط	%33
خطورة خسارة العملاء	%31
مخاوف أخرى	%23

بالإضافة إلى ذلك، وعلى الرغم من أن مشروع القانون قد نص على أن الحكومة ستعوِّض الشركات عن التكاليف التي تتحملها في محاولة التزامها بالقانون، فإن 5% فقط من الشركات توقعت أن تُعوَّض تعويضاً كاملاً عن التكاليف التي تحملتها نتيجة الالتزام بقانون TOLA. [138]

1.2. استبيان InnovationAus

تولَّت InnovationAus مهمة الاستبيان الثاني عام 2019 م. وInnovationAus دورية مستقلة تركز على السياسة العامة الأسترالية وعلى قضايا الابتكار في الأعمال، وذلك بالتعاون مع

[137] معهد السياسة الإستراتيجية الأسترالي ASPI (2018)، الهامش 8 السابق، صفحة 23. حُسِبت النسب اعتماداً على إجابات 48 شركة من التي أشارت إلى وجود مخاوف من قانون TOLA.

[138] معهد السياسة الإستراتيجية الأسترالي، الهامش 7 السابق، صفحة 27.

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

StartupAus،[139] وهي مجموعة لا تسعى إلى الربح، وتدعم الأعمال الناشئة، وتساعد المجتمع الفني في أستراليا؛[140] وتساعد كذلك تحالف الاتصالات ومتخصصي تكنولوجيا المعلومات هناك. وقد نُشِرت النتائج في كانون الأول/ ديسمبر 2019 م بعد سريان قانون TOLA بحوالي عام.[141]

وقد أُجري استبيان InnovationAus في الفترة من 5 إلى 12 كانون الأول/ ديسمبر 2019 م، بالتزامن مع الاحتفال بمرور عام على موافقة البرلمان على قانون TOLA. وقد أجاب الاستبيان 70 عضواً من أعضاء تحالف الاتصالات ومتخصصي تكنولوجيا الاتصالات بأستراليا. فصرَّح 40% من هؤلاء بأن هذا القانون قد تسبب في فقدان فرص عمل لشركاتهم، وصرَّح 51% بأن القانون له تأثير سلبي على سمعة شركات التكنولوجيا الأسترالية في الأسواق العالمية.[142] بالإضافة إلى ذلك، وبعد إقرار قانون TOLA، فإن 57% ممن أجابوا الاستبيان رأوا أن مؤسساتهم غير قادرة على إجراء أي عمليات للتطوير داخل أستراليا.[143]

1.3. ملخص المقابلات النوعية عبر الفيديو كونفرانس

كما شرحنا من قبل، أجرينا مقابلات موسعة مع تسعة من مقدمي خدمات الاتصالات المحددة، الذين يديرون أنشطتهم في أستراليا، ولهم خبرة كبيرة في مواجهة قانون TOLA، وماذا يعني لهم هذا القانون في إطار نشاط أعمالهم في أستراليا وخارجها.

وفي كل الأحوال، جاءت ردود المشاركين في الاستبيان واضحة فيما يتعلق بشأن معارضة أي طلبات من الحكومة تؤدي إلى فتح "أبواب خلفية" في عمليات التأمين الخاصة بهم، إذ يرون أن الالتزام بتنفيذ هذه الطلبات يُضعِف التأمين الذين يسعون إلى توفيره، ويتعارض مع التزامهم أمام عملائهم لحماية الحقوق القانونية وسرية المعلومات التي تقع تحت سيطرتهم. ويشمل ذلك الطلبات التي تتطلب توفير القدرة على إزالة أو تطويق التشفير لأي منتج لديه هذه الخاصية أو يُروَّج على هذا الأساس.

كذلك جاءت جميع ردود من جرت مقابلاتُهم واضحةً بشأن التزامهم بالطلبات القانونية الحكومية الخاصة بالوصول إلى البيانات بمقتضى القوانين والقواعد الأسترالية الحالية. ويرى شخص واحد فقط ممن أجابوا الاستبيان أن قانون TOLA يدعم الوضع القانوني فيما يتعلق

---

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

[140] انظر: https://startupaus.org/.

[141] InnovAUS (2019) "نبض الصناعة -قوانين التشفير- نتائج الاستبيان" تصدر عن InnovAus وStartupAus، وتحالف الاتصالات ومتخصصي تكنولوجيا الاتصالات بأستراليا، في 18 كانون الأول/ ديسمبر 2019، ومتاحة على: https://www.innovationaus.com/wp-content/uploads/2019/12/Encryption_Law_Survey_Results.pdf.

[142] InnovAus (2019) هامش 141 السابق، صفحة 3. بالإضافة إلى أن 51% يرون أن التأثير على سمعة الشركة سلبي، فإن 44% يرون أنه كان سلبياً إلى حد ما، و3% لا يتوقعون أي تأثير (لا توجد إجابات تتوقع تأثيراً إيجابياً). من ناحية أخرى، 61% ممن أجابوا الاستبيان يرون أن العملاء الدوليين أو المحليين قد عبروا عن مخاوفهم تجاه قانون TOLA.

[143] InnovAus (2019) هامش 141 السابق، صفحة 4. فقد توقع 30% فقط ألَّا يكون هناك تأثير على خطط التطوير، و7% توقعوا أن قانون TOLA سيدعم خطط التطوير في أستراليا. ومن ناحية أخرى، فإن 51% ممن أجابوا الاستبيان صرحوا بأن هذا القانون سيقلل فرص التوظيف التي تتيحها عمليات للتطوير التي تجري في أستراليا.

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

بوصول الحكومة للبيانات. وهذه الشركة ترى أن الملاذ الآمن الذي يوفره هذا القانون استجابةً لطلبات الوصول القانوني هو أفضل من الوضع الذي كان قبل صدور القانون، وذلك لأن هذا القانون يوفر وضوحاً أكثر تجاه عملية الوصول وحماية المسؤولية، مقارنةً بوضع ما قبل القانون، الذي كان أقل تماسكاً، ومن ثَم أكثر تخبطاً على المستوى البيروقراطي، وذلك ما تسفر عنه تجربتهم حتى الآن. بالإضافة إلى ذلك، ترى هذه الشركة أن شروط تعويض الشركات عن التكاليف المباشرة التي تتحملها نتيجة قانون TOLA جيدة حتى الآن. وهذه الشركة الوحيدة الداعمة لهذا القانون لا ترى فيه أي تهديد نتيجة مطالبتهم بإزالة التشفير، أو الإفصاح عن أكوادسرية، أو أي تهديد للعلامة التجارية لشركتهم أو عملائها في أستراليا أو خارجها.

أما الشركات الثماني الأخرى، فقد كانت لهم آراء سلبية بشأن قانون TOLA، إذ رأت فيه تهديداً محتملاً للأمن ونمو الطلب على خدمات المعلومات التي تقدمها، وأنه قد يحمل الشركات تكاليف أعلى عندما تحاول التصدي لهذه المخاطر الأمنية المتزايدة. ويرجع هذا الرأي إلى الاتفاق على أن نطاق القانون وعدم كفاية شروط الرقابة والغموض في المتطلبات وغياب الشفافية كل ذلك يمثل تهديداً لأمن البيانات الرقمية الثابتة والمتحركة. وقد توافقت هذه التعليقات مع الكثير من المخاوف المثارة ضمن إطار العملية الاستشارية التي سبقت إقرار قانون TOLA وانعكست[144] في المراجعات التي تلت ذلك، ومنها المراجعة التي أجرتها اللجنة المستقلة للرقابة على تشريعات الأمن القومي INSLM، والتي نُشرت في تموز/ يوليو 2020 م.[145] وعلى الرغم من أن الحكومة الأسترالية قد سعت إلى تناول الكثير من هذه المخاوف، التي اعتبرتها "خرافات" ليس لها أساس من الصحة[146]؛ فإن المراجعة التي أجرتها اللجنة المستقلة للرقابة على تشريعات الأمن القومي أوصت بعدد من الإصلاحات لدعم الرقابة التي ينص عليها قانون TOLA، وإلى مزيد من التوضيح بشأن شروط القانون.

وعلى الرغم من التأكيدات المستمرة من الحكومة أنه لا يمكن إساءة استخدام قانون TOLA، وأن تطبيقه سيكون مقتصراً على حالات محدودة، مثل الحالات التي تتضمن محاكمة الجرائم الكبيرة كالإرهاب الدولي، ومواد استغلال الأطفال جنسياً، أو تجارة الأعضاء البشرية، فإن كثيراً ممن أجابوا الاستبيان لم يكونوا على يقين بذلك، لما شاهدوه من فشل في الرقابة التي طُبِّقت في سياقات أخرى في أستراليا وخارجها. وكان هناك قلق من أن الحاجة إلى توسيع سلطة الحكومة للوصول إلى البيانات السرية بطرق غامضة قد تتطلب مزيداً من الحذر المستمر (ومزيداً من

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

[145] انظر: "ثق ولكن تأكد: تقرير عن تعديل تشريع الاتصالات وغيره (المساعدة والتفاذ) قانون 2018 والأمور المرتبطة به"، اللجنة المستقلة للرقابة على تشريعات الأمن القومي، حزيران/ يونيو 2020، متاح على: https://www.inslm.gov.au/sites/default/files/2020-07/INSLM_Review_TOLA_related_matters.pdf.

[146] انظر: "المساعدة والنفاذ: أفكار مغلوطة وخرافات شائعة"، متاح على: 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, United Kingdom +44 7554 065 718

التكاليف التي يتحملها مقدمو خدمات الاتصالات المحددة) لحماية أعمالهم من أي استغلال تحاول الرقابة منعه.

وخلال التجهيز لإقرار قانون TOLA وخلال الفترة الأولى من إقراره، عبر العديد ممن أجابوا الاستبيان عن خوفهم من أن القانون قد يقودهم لوضع غير محتمل (وذلك بسبب الشروط المرتبكة والمقيدة بشأن المعلومات التي يحق لمتلقي إنذارات هذا القانون أن يشاركوها) على سبيل المثال، أعرب بعضهم عن قلقهم من أن الموظف الذي يتلقى إنذاراً بمقتضى قانون TOLA قد يكون غير قادر على مشاركة هذه المعلومات مع الإدارة العليا دون التعرض لعقوبات قانونية. وهذا السيناريو قد يعرض الموظفين والشركة لمسؤولية قانونية غير مقبولة.

وقد أدت مناقشات تالية مع الهيئات التنظيمية المسؤولة عن قانون TOLA إلى حسم هذا الخطر، إلا أن مجرد إثارة هذا القلق يشير إلى حجم الارتباك والغموض القانوني (ومن ثَم الخاص بالأعمال) الذي يثيره هذا القانون منذ اقتراحه حتى هذا اليوم. وأضف إلى ذلك أن الوضع يمكن أن يتغير مع تغيير القيادة والمسؤولين داخل الهيئات التنظيمية وتولي مسؤولين آخرين لهم وجهات نظر مختلفة، لأن هذا الحسم غير صريح في لغة القانون.

وأشار عدد كبير ممن أجابوا الاستبيان إلى أن إزالة أو تطويق التشفير لأحد المنتجات قد يكون غير ممكن الحدوث، إذا كان المستهدف جهة واحدة، إذ قد يُحدِث ذلك الإجراء ثغرة أمنية قد تمتد لتُحدِث أثراً سلبياً على أمن المنتج أو الخدمة للمستخدمين الآخرين. وينطبق ذلك على مقدمي خدمات الاتصالات المحددة الذين يقدمون ويعتمدون على خدمات قائمة على المصدر المفتوح، أو تعتمد على التشفير وحماية الأمن، إذ يصعب تحديد الإجراء ليُطبَّق على مستخدم واحد. وقد يعتمد بعض مقدمي خدمات الاتصالات المحددة على خدمات من هذا النوع، حتى وإن لم يكونوا هم مَن يقدمونها.

وعند مطالبة مقدم الخدمة بإزالة أمن المنتج بموجب قانون TOLA، فقد يشكل ذلك خطراً يلزم الشركة بسحب عملياتها ومبيعات منتجها/ خدمتها إلى خارج أستراليا. وقد علق بعض ممن أجابوا الاستبيان، وأوكوا هذا الخطر، أنهم سيعارضون الالتزام بأي من هذه الطلبات على قدر ما تسمح به إمكاناتهم القانونية، وسيواجهون هذا الطلب، ويصعِّدون هذه الجهود إلى أي مستوى قد يتطلبه الأمر.

وعلى الرغم من أن بعض سيناريوهات إساءة استغلال قانون TOLA قد يكون مبالغاً فيها، فإن مجرد إثارة هذا الأمر مثير للقلق، إذ عبر مقدمو خدمات الاتصالات المحددة عن قلقهم تجاه انخفاض تأمين المنتجات والخدمات التي يقدمونها بسبب هذا القانون، وأن هذا الانخفاض في التأمين قد يؤدي إلى تسريب للبيانات، وإلى انتهاك للتأمين ليس في أستراليا فقط، بل في أماكن أخرى. وقد تبنى جميع المشاركين في الاستبيان، عدا مشارك واحد، وجهة النظر التي ترى أن

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

قانون TOLA يمثل سياسة سيئة للتأمين، ورأوا أيضاً في هذه الإجراءات تهديداً للعلامة التجارية لشركاتهم، الأمر الذي يتطلب المراقبة الجيدة، وأخذ هذا التهديد المحتمل في الاعتبار عند وضع خططهم الإستراتيجية في المستقبل، لتطوير وتوفير خدمات أمن للبيع داخل أستراليا.

وذكر عدد من المشاركين أن قانون TOLA، وما يثيره من تغيير لوضع التدخل الحكومي وتنظيم منتجات التأمين، سوف يكون عاملاً يؤخذ في الاعتبار في خططهم المستقبلية عند صياغة خطط التطوير والمبيعات الخاصة بهم داخل أستراليا. فعلى سبيل المثال، قد يكون ذلك عاملاً في اختيار موردي الخدمات، مثل مراكز البيانات العاملة داخل أستراليا، التي ينطبق عليها هذا القانون. ومن ناحية أخرى، ولما كان متلقو إنذارات هذا القانون ممنوعين من مشاركة المعلومات الخاصة بتلك الإنذارات التي يتلقونها، فإن عملاءهم قد لا يعلمون أي مقدمي خدمات الاتصالات المحددة قد تلقى تلك الإنذارات، وماذا كانت استجاباتهم لذلك.

وكان أحد مَن جرت مقابلاتهم مقدم خدمات اتصالات محددة يعمل في أستراليا، وتشهد أعماله نمواًسريعاً، ويتطلع إلى التوسع في الأسواق الدولية، وهو يرى ذلك فرصةً جيدة تحقق له مليارات الدولارات. ولكن بعد إقرار قانون TOLA، أدى التأثير السلبي على العلامة التجارية لمنتجاته أن يتخلى عن خطط التوسع في مبيعات الصادرات، ومن ثَم، عن فرصة كبيرة لنموشركته. وأشار هذا المشارك إلى أن الشركة قد خسرت فرصاً للتعاون مع العملاء الحاليين، الذين قرروا نقل عملهم لمقدمي خدمات آخرين لا ينطبق عليهم هذا القانون.

وأشار بعض المشاركين إلى أن العملاء قد أعربوا عن قلقهم بشأن تأمين بياناتهم، وأن هذا القلق أصبح عاملاً يجب أن يؤخذ في الاعتبار عند وضع الخطط المستقبلية، إذ يجب عليهم ضمان الالتزام بحمايةسرية البيانات للعملاء.

وباستثناء الحالة الوحيدة المذكورة آنفاً، أقر معظم المشاركين أن التكاليف التي يتسبب فيها قانون TOLA لم تكن مبالغاً فيها، على الرغم من أن معظمهم قد عبروا عن شكّهم في ظروف التعويض للتكاليف المرتبطة بتنفيذ هذا القانون، وأن هذه التعويضات قد تعوضهم حقاً عن أي تأثيرات سلبية مرتبطة بالتكاليف. وتوقع المشاركون أن معظم التكاليف المرتبطة بهذا القانون ستكون تكاليف غير مباشرة (مثل تدمير العلامة التجارية للشركة، أو انخفاض الطلب على خدمات ومنتجات مقدمي الاتصالات المحددة DCPs الأسترالية)، أكثر منها تأثيرات مباشرة (مثل التزام الموظفين بتنفيذ طلب معين).

وأوضح معظم المشاركين في الاستبيان أنهم يتبعون إجراءات حماية إضافية في مواجهة قانون TOLA (وهو ما يزيد التكاليف التي يتحملونها)[147]، لكن معظمهم لم يشر إلى أن هذا القانون قد

[147] على سبيل المثال، ذكر الكثير من المشاركين أن حماية عمليات التشغيل تتضمن إضافة طبقة أخرى من المراجعة للاستثمار وخطط تطوير المنتجات من أجل مواجهة التأثير المحتمل لقانون TOLA.

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

تسبب بالفعل في تغيير تصميم عروض المنتجات الخاصة بهم، أو في تغيير قرارات تعيين الموظفين فيما يتعلق بتعيينهم داخل أستراليا أو خارجها. لكن هذه الإجراءات الإضافية تشير إلى أن هذه النوعية من القرارات قد تكون عاملاً من العوامل المؤثرة في اتخاذ القرارات فيما بعد. وقد أشار كثير من المشاركين في الاستبيان إلى أن غياب الدليل على وجود تكاليف مباشرة كبيرة لم يكن أمراً مفاجئاً في ضوء التطبيق المحدود لسلطة قانون TOLA منذ إقراره. وقد أرجعوا ذلك إلى أن الأمر يستغرق بعض الوقت للشعور بآثار هذه التشريعات، مع استمرار الجدال بشأن الدعاوى لإجراء تعديلات بشأن هذا القانون.

بالإضافة إلى ذلك، يرى البعض أن قانون TOLA كان خطوة غير جيدة، وأنه قد يعظّم التهديد العالمي الذي يمثله القانون بالفعل تجاه تأمين البيانات، وذلك إذا أصبح أكثر انتشاراً مع وجود تشريعات أخرى مماثلة.

وأخيراً، وفي ظل قرار تموز/ يوليو 2020 م (Shrems II)[148] في الاتحاد الأوروبي، الذي أطاح بحل حماية الخصوصية المعروف بالملاذ الآمن، والذي أُقِرَّ لحماية ترتيبات مشاركة البيانات الدولية نتيجة عدم الالتزام بقوانين حماية البيانات داخل الاتحاد الأوروبي، أشار عدد من المشاركين إلى أنهم قلقون من التهديد الذي قد يفرضه قانون TOLA على تدفقات البيانات الدولية من أستراليا وإليها. وأي تهديد مماثل، إذا حدث، قد يعرض الشركات لتحمُّل تكاليف كبيرة على عمليات التشغيل للبيانات العالمية وأسواق الاتصالات.

1.4. نتائج الاستبيان الخاص بالشركاء الاستشاريين للقانون والاقتصاد LECA

1.4.1. المشاركون في الاستبيان الإلكتروني

كما سبقت الإشارة إلى ذلك، شارك 79 مشاركاً في الاستبيان الذي أجرته شركة الشركاء الاستشاريين للقانون والاقتصاد LECA بمساعدة مركز Clarity Strategic Research. وكما في حال الاستبيانات السابقة، مثَّل المشاركون في الاستبيان شركاتٍ ذات أحجام مختلفة، وتعمل في أستراليا من مختلف قطاعات الاقتصاد (يقاس الحجم اعتماداً على الموظفين أو العوائد):

- 54% من الشركات مقرها أستراليا (68% أو 79/54)
- يتراوح حجم الشركات المشارِكة في الحجم بين شركات أقل من 10 موظفين (34% أو 79/27) وشركات تضم أكثر من 500 موظف (28% أو 79/22)
- صرحت نسبة كبيرة من المشاركين أن كل موظفي شركاتهم يعيشون في أستراليا (46% أو 79/36)، بينما صرحت النسبة الأقل بأن أقل من نصف عدد موظفي شركاتهم يعيشون في أستراليا، وهذه نسبة ما زالت تمثل نسبة ليست بالبسيطة (27% أو 79/21)

[148] انظر: "قرار Shrems II: دراسة نقل البيانات بين الاتحاد الأوروبي والولايات المتحدة الأمريكية"، 16 تموز/ يوليو 2020، متاح على: 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, United Kingdom +44 7554 065 718

- على صعيد العوائد الكلية للشركة، فإن 43% من الشركات (79/34)شركات صغيرة (أقل من خمسة ملايين دولار أسترالي)، بينما 13% من الشركات أو 79/10شركات كبيرة (أكبر من خمسة آلاف مليون دولار أسترالي).
- كما هو متوقع،صرح معظم المشاركين أنشركاتهم تعمل في مجال تكنولوجيا الاتصالات (54% أو 79/43)،وكثير منها له أنشطة عبر عدد من القطاعات في أعمال تكنولوجيا الاتصالات.
- من الشركات غير العاملة في مجال تكنولوجيا المعلومات (43% أو 79/34)، وصف المشاركونشركاتهم بأنهاشركات عاملة في مجال الخدمات (44% أو 34/15)، وفي الإدارة العامة والسلامة (18% أو 34/6)، أو في قطاعات أخرى (38% أو 34/13)، تمتد من التصنيع إلى التعليم. [149]

- تشير مناصب المشاركين إلى أن كثيراً منهم ، إن لم يكن جميعهم، يعملون في أعمال مرتبطة بتكنولوجيا المعلومات، وهو أمر متوقع لأنهم مَن تلقوا الاستبيان.

وتلخص الجداول التالية النتائج التي توصل إليها الاستبيان:

جدول 6.2: سؤال وإجابة QA1i: أين يقع مقر الشركة؟

	العدد	النسبة المئوية
أستراليا	54	%68
أي مكان آخر	23	%29
لا يوجد إجابة	2	%3
الإجمالي	79	%100

جدول 6.3: سؤال وإجابة QA3i: ما عدد الموظفين على مستوى العالم (تقريباً)؟

الموظفون على مستوى العالم(#)	العدد	النسبة المئوية
لا توجد إجابة	10	%13
10-0	27	%34
499-11	20	%25
+500	22	%28
الإجمالي	79	%100

[149] مشاركان اثنان (3% من ال79) لم يجيبا عن الأسئلة.

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

جدول 6.4: عدد الموظفين في أستراليا	العدد	النسبة المئوية
لا توجد إجابة	12	%15
10% أو أقل	16	%20
أكثر من 10% وأقل من 100%	15	%19
%100	36	%46
%0	4	%5
أقل من 50%	21	%27
الإجمالي	79	%100

جدول 6.5: هل تعمل الشركة في مجال تكنولوجيا الاتصالات؟		
القطاع	العدد	النسبة المئوية
لا توجد إجابة	2	%3
قطاع تكنولوجيا المعلومات	43	%54
خارج قطاع تكنولوجيا المعلومات	34	%43
الإجمالي	79	%100

جدول 6.5 B:موقع المقر ونشاط العمل				
		نشاط العمل		
موقع المقر	تكنولوجيا الاتصالات والمعلومات	خارج قطاع تكنولوجيا الاتصالات والمعلومات	لا إجابة	الإجمالي
أستراليا	31 (%39)	23 (%29)	0 (%0)	54 (%68)
خارج أستراليا	12 (%15)	10 (%13)	1 (%1)	23 (%29)
لا إجابة	0 (%0)	1 (%1)	1 (%1)	2 (%3)
الإجمالي	43 (%54)	34 (%43)	2 (%3)	79 (%100)

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

جدول 6.6: أنشطة عمل تكنولوجيا الاتصالات والمعلومات		
	الكود	العدد
عمليات وأجهزة وخدمات شبكات تكنولوجيا الاتصالات	1-3, 10,13	18
مقدم خدمة إنترنت، موقع للبحث على الإنترنت، خدمات إنترنت أخرى	4-5	7
خدمات تخزين الكترونية	6	6
مطور ومورد برامج	7-8	25
تصنيع ومبيعات أجهزة كمبيوتر	9-12, 13-14	17
أنشطة أخرى لتكنولوجيا الاتصالات (حددها)	97	13
لا أعرف، أفضل عدم الإفصاح	98-99	3
الإجمالي		89

جدول 6.7: أنشطة أعمالشركات خارج قطاع تكنولوجيا الاتصالات والمعلومات			
القطاع	الكود	العدد	النسبة المئوية
الخدمات	10,12,18	12	%46
الإدارة والسلامة العامة	14	6	%23
أخرى (التصنيع، التشييد، التعليم)	3,5,7,15	8	%31
الإجمالي		26	%100

1.4.2. أهمية خدمات تشفير للأعمال

صرح الأغلبية العظمى من المشاركين في الاستبيان أن خدمات التشفير وإمكاناته تُعد مهمة جداً للأعمال من عدة أبعاد - للاتصالات (البيانات المتحركة) والبيانات المخزنة (البيانات الثابتة)، وذلك للاستخدام الداخلي، وفي الاتفاقات التجارية معشركات مع المشركات والموردين القائمين على عملية الإنتاج ومع العملاء. وأشار 96% (أو 79/76) من المشاركين إلى أهمية خدمات

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

التشفير لفئة واحدة على الأقل من الاستخدام.[150] بالإضافة إلى ذلك فإن الجدول 6.8 يوضح أن 85% (أو 79/67) من المشاركين يرون أن خدمات التشفير وإمكاناته مهمة لمعظم أنواع الاستخدام، كلٌّ على حدة، ومن هؤلاء 53% (أو 79/42) يرون أن خدمات التشفير وإمكاناته مهمة للغاية.

بالإضافة إلى ذلك، أشار المشاركون في الاستبيان إلى أنهم قد حصلوا بالفعل على قدرات التشفير المطلوبة بعدة طرق مختلفة: أحياناً عن طريق تطوير تلك القدرات داخلياً، وأحياناً بالاعتماد على أطراف ثالثة لإنتاج منتجات وخدمات ذات هدف عام (أي أن قدرات التشفير يمكن أن تكون خاصية متضمنة داخل منتج أو خدمة لتكنولوجيا الاتصالات)، أو من خلال مقدمي خدمة متخصصين في التشفير. وتختلف طرق الحصول على التشفير باختلاف الاستخدام (أي البيانات المتحركة أو الثابتة، المستخدمة داخلياً، مع التجار والموردين أو مع العملاء). وقد استخدم عدد من المشاركين اتجاهات مختلفة في سياقات مختلفة، وأحياناً استخدموا اتجاهات متعددة في سياقات بعينها. وعلى الرغم من أن الاستبيان بغير ذكر أسماء لا يسمح بتعقب العلاقات الاعتمادية التي تربط بين الشركات (أي أن بعض المشاركين قد يكونون عملاء و/ أو مقدمي خدمات تشفير لمشاركين آخرين)، فمن الواضح أن استخدام قدرات التشفير وخدماته منتشر بين الأعمال المختلفة لتكنولوجيا الاتصالات، وأيضاً خارج نطاق تكنولوجيا الاتصالات.

وتشير هذه النتائج إلى انتشار العلاقات الاعتمادية بين خدمات التشفير في كل أنواع الأعمال في القطاع الاقتصادي، وإلى ردود الأفعال المتشابكة المحتملة التي يمكن أن تنتشر بين الشركات في أستراليا وعلى المستوى الدولي لو حدث أي تهديد لقدرات التشفير حتى لو لمجموعة من الشركات. ويزيد انتشارُ مثل هذه الآثار السلبية في الاقتصاد التأثيرَ السلبي المباشر. ولا تسمح هذه الإجابات القليلة التي جرى الحصول عليها من خلال الاستبيان، وغياب البيانات المتاحة عن التجارة في السلع والخدمات التي تعتمد على الإمكانات المشفرة، بتقييم الأساليب التي يمكن أن يكون لها آثار مباشرة وغير مباشرة على الاقتصاد.

جدول 6.8: ما أهمية خدمات التشفير وقدراته للأعمال؟

	مهمة جداً أو مهمة للغاية	ليست مهمة (على الإطلاق) أو غير مستخدمة	لا أعلم أو لا توجد إجابة	الإجمالي	النسبة المئوية (أ) ممن أجابوا أنها خدمات مهمة جداً

[150] يرى مشارك واحد فقط أنهم لا يستخدمون خدمات التشفير، بينما أشار مشارك آخر إلى أن خدمات التشفير مهمة للغاية لفئة واحدة من فئات الاستخدام، ومشارك واحد فضَّل ألَّا يُقِر بأهمية هذه الخدمات لكل أنواع الاستخدام، وذلك يمثل 4% (أو 76/3) من إجمالي المشاركين في الاستبيان.

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

	(أ)	(ب)	(ت)	(أ) + (ب) + (ت)	
الاتصالات الداخلية للشركة	%85	%14	%1	%100	%53
البيانات الداخلية للشركة	%92	%6	%1	%100	%73
الاتصالات (البيانات المتحركة) مع الموردين والشركات	%90	%9	%1	%100	%59
بيانات الشركة (البيانات الثابتة) التي يمتلكها الموردون والتجار	%91	%6	%3	%100	%70
الاتصالات (البيانات المتحركة) مع العملاء	%91	%8	%1	%100	%65
البيانات (البيانات الثابتة) للمنتجات والخدمات التي توفرها الشركة للعملاء	%78	%12	%1	%100	%71

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

1.4.3. الوعي بقانون TOLA ومعرفته والتعامل معه

من المشاركين البالغ عددهم 79، أشار 58 منهم إلى أنهم سمعوا عن قانون TOLA، وهؤلاء المشاركون يعملون في شركات مقرها في أستراليا (68%)، ويتركز نشاطهم الأساسي في مجال تكنولوجيا المعلومات (60% أو 58/35)، و40% (أو 58/23) من المشاركين أشاروا إلى أنهم على دراية جيدة بهذا القانون.

جدول 6.9 : وعي المشاركين في الاستبيان بقانون TOLA حسب موقع المقر			
	على علم	ليسوا على علم أو لا توجد إجابة	الإجمالي
أستراليا	42 (53%)	12 (15%)	54 (68%)
خارج أستراليا	16 (20%)	9 (11%)	25 (32%)
الإجمالي	58 (73%)	21 (27%)	79 (100%)

جدول 6.10 : معرفة المشاركين في الاستبيان بقانون TOLA حسب نوع نشاط العمل			
	على علم	ليسوا على علم أو لا توجد إجابة	الإجمالي
تكنولوجيا الاتصالات	35 (44%)	8 (10%)	43 (54%)
خارج قطاع تكنولوجيا الاتصالات	23 (29%)	13 (16%)	36 (46%)
الإجمالي	58 (73%)	21 (27%)	79 (100%)

جدول 6.11: درجة المعرفة بقانون TOLA		
معروف جداً/ جيد جداً	23	%40
غير معروف جيداً	29	%50
غير معروف	4	%7
لا توجد إجابة	2	%3
الإجمالي	58	%100

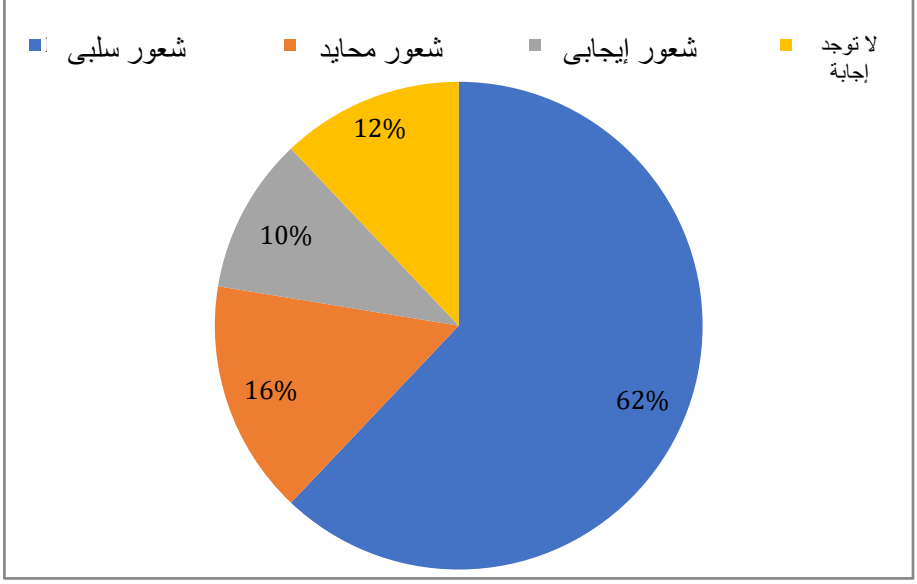
Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

1.4.4. تعامل المشاركين في الاستبيان مع قانون TOLA

من بين المشاركين الذين أجابوا بأنهم يعرفون قانون TOLA فإن نسبة كبيرة منهم (63% أو 58/36) لهم مواقف سلبية تجاه التغييرات التي يحدثها قانون تكنولوجيا الاتصالات لعام 1997 م. ويشعر 10% فقط (58/6) بالإيجابية. ويلخص الرسم البياني الآتي الوعي ومعرفة القانون وتعامل المشاركين البالغ عددهم 58 معه.

قانون 6.12: مشاعر المشاركين تجاه قانون TOLA	
إيجابي جداً	
إيجابي إلى حد ما	%10
محايد	%16
سلبي إلى حد ما	%26
سلبي جداً	%36
لا توجد إجابة	%12
الإجمالي	%100

الشكل 6.1
من الـ 58 حالة الذين على دراية بقانون TOLA



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

وعند سؤال المشاركين عن رأيهم في تأثير قانون TOLA على مختلف قضايا السياسة، رأى معظم المشاركين ممن أجابوا الاستبيان أن هذا القانون له أثر سلبي على العلاقات الخارجية لأستراليا وعلى أمن البيانات الرقمية ونزاهتها، بل على الاقتصاد الأسترالي نفسه. وينتاب المشاركين في الاستبيان مشاعرُ مختلفة تجاه تأثير القانون على الأمن القومي الأسترالي، لكن أكثر الآثار الإيجابية أهمية التي ذُكرت (أقل من الأغلبية كثيراً)، فتتمثل في قدرة هذا القانون على فرض القانون الجنائي في أستراليا (انظر: الجدول رقم 6.13)

جدول 16.3: توقعات المشاركين بشأن تأثير قانون TOLA على مختلف القضايا

	سلبي	لا يوجد تأثير	إيجابي	لا توجد إجابة	الإجمالي
الأمن القومي لأستراليا	%33	%22	%24	%21	%100
العلاقات الخارجية الأسترالية	%53	%7	%9	%31	%100
المصلحة الاقتصادية القومية لأستراليا	%52	%10	%16	%22	%100
أمن ونزاهة المعلومات التي تُشغَّل أو تُخزَّن، أو التواصل بها من خلال الوسائل الإلكترونية أو ما شابهها	%59	%12	%10	%19	%100
فرض القانون الجنائي في أستراليا	%12	%29	%34	%24	%100

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

فرض القانون الجنائي في دول أخرى	%10	%50	%7	%33	%100

1.4.5. تأثير قانون TOLA على أعمال المشاركين في الاستبيان

على أعمالهم بشتى الطرق، أجاب TOLAعند سؤال المشاركين في الاستبيان عن تأثير قانون)، وأجاب متوسط 6.14Aمنهم أن القانون قد أثر على أعمالهم بطريقة أو بأخرى (جدول 41%
18% من المشاركين الذين على علم بالقانون (58 من 79) أنه قد أثَّر على أعمالهم في كل أنواعه.

جدول 6.14A: الشركات التي صرحت بوجود تأثيرات على مختلف أنواع العمل	
لا يوجد تأثير	%59
تأثير في نوع واحد من الأعمال	%5
نوعان أو ثلاثة من التأثير	%36

جدول 6.14 B: هل كان لقانون TOLA تأثير على الأعمال					
	نعم له تأثير	لا يوجد تأثير	لا أعلم	لا توجد إجابة	الإجمالي
المبيعات	%16	%47	%31	%7	%100
سمعة العمل	%14	%45	%36	%5	%100
علاقات التجار	%16	%52	%28	%5	%100
علاقات العملاء	%16	%48	%31	%5	%100
تطوير المنتج، قرارات التسويق	%31	%43	%22	%3	%100
تكاليف التشغيل والأصول	%21	%45	%33	%2	%100

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

مجالات أخرى للأعمال	%21	%40	%36	%3	%100
المتوسط	%19	%46	%31	%4	

وعند توجيه سؤال عن طبيعة التأثيرات حتى تاريخه، وإن كانت إيجابية أو سلبية، وتوقعات المشاركين بشأن التأثيرات في المستقبل على عدد من أمور الأعمال، أشار المشاركون الذين لمسوا تأثيراً بالفعل إلى وجود عدد من التأثيرات (انظر: جداول 6.15A و6.15B و6.15C). وعلى الرغم من أن معظم الشركات لم تصرح بمواجهتها لأي تأثير (جدول 6.14)، فإن الشركات التي تعمل في نوع واحد من الأعمالصرحت بمواجهة تأثيرات سلبية أكثر كثيراً من التأثيرات الإيجابية. بالإضافة إلى ذلك، فمن المتوقع أن تستمر الآثار السلبية في المستقبل لتغطي 15 مجالاً من مجالات التأثير. وبالنسبة لمجالات التأثير (11 من 15 من مجالات التأثير أو 73%) فإن هناك مزيداً من الشركات التي تتوقع حدوث آثار سلبية في المستقبل مقارنةً بتلك الآثار التي واجهتها الشركات حتى تاريخه (جدول 6.15C)- لتزيد من 18% إلى 20%. ومن ثَم، فإن توقعات المشاركين في الاستبيان تتوافق مع الرؤية الرامية إلى أن التأثيرات الاقتصادية سوف تستمر، أو حتى ستكون أسوأ في المستقبل. وأخيراً فإن 36% (أو 58/21) من الشركات قد واجهت تأثيرات سلبية على أعمالهم في واحد أو أكثر من المجالات حتى تاريخه، وتتوقع آثاراً مستقبلية (جدول 6.15D)

جدول 6.15A: الشركات التي واجهت تأثير حتى تاريخه (منذ 2018 م)

نسبة الشركات التي واجهت تأثيرات	سلبية	لا يوجد تأثير	إيجابية	لا يوجد إجابة	الإجمالي
إجمالي العائد على المستوى العالمي	%10	%12	%3	%74	%100
العائد من الخدمات المشفرة على المستوى العالمي	%9	%16	%2	%74	%100
تكاليف التشغيل العالمية لنشاط العمل، ومنها تكاليف الالتزام والتعويض	%16	%14	%2	%69	%100

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

الاستثمار العالمي في الخدمات المشفرة	%21	%9	%3	%67	%100
المستوى العالمي من الاستثمار والتمويل	%17	%9	%3	%71	%100
الإنفاق العالمي على إستراتيجية الابتكار وعلاقتها بخدمات التشفير	%21	%7	%5	%67	%100
الاستثمار العالمي في تطوير المنتجات الجديدة	%22	%7	%2	%69	%100
الإنفاق على البحث والتطوير على المستوى العالمي	%19	%9	%3	%69	%100
القيمة العالمية للعلامة التجارية أو السمعة	%19	%10	%3	%67	%100
القيمة العالمية للملكية الفكرية (براءات الاختراع وحقوق النشر، ... إلخ)	%14	%14	%2	%71	%100
القدرة العالمية على جذب طاقم العمل الجيد للعمل	%12	%17	%2	%69	%100
القدرة العالمية على شراء المنتجات والخدمات المشفرة التي يحتاجها نشاط عملك	%10	%17	%3	%69	%100
سرية الخدمات المشفرة أو تأمينها أو خصوصيتها، على المستوى العالمي	%28	%9	%2	%62	%100

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

مخاطرة نشاط العمل على المستوى العالمي	%36	%2	%2	%60	%100
مستويات التوظيف في الخدمات المشفرة على المستوى العالمي	%14	%9	%3	%74	%100

جدول 6.15B: الشركات التي تتوقع أن تواجه تأثيراً في المستقبل					
نسبة الشركات التي واجهت تأثيرات	سلبية	لا يوجد تأثير	إيجابية	لا يوجد إجابة	الإجمالي
إجمالي العائد على المستوى العالمي	%14	%7	%7	%72	%100
العائد من الخدمات المشفرة على المستوى العالمي	%14	%9	%2	%76	%100
تكاليف التشغيل العالمية لنشاط العمل، ومنها تكاليف الالتزام والتعويض	%21	%10	%2	%67	%100
الاستثمار العالمي في الخدمات المشفرة	%28	%9	%0	%64	%100
المستوى العالمي من الاستثمار والتمويل	%19	%9	%3	%69	%100
الإنفاق العالمي على استراتيجية الابتكار وعلاقتها بخدمات التشفير	%24	%9	%0	%67	%100
الاستثمار العالمي في تطوير المنتجات الجديدة	%21	%7	%3	%69	%100
الإنفاق على البحث والتطوير على المستوى العالمي	%19	%12	%2	%67	%100

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

القيمة العالمية للعلامة التجارية أو السمعة	%19	%9	%5	%67	%100
القيمة العالمية للملكية الفكرية (براءات الاختراع وحقوق النشر، ... إلخ)	%16	%14	%0	%71	%100
القدرة العالمية على جذب طاقم العمل الجيد للعمل	%14	%16	%5	%66	%100
القدرة العالمية على شراء المنتجات والخدمات المشفرة التي يحتاجها نشاط عملك	%19	%12	%2	%67	%100
سرية الخدمات المشفرة أو تأمينها أو خصوصيتها، على المستوى العالمي	%29	%5	%3	%62	%100
مخاطرة نشاط العمل على المستوى العالمي	%33	%2	%2	%64	%100
مستويات التوظيف في الخدمات المشفرة على المستوى العالمي	%16	%7	%3	%74	%100

جدول 6.15C: الشركات التي واجهت أو تتوقع أن تواجه تأثيرات سلبية مستقبلية لقانون TOLA على نشاط أعمالهم

نسبة الشركات التي واجهت تأثيرات	حتى تاريخه	في المستقبل
إجمالي العائد على المستوى العالمي	%10	%14

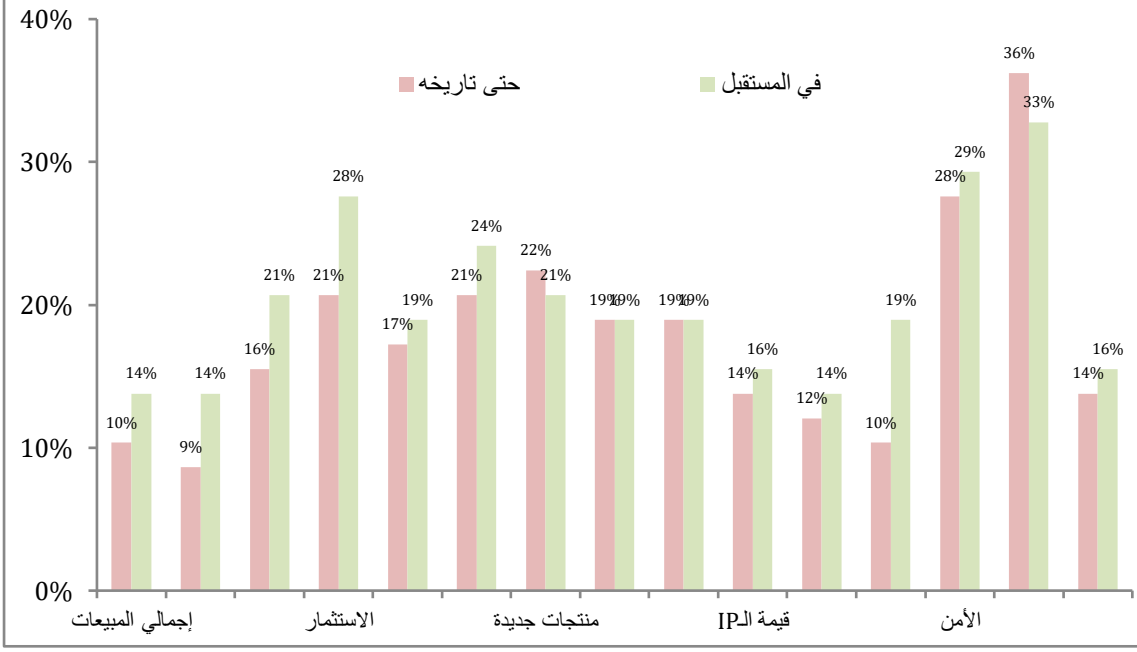
Level 12, Chifley Tower, 2 Chifley Square, Sydney, NSW 2000, Australia +612 8236 6060
16 Upper Woburn Place, London WC1H 0AF, United Kingdom +44 7554 065 718

العائد من الخدمات المشفرة على المستوى العالمي	%9	%14
تكاليف التشغيل العالمية لنشاط العمل، ومنها تكاليف الالتزام والتعويض	%16	%21
الاستثمار العالمي في الخدمات المشفرة	%21	%28
المستوى العالمي للاستثمار والتمويل	%17	%19
الإنفاق العالمي على إستراتيجية الابتكار وعلاقتها بخدمات التشفير	%21	%24
الاستثمار العالمي في تطوير المنتجات الجديدة	%22	%21
الإنفاق على البحث والتطوير على المستوى العالمي	%19	%19
القيمة العالمية للعلامة التجارية أو السمعة	%19	%19
القيمة العالمية للملكية الفكرية (براءات الاختراع، وحقوق النشر، ... إلخ)	%14	%16
القدرة العالمية على جذب طاقم العمل الجيد للعمل	%12	%14
القدرة العالمية على شراء المنتجات والخدمات المشفرة التي يحتاجها نشاط عملك	%10	%19
سرية الخدمات المشفرة أو تأمينها أو خصوصيتها، على المستوى العالمي	%28	%29
مخاطرة نشاط العمل على المستوى العالمي	%36	%33

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

مستويات التوظيف في الخدمات المشفرة على المستوى العالمي	%14	%16
متوسط الصفوف	%18	%20

الشكل 6.2
التأثير السلبي في الماضي والمستقبل
% الشركات الأسترالية والأجنبية



جدول 6.15D: عدد التأثيرات السلبية الحالية والمتوقعة التي واجهتها الأعمال حسب نوع العمل

التأثير السلبي (على المستوى العالمي وفي أستراليا) إجمالي الحالات التي على دراية بقانون TOLA= 58	عدد الحالات حتى تاريخه	عدد الحالات في المستقبل
0 (ومن ذلك: لا توجد إجابة) في كل الأنواع	37 (%64)	37 (%64)
نوع من 15	0 (%0)	0 (%3)

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

نوعان من 15	2 (%3)	0 (%0)
ثلاثة أنواع من 15	2 (%3)	2 (%2)
أربعة أنواع أو أكثر من 15	17 (%29)	18(%31)
الإجمالي	58 (%100)	58 (%100)
التأثير السلبي في نوع على الأقل من 15	21 (%36)	21 (%36)

1.5. نتائج البحث التجريبي

إن المخاطر الاقتصادية المفترضة، التي نذكرها في الفصل الخامس، أشارت إليها أيضاًشركات الاتصالات وتكنولوجيا المعلومات التي أجرينا مقابلات معها، كذلك ذُكِرت أيضاً في إجابات الاستبيانات. وكان هناك اتفاق لما يفرضه قانون TOLA من تهديد اقتصادي على فرص العمل الخاصة بشركات الاتصالات وتكنولوجيا المعلومات، وعلى الاقتصاد الأسترالي والعالمي.

وأشار الدليل المتاح أيضاً إلى غياب الدليل التجريبي حتى الآن على وجود أي تكاليف اقتصادية كبيرة (وحتى أي مزايا) يمكن أن تعود مباشرة إلى قانون TOLA. لكن غياب الدليل التجريبي لا يُعد مؤشراً على عدم وجود دليل من الأساس. وعلى الرغم من أن الأمر يستحق البحث عن دليل عن التكاليف التي تحمَّلتها الشركات منذ عام 2018 م، لكن ليس من المستغرب أنه لم يُعثَر على مثل هذا الدليل في ضوء النشاط المحدود للغاية المرتبط بهذا القانون، وفي ظل التحديات المستمرة والجدال الذي يجعل من مستقبل قانون TOLA أمراً غير واضح. بالإضافة إلى ذلك، فإن قواعد عدم الإفصاح والسرية التي تحيط بهذا القانون تمثل عائقاً كبيراً في هذا الإطار. وعلى الرغم من ذلك، فإن الأدلة المحدودة المتاحة لها دلالة. فالمشارك الوحيد الذى رأى في تأثير القانون أمراً جيداً يعتقد أن التأثير الوحيد في ترشيد التشريع القائم على الوصول الحكومي القانوني للبيانات الرقمية يتماشى مع وجهة النظر التي ترى أن المنافع المباشرة لقانون TOLA بسيطة. وبالعكس، فإن المشارك الوحيد، الذى كان قادراً على تحديد الضرر الاقتصادي الذي يعاني منه عمله نتيجة هذا القانون، يستطيع أن يوصل هذا الضرر إلى مليار دولار من الدخل المفقود، وهذا الرأي يتماشى مع توقُّع أن يكون الضرر الاقتصادي المباشر للقانون كبيراً.

بالإضافة إلى ذلك، فإن حجم الاستبيان الذي بلا أسماء وتحديات الاعتماد على تلك البيانات تقيِّد من القدرة على تحديد حجم الآثار الاقتصادية. لكن النتائج تتماشى مع ملاحظات الاستبيانات السابقة، التي توضح أن الشكوك والمخاوف المثارة قبل إقرار قانون TOLA مازالت

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

مستمرة حتى الآن، وإذا تحققت هذه المخاوف بالفعل، فإن التأثيرات الاقتصادية السلبية تكون كبيرة.

وتوضح إجابات الاستبيان حقيقة أن التأثيرات السلبية موجودة في شركات الاتصالات وتكنولوجيا المعلومات، وأيضاً في الشركات الأخرى، وأن شركات كثيرة ما زالت لا تستوعب التهديد الذي يفرضه قانون TOLA على نشاط أعمالهم.

5. ملاحق المصطلحات والاختصارات والتعريفات

1.6. المصطلحات والاختصارات والتعريفات

- قانون ASIO: منظمة الأمن والاستخبارات الأسترالية، قانون 1979 م.
- ASIO: منظمة الأمن والاستخبارات الأسترالية التي انضمت إلى قائمة الهيئات الحكومية الأسترالية التي يمكن أن تصدر طلبات و/ أو إنذارات بموجب قانون TOLA.
- Cth: تعني الكومنولث، وتستخدم للتفرقة بين التشريع الذي يصدره الكومنولث والإصدار الخاص بالدولة.
- DCP: مقدم خدمات الاتصالات المحددة، وهي فئة محددة بموجب قانون TOLA، تضم الكيانات التي ينطبق عليها هذا القانون. انظر: قائمة أنواع مقدمي خدمات الاتصالات المحددة في القسم 317C من قانون TOLA.
- INSLM: اللجنة المستقلة للرقابة على تشريعات الأمن القومي (الرابط)، التي أصدرت تقرير مراجعة قانون TOLA في 20 تموز/ يوليو 2020 م (الرابط).
- PJCIS: اللجنة البرلمانية المشتركة المعنية بشؤون الأمن والاستخبارات أجرت استفسارات عن TOLA قبل إقراره، وروجع القانون أكثر من مرة منذ ذلك الوقت.
- TOLA: قانون تشريع تكنولوجيا الاتصالات وغيره (المساعدة والنفاذ) قانون 2018 م، الذي يُعرَف أيضاً بقانون التشفير أو قانون المساعدة والنفاذ (الرابط). وراجَع هذا القانون اللجنةُ المستقلة للرقابة على تشريعات الأمن القومي INSLM. ويتكون القانون من خمسة جداول، وجدول 1 (يتعلق بإزالة وتطويق التشفير أو الوصول الاستثنائي) هو أساس العمل.
- TAR: طلب المساعدة الفنية، وTAN إنذار المساعدة الفنية، وTCN إنذار بناء القدرة الفنية، وهو ثلاثة أنواع من الإشعارات التي تصدر بموجب قانون TOLA؛ إما شفاهةً أو كتابةً (317H).

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

- TAR = طلب المساعدة الفنية الذي يُطلب بمقتضاه من مقدم خدمات الاتصالات المحددة أن يقوم بإتخاذ إجراءات غير إلزامية 317L
- TAN = إنذار المساعدة الفنية يوجه مقدم خدمات الاتصالات المحددة لتقديم المساعدة الفنية 317M.

· TCN = إنذار بناء القدرة الفنية يوجه مقدم خدمات الاتصالات المحددة لاتخاذ إجراءات محددة منها بناء القدرة 317T.

- TIA: قانون تكنولوجيا الاتصالات (النفاذ والتنصت) 1979 م.
- TA: قانون الاتصالات 1997 م.
- SD ACT: قانون أجهزة المراقبة 2004 م (SD ACT).
- MACMA: قانون المساعدة المتبادلة في الأمور الجنائية 1987 م.
- ASIO Act: قانون منظمة الأمن والاستخبارات الأسترالية 1979 م.

1.7. تعريفات من قانون TOLA

تعريفات 317B

الحماية الإلكترونية تشمل:

أ) التوثيق؛
ب) والتشفير.

التكنولوجيا المستهدفة:

أ- لأغراض هذا التقرير، خدمة النقل المعين، عندما يستخدم الخدمة أو يُحتمل أن يستخدمها (سواء بشكل مباشر أو غير مباشر) شخصٌ معين، هي التكنولوجيا المستهدفة التي ترتبط بذلك الشخص؛
ب- ولأغراض هذا التقرير، الخدمة الإلكترونية المعينة، عندما يستخدم الخدمة أو يحتمَل أن يستخدمها (بشكل مباشر أو غير مباشر) شخصٌ معين، هي التكنولوجيا المستهدفة التي ترتبط بهذا الشخص؛
ج- ولأغراض هذا التقرير، البرمجية التي تُركَّب أو التي ستُركَّب على:

1. كمبيوتر معين؛
2. وجهاز معين

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

يستخدمها أو يمكن أن يستخدمها (بشكل مباشر أو غير مباشر) شخصٌ معين، هي التكنولوجيا المستهدفة التي ترتبط بهذا الشخص،

د- ولأغراض هذا التقرير، تحديث البرمجية التي تُرَكَّب في:

1. كمبيوتر معين،
2. جهاز معين

يستخدمه أو يمكن أن يستخدمه (بشكل مباشر أو غير مباشر) شخصٌ معين، هي التكنولوجيا المستهدفة المرتبطة بهذا الشخص،

هـ- ولأغراض هذا التقرير، فإن جهازاً من أجهزة العميل، يستخدمه أو يحتمل أن يستخدمه (بشكل مباشر أو غير مباشر) شخصٌ معين، هى التكنولوجيا المستهدفة المرتبطة بهذا الشخص،

و- ولأغراض هذا التقرير، فإن جهاز تشغيل البيانات، الذي يستخدمه أو يحتمل أن يستخدمه (بشكل مباشر أو غير مباشر) شخصٌ معين، هى التكنولوجيا المستهدفة المرتبطة بهذا الشخص.

ولأغراض الفقرات (أ) و(ب) و(ج) و(د) و(هـ) و(و) من غير المهم تحديد الشخص بعينه.

مقدمو خدمات الاتصالات المحددة

مقدمو خدمات الاتصالات المحددة 317C

لأغراض هذا التقرير، يحدد الجدول التالي ما يلي:

(أ) مقدمي خدمات الاتصالات المحددة،
(ب) والأنشطة المسموح بها لمقدم خدمات الاتصالات المحددة.

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

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

مقدم خدمات الاتصالات المحددة والأنشطة المسموح بها		
الصنف	يكون الشخص مقدم خدمات اتصالات محددة إذا كان ...	الأنشطة المسموح بها للشخص هي...
1	ناقل أو مقدم خدمة نقل	(أ) العملية التي يجريها شخص تابع لشبكات تكنولوجيا الاتصالات أو للمرافق في أستراليا؛ (ب) تزويد الشخص بخدمات النقل المدرجة في القائمة.
2	وسيط خدمة نقل يرتب للإدراج بقائمة خدمات النقل بوصفه مقدم خدمة نقل	(أ) الترتيب الذي يؤديه للإدراج بقائمة من خدمات النقل من قبل مقدم خدمة النقل، (ب) أو العملية التي يجريها شخص تابع لشبكات تكنولوجيا الاتصالات أو للمرافق في أستراليا، (ت) أو الإمداد بخدمات نقل أدرجها مقدم خدمة النقل.
3	يقدم خدمة تسهيل الإمداد بخدمات نقل مدرجة، أو أن تكون خدمة إضافية أو طارئة	تقديم خدمة تسهيل الإمداد بخدمات نقل مدرجة، أو أن تكون خدمة إضافية أو طارئة
4	يقدم خدمة إلكترونية لديها مستخدم نهائي أو أكثر في أستراليا	تقديم خدمة إلكترونية، ويكون لهذه الخدمة مستخدم نهائي أو أكثر في أستراليا
5	يقدم خدمة إلكترونية تعمل على تسهيل تقديم الخدمة الإلكترونية التي لديها مستخدم نهائي أو أكثر في أستراليا، أو تكون مكملة أو طارئة على هذه الخدمة	تقديم خدمة، تعمل هذه الخدمة على تسهيل تقديم خدمة إلكترونية لديها مستخدم نهائي أو أكثر في أستراليا، أو تكون مكملة أو طارئة على هذه الخدمة
6	يطوِّر أو يورِّد أو يحدِّث برمجية مستخدمة، أو يمكن استخدامها وتكون مرتبطة بالتالي: (أ) خدمة نقل مسجلة، (ب) أو خدمة إلكترونية لديها مستخدم نهائي أو أكثر في أستراليا	(أ) تطوير برمجية، (ب) توريد البرمجية، (ت) تحديث البرمجية.

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

7	يصنِّع أو يورِّد أو يركِّب أو يتولى صيانة أو تشغيل مرفق	(أ) تصنيع مرفق للاستخدام، أو لاحتمالية الاستخدام في أستراليا، (ب) أو توريد مرفق للاستخدام، أو لاحتمالية الاستخدام في أستراليا، (ت) أو تركيب مرفق في أستراليا، (ث) أو تنفيذ أعمال الصيانة لمرفق في أستراليا، (ج) أو تشغيل مرفق في أستراليا
8	يصنِّع أو يورِّد مكونات للاستخدام، أو يمكن أن تستخدم في تصنيع مرفق للاستخدام، أو يمكن أن تستخدم في أستراليا	(أ) تصنيع أيٍّ من هذه المكونات، (ب) توريد مثل هذه المكونات.
9	يوصِّل المرفق بشبكة لتكنولوجيا الاتصالات في أستراليا	توصيل مرفق بشبكة لتكنولوجيا الاتصالات في أستراليا
10	يصنِّع أو يورِّد أجهزة للعملاء بغرض الاستخدام، أو احتمالية الاستخدام في أستراليا	(أ) تصنيع مثل هذه الأجهزة الخاصة بالعملاء، (ب) أو توريد أي من هذه الأجهزة الخاصة بالعملاء.
11	يصنِّع أو يورِّد مكونات بغرض الاستخدام، أو احتمالية الاستخدام في تصنيع أجهزة العملاء بغرض الاستخدام، أو إمكانية الاستخدام في أستراليا	(أ) تصنيع أي من هذه المكونات، (ب) أو توريدأي من هذه المكونات.
12	(أ) يركِّب أو يتولى صيانة أجهزة العملاء في أستراليا، (ب) ويفعل ذلك بالنيابة عن المستخدم النهائي للجهاز.	(أ) تنفيذ أي من هذه التركيبات لجهاز العميل، (ب) تنفيذ أي أعمال صيانة لجهاز العميل.

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

13	(أ) يوصِّل جهاز العميل بشبكة الاتصالات في أستراليا، (ب) ويفعل ذلك بالنيابة عن المستخدم النهائي للجهاز.	تنفيذ أي من هذه التوصيلات لجهاز العميل بشبكة الاتصالات في أستراليا.
14	شركةً قانونية تنفِّذ التالي: (أ) تصنيع، (ب) أو توريد (ت) أو تركيب، (ث) أو صيانة أجهزة تشغيل البيانات	(أ) تصنيع جهاز تشغيل البيانات بغرض الاستخدام، أو احتمالية الاستخدام في أستراليا، (ب) أو توريد جهاز تشغيل البيانات بغرض الاستخدام، أو احتمالية الاستخدام في أستراليا، (ت) أو تركيب جهاز تشغيل البيانات في أستراليا، (ث) تولّي شخص داخل أستراليا بصيانة جهاز تشغيل البيانات.
15	شركةً قانونيةً تنفِّذ التالي: (أ) تطوير، (ب) أو توريد، (ت) أو تحديث البرمجيات التي يمكن تركيبها على الكمبيوتر أو أي جهاز آخر يكون متصلاً، أو يمكن أن يتصل، بشكة الاتصالات داخل أستراليا.	(أ) تطوير مثل هذه البرمجية، (ب) أو توريد مثل هذه البرمجية، (ت) أو تحديث مثل هذه البرمجية.

ملحوظة 1: انظر أقسام رقم 317HAA و 317MAA و 317TAA (المشورة لمقدمي خدمات الاتصالات المحددة).

ملحوظة 2: انظر أيضاً 317ZT (أساس دستوري بديل).

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

الأنشطة والأشياء المدرجة 317E

(1) بهدف تطبيق هذا التقرير لمقدم خدمات الاتصالات المحددة، الفعل أو الشيء المدرج يعني:

(أ) إزالة واحد أو أكثر من أشكال الحماية الإلكترونية التي تُطبَّق، أو كانت تطبق، من خلال مقدم الخدمة أو بالنيابة عنه؛
(ب) أو تقديم المعلومات الفنية؛
(ت) أو تركيب أو صيانة أو اختبار أو استخدام برمجية أو جهاز؛
(ث) أو ضمان أن المعلومات التي جرى الحصول عليها فيما يتعلق بتنفيذ ضمان أو توكيل ما مقدمة في الشكل السليم؛

(ث 1) أو النشاط أو الشيء الذي يُنفَّذ للمساعدة في أو تسهيل:

1. فعالية ضمان أو تفويض بموجب قانون الكومنولث أو الدولة أو الإقليم؛
2. أو الحصول على معلومات بشكل فعال، تتعلق بضمان أو تفويض بموجب قانون الكمنولث أو الدولة أو الإقليم؛

(ج)أو تسهيل أو المساعدة في الوصول إلى أي من الأنشطة التالية لمقدم الخدمة، التي تنطبق عليها الشروط:

1. مرفق؛
2. جهاز للمستهلك؛
3. جهاز لتشغيل البيانات؛
4. خدمة نقل مدرجة؛
5. خدمة تسهيلية أو تكميلية أو طارئة للإمداد بخدمة النقل المدرجة؛
6. خدمة إلكترونية؛
7. خدمة تسهيلية أو تكميلية أو طارئة لتوفير الخدمة الإلكترونية؛
8. برمجية مستخدمة للاستخدام، أو يمكن أن تُستخدم، متعلقة بخدمة إلكترونية؛
9. برمجية يمكن تركيبها على الكمبيوتر أو أي جهاز آخر متصل، أو يمكن أن يتصل، بشبكة اتصالات.

(ح) أو المساعدة في اختبار وتعديل أو تطوير أو صيانة تكنولوجيا أو بناء القدرة؛
(خ) أو الإخبار بإجراء أنواع معينة من التغيير أو التطوير يكون لها تأثير على الأنشطة الخاصة بمقدمي خدمات الاتصالات المحددة، التي ينطبق عليها الشروط، إذا كانت هذه التغييرات ترتبط بتنفيذ ضمان أو تفويض ما؛

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

(د) أو تعديل أو تسهيل التعديلات أو أي من السمات الخاصة بخدمة معينة يقدمها مقدم خدمة الاتصالات المحددة؛

(ذ) أو استبدال أو تسهيل استبدال خدمة يقدمها مقدم خدمات اتصالات محددة، وذلك بـ:

1. خدمة أخرى يقدمها مقدم الخدمة؛
2. أو خدمة يقدمها مقدم خدمات اتصالات محددة آخر.

(ر) أو نشاط أو شيء يُنجَز لإخفاء حقيقة أن أي شيء قد حدث سراً عند أداء أي مهمة أو ممارسة أي سلطة، بموجب قانون الكومنولث أو الدولة أو المنطقة، ما دامت المهمة أو السلطة تتعلق بالتالي:

1. فرض قانون جنائي يتعلق بالجرائم الأسترالية الكبيرة؛
2. أو المساعدة في فرض القوانين الجنائية في دولة أجنبية، إذا تعلقت هذه القوانين باتهامات كبيرة أجنبية؛
3. أو مصالح الأمن القومي الأسترالي ومصالح العلاقات الخارجية الأسترالية أو مصالح المصلحة الاقتصادية القومية لأستراليا.

(2) الفقرة (ز) (1) لا تنطبق على:

(أ) التصريح ببيان خاطئ أو مضلل؛

(ب) أو الاشتراك في عمل غير أمين.

شروط الالتزام:

شروط وأحكام 317ZK التي تُقدَّم المساعدة بمقتضاها... إلخ

الإطار

(1) ينطبق هذا القسم إذا كان مقدم خدمة الاتصالات المحددة تنطبق عليه شروط بمقتضى:

(أ) إنذار المساعدة الفنية؛
(ب) أو إنذار بناء القدرة الفنية.

الشروط والأحكام:

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

2) يجب على مقدم خدمة الاتصالات المحددة الالتزام بمتطلبات هذه الشروط والأحكام كما هو:

أ. متفق عليه بين الأطراف التالية:

1. مقدم الخدمة؛
2. أو مفاوض التكاليف.

ب. أو الفشل في الوصول إلى الاتفاق الذي يحدده الحكم الذي يعينه الأطراف.

معايير صنع القرار 317V

لا يحق للنائب العام أن يصدر إنذاراً ببناء القدرة الفنية لمقدم خدمة اتصالات محددة إلا في حالة:

(أ) أن يكون النائب العام على قناعة بأن متطلبات إصدار الإنذار معقولة ومناسبة،
(ب) وأن يكون النائب العام على قناعة بأن الالتزام بالإنذار:

1. عملي؛
2. وملائم فنياً.

ملحوظة: انظر القسم أيضاً 317ZAA

من حق مقدم الخدمة أن يطلب تقييماً للالتزام بالمذكور آنفاً، وعند تنفيذ التقييم المرتبط بإنذارات القدرة الفنية يجب على من يجري التقييم

(أ) أن يأخذ ما يأتي في الاعتبار:

1. إذا كان إنذار بناء القدرة الفنية المقترح يتعارض مع القسم 317 ZG؛
2. وإذا كانت المتطلبات التي يفرضها إنذار بناء القدرة الفنية معقولة ومتوازنة؛
3. وإذا كان الالتزام بإنذار القدرة الفنية المقترح عملياً؛
4. وإذا كان الالتزام بإنذار القدرة الفنية المقترح يمكن تحقيقه فنياً؛
5. وإذا كان إنذار بناء القدرة الفنية المقترح هو الإجراء الأقل إقحاماً، الذي يمكن أن يكون فعالاً في تحقيق هدف إنذار بناء القدرة الفنية المقترح.

(ب) وأن يعطي أهمية كبيرة للأمور المذكورة في الفقرات الفرعية أ (1).

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

8. عن المؤلفين

1.8. جورج بلاكر

جورج بلاكر هو مدير الشركاء الاستشاريين في الاقتصاد والقانون LECA، وخبير في التحليل الاقتصادي للقانون والتنظيم. ويتولى حالياً منصب أستاذ مساعد فخري في الجامعة الوطنية الأسترالية ANU، وعضو كلية ولفسون، بجامعة أكسفورد. ويدرِّس أحياناً الاقتصاد التنظيمي للعاملين في الهيئات والشركات التنظيمية الأسترالية، وأجرى أبحاثاً عامة جيدة، وقدَّم المشورة الاقتصادية الخبيرة للعديد من الجهات، وعلَّق على عدد كبير من القضايا المرتبطة بتنظيم صناعة تكنولوجيا الاتصالات والمعلومات، (مثل تنظيم الإنترنت، وتخصيص الطيف والاستخدام والنواقل وخدمات النقل والنفاذ للشبكات)، وصناعات المرافق (مثل الطاقة والنقل)، وكذلك قانون المنافسة والملكية الفكرية والعقود وقانون الضرائب الذي يؤثر على العديد من الصناعات في أستراليا ومنطقة المحيط الهادي الآسيوي وشمال أمريكا وأوروبا.

وشارك الدكتور بلاكر في عدد من مراجعات السياسة التنظيمية وسياسة المنافسة في أستراليا ومنطقة المحيط الهادي الآسيوي وشمال أمريكا وأوروبا.وكان له استشارات خبيرة على المستوى العالمي في العديد من الهيئات التنظيمية وفي قاعات المحاكم، لمراجعة القرارات التنظيمية في مرحلة الاستئناف، وأيضاً في قضايا التحكيم في لاهاي- وأمام الوزراء والبرلمانات المسؤولة عن التحقيقات، وعن عمليات الإصلاح في أستراليا والمملكة المتحدة والاتحاد الأوروبي ونيوزيلندا والصين وكوريا واليابان والفلبين. فعلى سبيل المثال، أدلى الدكتور بلاكر بخبرته وشهادته أمام المحاكم الفيدرالية الأمريكية والمحكمة الفيدرالية الأسترالية والمحكمة العليا لنيوزلندا. وقد أشارت المحكمة العليا في إنكلترا وويلز وكذلك اللجنة الأوروبية إلى التحليل الذي قدمه أمام مجلس اللوردات. وتولى منصب مدير مركز القانون والاقتصاد في الجامعة الوطنية الأسترالية ANU في الفترة من 1997-2017 م، وحصل على منحة Olin في القانون والاقتصاد من جامعة كورنل بالولايات المتحدة الأمريكية عام 2000 م. وكان بلاكر أستاذاً زائراً في كلية الاقتصاد في لندن في الفترة من 2015 إلى 2018 م، وفي مركز القانون والاقتصاد بجامعة لندن في الفترة من 2010 إلى 2015 م، وفي جامعة أوكسفورد عام 2008 م، وفي المعهد البريطاني للقانون الدولي والمقارن BIICL في الفترة من 2009 م إلى الآن. وعمل كبيرَ محللين ومستشاراً اقتصادياً لدى NZ Treasury في الفترة من 1984 إلى 1996 م. وهو عضو مجلس تحرير الدورية الأوروبية للقانون والاقتصاد. وحصل على درجة الدكتوراه في الاقتصاد من جامعة أوكسفورد عام 1992 م، ويجمل درجة الماجستير في الاقتصاد مع مرتبة الشرف وعلى بكالوريوس القانون.

1.9. ويليام ليهر

ويليام ليهر خبير اقتصادي في مجال تكنولوجيا الاتصالات وصناعة الإنترنت، وهو مستشار له خبرة تمتد لأكثر من خمسة وعشرين عاماً. ويقدِّم ليهر بانتظام المشورة لكبار مسؤولي الصناعة

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

وصناع القرار في الولايات المتحدة الأمريكية وخارجها بشأن السوق والصناعة وتداعيات السياسة على الأحداث فيما يتعلق بالنظام الإيكولوجي للإنترنت. وهو عالم باحث في مجال علوم الحاسوب ومعمل الذكاء الاصطناعي CSAIL بمعهد ماساشوستس للتكنولوجيا. ويشارك حالياً في عدد من مشاريع الأبحاث المتعددة التخصصات التي تركز على قضايا، مثل نفاذ إنترنت النطاق العريض والأمن السيبراني وهندسة شبكات الجيل القادم وإدارة الطيف. بالإضافة إلى العمل الأكاديمي، يقدِّم دكتور ليهر الاستشارات إلى عملائه في القطاعين العام والخاص في الولايات المتحدة الأمريكية وخارجها بشأن أمور إستراتيجية تكنولوجيا الاتصالات والمعلومات وقضايا السياسة. والدكتور ليهر حاصل على درجة الدكتوراه في الاقتصاد من جامعة ستانفورد، وعلى درجة الماجستير في إدارة الأعمال في التمويل من جامعة وارتون وعلى درجة MSE والبكالوريوس والـ BS من جامعة بنسلفانيا. http://people.csail.mit.edu/wlehr/ ولكي يشارك في إخراج هذا التقرير، عُين دكتور ليهر مديراً استشارياً في LECA.

1.10. مارك لوني

مارك لوني مدير استشارى في LECA، وخبير في أنظمة الاتصالات المتطورة وتقنياتها، وفي السياسة العامة وإدارة القطاع العام. وشغل منصباً تنفيذياً رفيعاً في قطاع الخدمات العامة الأسترالي خمسة عشر عاماً، إذ سعى لتقديم المشورة بشأن أمور إدارة الطيف والقضايا التنظيمية لتكنولوجيا الاتصالات للعملاء الدوليين منذ عام 2019 م. وعمل في منصب مدير تنفيذي لهيئة الاتصالات والإعلام الأسترالية ACMA في الفترة من 2005 إلى 2018 م،وكان له دور مهم في تأسيس الهيئة التنظيمية للاتصالات المتقاربة من 2004 إلى 2005 م. وقاد مارك التطوير والتنفيذ وتوصيل الترتيبات التنظيمية للإذاعة والاتصالات الراديوية وخدمات تكنولوجيا الاتصالات لأكثر من عشرين عاماً في وكالة إدارة الطيف وهيئة الاتصالات الأسترالية وهيئة الاتصالات والإعلام الأسترالية ACMA .وكان مارك الرئيسَ التنفيذي للوفد الأسترالي في المؤتمر العالمي للاتصالات الراديوية عام 2003 م.

وقد انضم مارك للخدمة العامة الأسترالية عام 1988 م في وزارة الدفاع، إذ شارك في بحث الاتصالات الموكبة لما يقرب من 9 أعوام. ومنذ عام 2010 م، شارك مارك في أبحاث لمؤتمرات معهد مهندسي الكهرباء والإلكترونيات الـ IEEE مثل DySPAN، وكذلك لدورية سياسة تكنولوجيا الاتصالات TelPol.

وفي عام 2014 م، قدَّم مارك الاستشارات لحكومة منغوليا بشأن التحول السريع لشبكات محمول الجيل القادم (LTE/LTE المتطور)، وكذلك قضايا أخرى مثل النواقل والمتطلبات الأمنية. وقد حصل مارك على شهادة البكالوريوس من جامعة Curtin، ثم واصل الدراسات العليا بالجامعة الوطنية الأسترالية.

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

1.11. دوج سيكر

دوجلاس سيكر خبير عالمي أمريكي في تقنيات الشبكات وتطبيقاتها وتأثيراتها في الصناعات الأخرى مثل الأنظمة اللاسلكية والأمن السيبراني للعصر الحالي والمستقبل. وهو يشغل حالياً منصب عميد مشارك أول للحوسبة وعلوم الحاسوب والهندسة الكهربائية، وهو أستاذ بجامعة كولورادو دنفر حرم Anschutz. وقد عمل من قبل رئيس قسم Lord Endowed Chair لكلية علوم الحاسوب وفي كلية الهندسة بجامعة Carnegie Mellon، ورئيس قسم في الهندسة. كذلك تولى مؤخراً منصب المدير المؤقت لـ CyLab بجامعة CMU، التي تتضمن خبرات من مختلف التخصصات بالجامعة، للتعاون في الأبحاث المتميزة والتعليم المصمم من أجل المساعدة في خلق عالم يمكن من خلاله الوثوق في التكنولوجيا. ويعمل دوج أيضاً مديراً تنفيذياً للمجموعة الاستشارية الفنية لإنترنت النطاق العريض BITAG، وقد عمل في منصب المسؤول الأول التكنولوجي CTO لإدارة الاتصالات والمعلومات الوطنية NTIA وللجنة الاتصالات الفيدرالية FCC، ومستشاراً أول للمعهد القومي للعدل التابع لوزارة العدل، ورئيساً للجنة التوجيه لمجلس موثوقية الشبكة والتشغيل البيني. وقبل ذلك، عمل في منصب مدير الهندسة الدولية لشركة اتصالات المستوى الثالث. وقد نشر العديد من الأعمال في مجالات إقامة الشبكات وأنظمة اللاسلكي وأمن الشبكة وسياسة الشبكة. ولغرض هذا التقرير، عُيِّن دكتور سيكر مديراً استشارياً في LECA.

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