Nota Preliminar:
Autentificación electrónica: algunas implicaciones

Por Sanya Reid Smith, Asesora legal y principal investigadora de la Red del Tercer Mundo
(Third World Network, sanya@twnetwork.org), parcialmente actualizado en agosto de 2018.
Gracias a Richard Hill por sus contribuciones, cualquier error restante es de Sanya.
Traduccion al español de Alejandro Villamar, miembro de la RMALC y la Coalición Mexico Mejor Sin TLCs,
alermalc@gmail.com

RESUMEN EJECUTIVO
INTRODUCCION

CIBERSEGURIDAD
Propuestas TPP, OMC, TLCEU y RCEP
- TPP
- OMC
- TLC UE
- RCEP

HTTPS COMO UN EJEMPLO DE SEGURIDAD
- La diferencia entre http y https
- Los beneficios de conexión con https
- El costo de conectarse con https
- ¿Qué tan común es el https?

ALGUNOS EJEMPLOS DE REGULACION GUBERNAMENTAL EXISTENTES DE LAS TRANSACCIONES ELECTRONICAS PARA LA SEGURIDAD / O QUIZA NECESARIAS
- Derecho Privado
- Transmisión de números de seguridad social (SSN) del sector privado, etc.
- El Problema
- Algunos gobiernos han aprobado legislación para enfrentar el problema

TRANSACCIONES SOBRE SALUD
BANCA EN LINEA
- El problema
- Los gobiernos ya requieren un cierto nivel de seguridad
- La norma del sector privado no es lo suficientemente segura

ENTIDADES FINANCIERAS
DATOS DE CREDITO Y TARJETAS DE CREDITO
- IMPLICACIONES DEL SECTOR PRIVADO PARA ELEGIR EL MÉTODO DE AUTENTICACIÓN APROPIADO PARA LAS TRANSACCIONES CON TARJETA DE CRÉDITO / DÉBITO
- Las empresas dominantes establecen los estándares y penalizan a quienes no cumplen
- Las empresas dominantes establecen un estándar que es difícil y costoso de cumplir
- El estándar del sector privado no es lo suficientemente seguro

WHATSAPP
UBER
SEGURIDAD EN OLEODUCTO
PLATAFORMAS DE COMERCIO DE STOCK INSEGURO
FACEBOOK ENVÍA DE DATOS A CREADORES DE APLICACIONES SIN ENCRIPTADO
SERVICIOS DE ANALÍTICA LIDE TERCEROS QUE UTILIZAN HTTP ENCRIPTADO
COMPAÑÍA DE INFORMES DE CRÉDITO (EQUIFAX)
DATOS DE SALUD

LOS REGLAMENTADORES DE LOS ESTADOS UNIDOS YA SE DAN CUENTA DE QUE LAS REGULACIONES EXISTENTES SON INSUFICIENTES

ALGUNAS IMPLICACIONES CUANDO SE COMBINAN CON OTRAS PROPUESTAS DE *ECOMMERCE* ETC

EFICACIA DE LAS EXCEPCIONES

SALUD / EXCEPCIÓN DEL MEDIO AMBIENTE
EXCEPCIÓN DE PRIVACIDAD
DEFENSA PRUDENCIAL
OTRAS EXCEPCIONES

CONCLUSIÓN

ANEXO: POSIBLES PROBLEMAS DE CIBERSEGURIDAD FUTUROS

ACCESO / USO NO AUTORIZADO DE INFORMACIÓN GENÉTICA / ADN
La falta de protección adecuada de la información genética ya ha tenido consecuencias
Las empresas de pruebas genéticas de consumidores generalmente no están sujetas a las regulaciones de EE.UU. sobre privacidad de datos de salud
Los piratas informáticos podrían robar datos genéticos
Se encuentran disponibles formas más seguras de manejar datos genéticos

La **autenticación** o **autentificación**[1]es el acto o proceso de confirmar que algo (o alguien) es quien dice ser. A la parte que se identifica se le llama **probador**. A la parte que verifica la identidad se la llama **verificador**. Es habitual que el probador sea un usuario que quiere acceder a ciertos recursos y el verificador sea un sistema que protege el acceso a dichos recursos y tiene que verificar que el que accede sea un usuario que tiene permisos para acceder a esos recursos. Para poder tener autenticación es necesaria, como condición previa, la existencia de identidades biunívocamente identificadas de tal forma que se permita su identificación. https://es.wikipedia.org/wiki/Autenticaci%C3%B3n (Nota del T.)

Resumen ejecutivo

Esta nota preliminar analiza las implicaciones de las propuestas de comercio electrónico en la autentificación electrónica (eauthentication) en los tratados comerciales, como la Asociación Económica Integral Regional (RCEP), la Asociación Transpacífico (TPP), la Organización Mundial del Comercio (OMC) y los acuerdos de libre comercio de la Unión Europea (UETLC) que requieren que los gobiernos le dejen al sector privado el establecer los métodos de autentificación (es decir, los estándares de seguridad) de las transacciones electrónicas (excepto tal vez una categoría de transacciones). Esta nota:

• Da ejemplos de violaciones a la ciberseguridad debido a estándares de seguridad insuficientes en las transacciones electrónicas
• destaca que la falla sistémica del mercado debido a las externalidades y las asimetrías de información hacen que dichas violaciones a la ciberseguridad puedan repetirse sin regulación. (A medida que Internet Society señala las fallas del mercado, 'a menudo la intervención del gobierno se usa para abordar la falla'). Esta intervención / regulación gubernamental está prohibida / restringida por estas propuestas de comercio electrónico.
• da algunos ejemplos de gobiernos de países desarrollados y en desarrollo (incluidos gobiernos subnacionales) que establecen ciertos estándares para métodos de autenticación para transacciones electrónicas y por qué lo hacen (por ejemplo, protección y privacidad del consumidor), incluso porque dejan que el sector privado elija sus estándares si sido problemático,
• proporciona un ejemplo de lo que sucedió cuando se dejó que el sector privado decidiera sus propios estándares:
o Las empresas dominantes establecieron estándares costosos y difíciles de cumplir.
o estas normas no eran lo suficientemente seguras

• señala cómo los problemas causados por esta propuesta de comercio electrónico pueden verse exacerbados por otras propuestas de comercio electrónico (o en otros capítulos de FTA como los servicios)
• destaca la posible dificultad de utilizar las excepciones habituales en los acuerdos comerciales por motivos de privacidad, salud, prudencia, etc.

Introducción

La seguridad cibernética

La Internet Society señaló en su informe de 2016:[1]

• "las infracciones de datos continúan aumentando en número, tamaño y costo" (consulte el Capítulo 2 para obtener detalles[a] que incluyen un dicho común de ciberseguridad: "Hay dos tipos de empresas: las que han sido pirateadas y las que no saben que han sido pirateados 'y que incluso las propias compañías de ciberseguridad han sido pirateadas[2]). Según un estudio, el 93% de las infracciones de datos podrían haberse evitado en función de las herramientas existentes, lo que deja un 7% (por ejemplo, el día cero para un *exploits*[b]) que no pueden protegerse, por lo que los datos en riesgo deben cifrarse para que no puedan hackeados.
o El robo de identidad es el más común y los detalles de la cuenta bancaria / tarjeta de crédito son las segundas infracciones más frecuentes.
• El costo de las infracciones de datos (que es una subestimación ya que muchos países aún no requieren informes de violaciones de datos y los costos para la sociedad y el usuario a menudo no están incluidos, ver más abajo) se estimaron en 2015 en "alrededor de USD 500" mil millones, y se cuadruplicaría a USD 2,1 billones en 2019, lo que representa el 2,2% del PIB mundial '

Además, existen fallas de mercado ampliamente reconocidas en ciberseguridad. P.ej:

• un informe del gobierno de EE. UU. de 2018 señaló que "los incentivos de mercado están desalineados". Los incentivos de mercado percibidos no se alinean con el objetivo de "reducir drásticamente las amenazas perpetradas por ataques automatizados y distribuidos". Los incentivos de mercado motivan a los desarrolladores, fabricantes y proveedores de productos para minimizar el costo y el tiempo de comercialización, en lugar de crear seguridad u ofrecer seguridad eficiente actualizaciones. Tiene que haber un mejor equilibrio entre la seguridad y la comodidad cuando se desarrollan productos"[3].
• La Agencia de la Unión Europea para Seguridad de Redes e Información establecida por la UE señaló en 2016 que "estamos viendo una falla de mercado para la ciberseguridad y la privacidad: las soluciones confiables son más costosas para los proveedores y los compradores son reacios a pagar una prima por seguridad y privacidad .'[4]

Además, el informe 2016 de Internet Society[5] incluye:

• Dada la frecuencia de grandes violaciones de datos (por ejemplo, Target tenía 40 millones de números de tarjetas de crédito robadas y puestas a la venta en línea), "la pregunta sigue siendo por qué, dado el costo de las infracciones, las organizaciones no hacen más para abordar las unos, y para reducir el costo y el impacto de los previsibles? 'La respuesta es que:

---

[a] Dado que muchos países no requieren informes de incumplimientos, estos son subestimados.

[b] Estas son vulnerabilidades de seguridad que el desarrollador de software desconoce hasta que se exponen (dando 'cero días' para arreglar la vulnerabilidad).

o 'Hay una falla del mercado que rige la inversión en ciberseguridad. Primero, las infracciones de datos tienen externalidades; costos que no son contabilizados por las organizaciones. En segundo lugar, incluso cuando se realizan inversiones, como resultado de la información asimétrica, es difícil para las organizaciones transmitir el nivel resultante de ciberseguridad al resto del ecosistema. . . [Es decir] El costo de una violación no es responsabilidad exclusiva de la organización violada, y el beneficio de ofrecer una mejor seguridad de los datos no es lo suficientemente alto. . . Como resultado, el incentivo para invertir en ciberseguridad es limitado; las organizaciones no soportan todo el costo de no invertir, y no pueden beneficiarse plenamente de haber invertido. Además, "en los países donde ni siquiera se requiere divulgación, las externalidades son aún mayores, ya que las empresas pueden incluso no asumir ningún costo de reputación la brecha, reduciendo aún más el incentivo para invertir en ciberseguridad '.

o Explica las externalidades como: 'La organización violada no asume todos los costos de la infracción; el costo que soportan otros es una externalidad que no necesariamente influye en sus decisiones sobre cómo protegerse contra las violaciones de datos.' Por ejemplo, las organizaciones pirateadas 'a menudo no soportan todo el costo financiero impuesto a otras organizaciones relacionadas por la violación, y no soportan todo el costo impuesto a los usuarios. En términos económicos, estos costos no contabilizados son externalidades. .

• Por ejemplo, cuando las tiendas Target se violaron por datos de tarjetas de crédito, las instituciones financieras sufrieron el costo de reemplazar las tarjetas de crédito y las siguieron para recuperar las pérdidas de Target. De hecho, Target fue violado a través de un contratista conectado, cuyas defensas fueron más débiles, pero es posible que no haya soportado el costo directo de la violación. Incluso los clientes de Target, cuyos detalles de la tarjeta de crédito fueron el objetivo de la violación, tuvieron que demandar por una compensación, llegando finalmente a un acuerdo legal '.

• Los costos para el usuario incluyen 'responsabilidad del usuario por fraude, tiempo dedicado a tratar de ser compensado por fraude y restaurar su identidad y crédito, sin mencionar el costo no financiero en términos de ansiedad e incertidumbre'. Por ejemplo, 'Uno de esos estudios mostró una proporción significativa de las víctimas de los números de seguridad social robada de los EE. UU. fueron objeto de robo de identidad. Cada incidente resultó en USD 3.300 en pérdidas junto con 20 horas de tiempo y USD 770 gastados en abogados. No está claro si estos costos se cubrieron después de esa violación: en general, los usuarios tienen que luchar para obtener una indemnización ".

• Algunas compañías limitan deliberadamente su exposición. Por ejemplo, al menos un servicio de administrador de contraseñas ha sido pirateado y algunos administradores de contraseñas limitan la responsabilidad del desarrollador a USD 100 por usuario. Como resultado, los costos potenciales significativos para los usuarios de un administrador de contraseñas son externalidades para el desarrollador. . . un administrador de contraseñas puede almacenar cientos de contraseñas, cuya violación podría infligir costos a los usuarios mucho mayores que el máximo de USD 100 que se cubre; este es un excelente ejemplo de una externalidad que una empresa hace soportar a sus usuarios ".

• 'La falta de responsabilidad organizacional por todos los costos de una infracción puede limitar el incentivo para detenerlos'.

o Explica **las asimetrías de información** [c] como: 'Los interesados no tienen información completa sobre los riesgos que pueden enfrentar en línea, por lo que es difícil tomar decisiones informadas. En particular, es difícil para las organizaciones beneficiarse de tomar los pasos correctos para evitar las infracciones de datos, porque no pueden transmitir su nivel de seguridad de datos a los clientes. Esto limita el incentivo para invertir en seguridad de datos. Por ejemplo, al elegir un administrador de contraseñas, un usuario no tendría forma de saber qué herramientas de seguridad se usan para el administrador de contraseñas y qué tan bien se implementan, lo que dificulta elegir el el más seguro. '

• 'Los problemas de selección adversa y riesgo moral surgen de la información asimétrica'.

• Selección adversa: "Aquellos con mejor información serán selectivos en cómo participan en un mercado. En el mercado de autos usados, sin un medio para indicar si un automóvil usado es de alta calidad, solo se venderán aquellos con autos de menor calidad, lo que resultará en un mercado de limones. En los mercados de seguros, las personas comprenden mejor su propio riesgo que la compañía de seguros, lo que también puede resultar en una selección adversa, ya que las personas con mayor riesgo tienen más probabilidades de contratar un seguro (y luego, con un grupo asegurado más riesgoso, aumentarán las primas). en consecuencia).'

• Riesgo moral: "El seguro puede hacer que las personas con cobertura tomen menos cuidado porque no soportan el costo total de sus acciones. Por ejemplo, si uno tiene un seguro de automóvil sin deducible y no aumenta las primas, entonces las personas tendrían menos incentivos para estacionar sus automóviles de forma segura, o incluso podrían correr más riesgos al conducir. Esto se conoce como riesgo moral ".

• 'Considere el ejemplo de un minorista en línea, que está preocupado por ser pirateado, y quiere tomar medidas para proteger a la empresa de una violación de datos.

  o Asumir que el minorista decidió invertir una cantidad significativa para proteger la información de sus usuarios de los piratas informáticos, como un medio para competir con otros minoristas en línea que podrían ser más vulnerables. ¿Cómo lo señalarían de manera creíble a los usuarios? Podrían señalar que no han sido pirateados, pero eso no significa que no puedan ser pirateados. Si no hay forma de señalizarlo, no hay forma de ganar más clientes, y por lo tanto mediante una selección adversa, el mercado estaría formado por minoristas que han invertido poco en seguridad.

  o Si el minorista todavía está preocupado por los riesgos de una violación de datos, al no haber invertido la cantidad óptima de ciberseguridad, la compañía podría elegir protección a través de un seguro de seguridad cibernética (esto sería un

[c] 'La información asimétrica surge cuando una parte en un acuerdo o intercambio tiene más información que la otra sobre el objeto del intercambio. El ejemplo clásico es el mercado de automóviles usados. El vendedor del automóvil sabe más sobre su calidad y cómo ha sido tratado que el comprador. Sin embargo, es difícil para los propietarios de automóviles de alta calidad convencer a los compradores de que son de alta calidad, por lo que los automóviles que son iguales en papel (modelo, año, kilometraje recorrido) se venderán por el mismo precio promedio. Como resultado, es menos probable que se vendan automóviles de alta calidad, y el mercado está lleno de 'limones' de baja calidad '.

ejemplo de selección adversa; aquellos que están en mayor riesgo son es probable que tome un seguro). Ahora el riesgo moral puede entrar en juego: tener el seguro significa invertir potencialmente aún menos en ciberseguridad, porque hay incluso un menor costo por una infracción, que por supuesto es más probable ".

• Dadas estas externalidades, el Servicio de Investigación del Congreso de EE. UU. Cuestionó si dejarlo al interés propio de las empresas, como los operadores de oleoductos, dará como resultado un nivel suficiente de ciberseguridad (por ejemplo, infraestructura crítica) porque significa: "En gran medida, por lo tanto, el público debe confiar en el interés propio de la industria del gasoducto para protegerse de las amenazas cibernéticas."[6]
Las empresas pueden no estar dispuestas a proporcionar más ciberseguridad de la que exige la ley (presumiblemente debido al costo y las externalidades y asimetrías de información anteriores). Por ejemplo, TalkTalk, un proveedor de banda ancha del Reino Unido, fue pirateado en octubre de 2015, lo que resultó en la violación de 157,000 registros de clientes no encriptados. Este fue su tercer evento de seguridad en una fila y todavía el CEO de Talk Talk dijo: "[Los datos del cliente] no fueron encriptados, ni está legalmente obligado a encriptarlos ... Hemos cumplido con todas nuestras obligaciones legales en términos de almacenamiento de información financiera. información. "'Por lo tanto, lo anterior indica que dejar que las empresas decidan el nivel de seguridad de sus transacciones electrónicas probablemente dé como resultado una ciberseguridad inadecuada (que es lo que también muestran los ejemplos a continuación).

o 'Aplicar el cifrado como la norma para los datos en tránsito y en reposo. . . Internet Society cree que el cifrado debe ser la norma para las comunicaciones y los datos de Internet. Más específicamente, las organizaciones deben usar un nivel de encriptación cuyo tiempo y costo para descifrar, si es posible, supera cualquier posible beneficio de que un atacante pueda obtener acceso. Muchos de los estudios de casos resaltan el costo de la falta de encriptación: Target, la Oficina de Administración de Personal y otros no tenían encriptación, mientras que TalkTalk, el Centro de Información Farmacéutica de Corea y otros usaban un cifrado insuficiente. . . Las razones económicas para el cifrado limitado o nulo son dobles: se considera que el costo de implementar correctamente el cifrado fuerte es alto, mientras que los beneficios no se perciben como suficientemente altos. ('El cifrado implica la codificación de datos para que solo las partes interesadas pueda leerlos ').

• Se puede requerir la intervención del gobierno en ciberseguridad:

Dadas las externalidades y asimetrías de información con la consiguiente selección adversa y riesgo moral en ciberseguridad, "los gobiernos pueden necesitar intervenir en ciertos casos para ayudar a transmitir ciertos atributos de seguridad". Por ejemplo, para conocer la calidad del airbag de un automóvil al comprar un nuevo coche, 'las personas pueden necesitar depender de un tercero, como el gobierno, para probar y certificar que el automóvil cumple con las normas mínimas. . . Para los atributos de crédito [sobre los cuales nunca se puede aprender], como la seguridad, un consumidor o un agente de un tercero privado tal vez nunca puedan evaluarlos. Es posible que los gobiernos tengan que imponer normas de seguridad. Por ejemplo, los gobiernos pueden estar mejor situados para probar accidentes de automóviles y garantizar que cumplan con las normas de seguridad ".

• 'En algunos casos, es posible que algunas normas mínimas para el manejo de datos deban ser obligatorias si no se adoptan voluntariamente (como las disposiciones sobre seguridad de datos y minimización de datos en la ley). . .

> • cuando la calificación externa o la certificación no es suficiente, o cuando los estándares voluntarios adecuados no se adoptan completamente, se puede necesitar un mandato del gobierno. Esto es particularmente cierto cuando la falla del mercado es significativa, ya sea por externalidades altas o por información asimétrica extrema. Las leyes de privacidad y protección de datos generalmente contienen requisitos mínimos de seguridad de datos. Como se señaló anteriormente, hay ejemplos donde los mandatos son más adecuados para resolver una falla del mercado.

> Las organizaciones deben ser inducidas a internalizar las externalidades negativas que causan a otras organizaciones y usuarios, y a la sociedad en general, para reducir el incentivo para crearlos. En muchos casos, esto puede ser monetario: así como los impuestos pueden reducir ciertos tipos de contaminación, el aumento de la responsabilidad o penalización que enfrenta la organización responsable de permitir que ocurra una infracción, sin duda, reducirá la probabilidad de que ocurra. Del mismo modo que algunos tipos de contaminación son demasiado tóxicos y deben prohibirse, como el plomo en la pintura o la gasolina, puede ser necesario imponer ciertas prácticas de seguridad de datos.

Otros expertos en ciberseguridad, como el asesor especial de IBM Security, están de acuerdo: "Los ingenieros de seguridad están trabajando en tecnologías que pueden mitigar gran parte de este riesgo, pero muchas soluciones no se implementarán sin la participación del gobierno. Esto no es algo que el mercado pueda resolver. ... los intereses de las empresas a menudo no coinciden con los intereses de las personas. ... Los gobiernos deben desempeñar un papel más importante: establecer estándares, vigilar el cumplimiento e implementar soluciones en las empresas y las redes"[7].

Propuestas en TPP, OMC, TLCEU y RCEP

TPP

El Artículo 14.6 de la Asociación Transpacífico [d] (TPP) [8] restringe a los gobiernos el establecimiento de estándares para la seguridad de las transacciones electrónicas:

> '2. Ninguna Parte adoptará o mantendrá medidas para la autenticación electrónica que:
> (a) prohibir a las partes en una transacción electrónica determinar mutuamente los métodos de autenticación apropiados para esa transacción; . . .
> 3. No obstante lo dispuesto en el párrafo 2, una Parte podrá exigir que, para una categoría particular de transacciones, el método de autenticación cumpla con ciertas normas de funcionamiento o esté certificado por una autoridad acreditada de conformidad con su legislación.

El capítulo de comercio electrónico del TPP tiene algunas excepciones menores, el capítulo no se aplica a:

- Compras del Gobierno

[d] Ahora se le cambió el nombre al texto por el de Acuerdo Global y Progresista de Asociación Transpacífico, pero el capítulo de comercio electrónico sigue siendo el mismo que en el TPP. https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/tpp-and-cptpp-the-differences-explained/ y https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/.

- "Información retenida o procesada por o en nombre de una Parte, o medidas relacionadas con dicha información, incluidas las medidas relacionadas con su recopilación".

OMC

La Unión Europea (UE) hizo una propuesta similar en la Organización Mundial del Comercio (OMC): la versión 2017 también tiene una excepción para 'una categoría particular de transacciones'[9], pero esta excepción no está presente en la propuesta de la OMC en 2018[10]. Actualmente no existe un mandato para **negociar** reglas de comercio electrónico en la OMC. En la OMC, el mandato actual es meramente **examinar** varios asuntos de comercio electrónico[11]. Sin embargo, en la Conferencia Ministerial de la OMC celebrada en Buenos Aires del 10 al 13 de diciembre de 2017 (MC11), algunos Miembros de la OMC firmaron una declaración conjunta diciendo que "iniciarán un trabajo exploratorio hacia negociaciones futuras de la OMC sobre los aspectos del comercio electrónico relacionados con el comercio"[12]. las reuniones de este grupo ya se han celebrado en 2018.

EUFTA

Todas las propuestas de comercio electrónico de la UE (TLC) disponibles en inglés en el sitio web de la UE (es decir, Chile e Indonesia[e]) tienen la disposición anterior, sin categorías de excepciones[f] a la disposición anterior (que requieren que el sector privado el método de autenticación apropiado para la transacción electrónica).
Sin embargo, esta propuesta extrema parece ser una posición de negociación a la que la UE está dispuesta a agregar excepciones (presumiblemente a cambio de concesiones del otro país) en sus ALC concluidos. Por ejemplo:

- En el TLC Japón-EU, hay una excepción para 'una categoría particular de transacciones'.[13]
- En el TLC México-EU, hay una excepción donde 'una Parte puede requerir que, para una categoría particular de transacciones, el método de autenticación cumpla con ciertas normas de desempeño o esté certificado por una autoridad acreditada de acuerdo con su ley. **Dichos requisitos deberán ser objetivos, transparentes y no discriminatorios, y deberán referirse únicamente a las características específicas de la categoría de transacciones en cuestión**."[14] Esto parece limitar la excepción a una categoría de transacciones e incluso eso se ve restringido por la oración en negrita que exige que las normas, etc., requeridas para esa categoría de transacciones deben ser objetivas, transparentes y no discriminatorias, y se refieren únicamente a las características específicas de la categoría de transacciones en cuestión. Esto limita las regulaciones posibles incluso para la única categoría de transacciones para las cuales se permite una excepción y es más restrictiva que el TLC Japón-EU.

RCEP

Se pudo haber hecho una propuesta similar en las negociaciones de comercio electrónico de la Asociación Económica Integral Regional (RCEP).[g]

---

[e] las otras propuestas de EUFTA en http://trade.ec.europa.eu/doclib/press/index.cfm?id=1395 no incluyen actualmente el capítulo de comercio electrónico, o solo están disponibles en francés (con Túnez).

[f] La UE propone una excepción al capítulo de comercio electrónico en general para "servicios de juegos de azar, servicios de radiodifusión, servicios audiovisuales, servicios de notarios o profesiones equivalentes y servicios de representación legal", pero no incluye la excepción para "una categoría particular de transacciones". 'que se encuentra en su propuesta de firma / eauthentication de OMC 2017.

[g] Dado que los términos de referencia filtrados para el capítulo de comercio electrónico de RCEP incluyen un artículo de firma electrónica, http://bilaterals.org/?rcep-draft-e-commerce-chapter .

Https como ejemplo de seguridad

La diferencia entre http y https

Un sitio web que utiliza http no está encriptado, lo que significa que cualquier persona puede ver la información que le da (por ejemplo, detalles de inicio de sesión, contraseñas, etc.), como si estuviera pasando por un tubo transparente porque es texto claro[15].
Si los sitios web usan https[h], esto significa que está encriptado por lo que es más difícil para terceros (por ejemplo, ladrones) ver los detalles de la tarjeta de crédito que un cliente coloca en un sitio web para comprar algo en línea / reservar un boleto aéreo o hotel, etc. los tubos se vuelven opacos. Solo la gente al final puede ver lo que se transmite a través de ellos"[16].

Los beneficios de cambiar a https

Como se señaló anteriormente, el uso de https significa que cuando se está transmitiendo información personal confidencial, como números de tarjetas de crédito, no puede ser leída por otros. Además, 'las filtraciones de Edward Snowden sobre la NSA (Agencia de Seguridad Nacional, una agencia de inteligencia del Gobierno de los Estados Unidos) también dejaron en claro la cantidad de datos no encriptados que la NSA estaba capturando masivamente desde Internet, renovando el interés de la gente en proteger sus conexiones'.[17]

https también protege "el derecho a leer en privado". Un visitante de Wikipedia podría estar aprendiendo acerca de una condición médica que puede sufrir. Alguien que busque en el sitio de anuncios clasificados como Craigslist podría estar buscando un nuevo trabajo. Un estudiante leyendo el Washington Post podría estar siguiendo asuntos políticos de transgénero. Todas esas actividades, se argumenta, merecen estar protegidas de un proveedor de Internet, un empleador o un administrador de la escuela tanto como el número de la tarjeta de crédito de la persona.[18]

"De hecho, HTTPS protege más que la confidencialidad. También ofrece autentificación y lo que los administradores de sitios web llaman "**integridad**".

> • Para que un sitio se registre en un navegador como HTTPS encriptado, se observa con un candado en la barra de direcciones del navegador, necesita **autentificarse**: para demostrar que es el sitio que dice ser, en lugar de un impostor. Para hacer eso, el administrador de un sitio web le pide a una empresa de "autoridad certificadora" como Comodo o Symantec que emita el sitio un "certificado", que dice que la clave pública de cifrado asociada con el sitio realmente pertenece al sitio. Aunque las autoridades certificadoras han sido hackeadas ocasionalmente, como en el caso de la firma holandesa Diginotar en 2011, rompiendo ese sistema de confianza. Pero, en general, un certificado significa que cuando tu navegador dice que estás en https://google.com, realmente estás compartiendo tus datos con un servidor de Google y con nadie más.
>
> • En cuanto a la "**integridad**", HTTPS también evita que cualquier intruso en su red local manipule o bloquee parcialmente el contenido de un sitio en su camino desde un servidor a su navegador. Sin HTTPS, un censor gubernamental puede elegir bloquear ciertas páginas de un sitio o incluso partes de una página. Una manipulación más activa podría permitir que un proveedor de servicios de Internet inserte anuncios o hackers para inyectar código diseñado para comprometer su computadora".[19]

---

h 'HTTPS (Hyper Text Transfer Protocol Secure) aparece en la URL cuando un sitio web está protegido por un certificado SSL', https://www.websecurity.symantec.com/security-topics/what-is-ssl-tls-https

Dada la forma en que los datos enviados por simple http pueden ser interceptados fácilmente, el gerente de investigación de seguridad de aplicaciones de la compañía que encontró la vulnerabilidad de la aplicación de citas (ver más abajo) dijo: "Realmente no hay excusa para usar HTTP estos días".[20]

Los costos de cambiar a https

Hay costos únicos y continuos[i] para cambiar de http a https[21]. Por ejemplo, los sitios web que usan los servicios en la nube de Amazon tienen que pagar más constantemente por un sitio web https.[22] (Amazon tiene el 35% de la cuota de mercado mundial de la nube, la mayoría de las empresas[23]).

¿Qué tan común es https?

Dados los costos de cambio, muchas empresas no cambiarán a https sin que un gobierno les exija hacerlo (por ejemplo, por razones de protección al consumidor, ver más abajo). Por ejemplo:

• Un estudio citado en 2016 de '540 empresas B2B en el Reino Unido demostró que la aceptación de cambiar a HTTPS estaba en el rango del 2 al 3 por ciento'[24]
• Un estudio de marzo de 2016 "mostró que 79 de los 100 sitios web con mayor tráfico en Internet todavía no usan el cifrado HTTPS".[25]

"La mayoría de los usuarios aún desconoce HTTPS, y aunque lo hagan, no tienen ningún control sobre ellos. Deben transmitir sus datos sin restricciones o ir a otro lugar", dice Aas. "Si vamos a proteger a esas personas, tenemos que lograr que los sitios web adopten HTTPS ... Realmente es un punto clave en la seguridad de Internet en este momento".[26]

Dado que los usuarios / consumidores no pueden obligar a los sitios web a usar https, se ven obligados a enviar sus datos sin cifrar o no usar ese servicio. Esta es una razón por la cual los gobiernos pueden necesitar regular para requerir el uso de https (por ejemplo, para ciertos tipos de datos confidenciales, ver a continuación).

Algunos ejemplos de dónde existe la regulación gubernamental de las transacciones electrónicas para garantizar su seguridad.

Es posible que los gobiernos necesiten asegurarse de que las transacciones electrónicas estén seguras de no ser pirateadas en una serie de situaciones. Algunos de estos están abajo. Las regulaciones gubernamentales a continuación (y aquellas que puedan ser necesarias en las situaciones siguientes) no serían posibles si se acuerdan las anteriores propuestas de autenticación electrónicas (o solo son posibles para una categoría de transacciones si se permite esa excepción), a menos que se acuerden otras excepciones.

Los ejemplos que figuran a continuación se obtuvieron de una búsqueda de algunas horas, y cada semana se producen nuevos ejemplos dada la rápida velocidad del cambio tecnológico. Por lo tanto,

[i] por ejemplo el alto costo de certificados de seguridad, https://www.wired.com/2011/03/https-is-more-secure-why-isnt-the-web-using-it-today/

para cuando finalicen las negociaciones de comercio electrónico es probable que se necesiten muchas más excepciones, incluso en sectores actualmente imprevistos/regulaciones.

Acordar restricciones a la capacidad de los gobiernos para establecer métodos de autentificación para las transacciones electrónicas en los acuerdos comerciales (que generalmente son difíciles de actualizar/enmendar porque requieren el consentimiento de todos los países involucrados) bloquearían las restricciones/prohibiciones sobre la capacidad de regular en un campo que cambia rápidamente donde la necesidad de regulación ya es clara y es probable que aumente.

Leyes de privacidad

Las regulaciones en el estado de Massachusetts requieren "Cifrado de todos los registros y archivos transmitidos que contienen información personal [j] que viajará a través de redes públicas, y la encriptación de todos los datos que contienen información personal para ser transmitidos de manera inalámbrica" que se trate de un residente de Massachusetts[27].

El estado de Nevada de EE.UU.especifica que los recopiladores [k] de datos solo pueden transferir información personal electrónicamente[l] si 'el recopilador de datos usa encriptación para garantizar la seguridad de la transmisión electrónica' (excepto para faxes y llamadas de voz)[28].

Muchos otros estados de los EE. UU. han promulgado leyes independientes de la industria que regulan la transmisión de información personal.[29]

Transmisión de números de seguridad social (SSN) del sector privado, etc.

El problema

"Desde la creación de la SSN en 1936, el sector privado la ha utilizado cada vez más para diversos fines, como identificador y autenticador, porque es la única información permanente y única que la mayoría de los estadounidenses tienen sobre sí mismos. El uso del SSN se ha expandido a medida que las organizaciones han adaptado sus sistemas comerciales y de mantenimiento de registros para utilizar

---

[j] se define como 'el primer nombre y apellido de un residente de Massachusetts o la primera inicial y el apellido en combinación con uno o más de los siguientes elementos de datos que se relacionan con dicho residente: (a) Número de seguro social; (b) número de licencia de conducir o número de tarjeta de identificación emitida por el estado; o (c) número de cuenta financiera, o número de tarjeta de crédito o débito, con o sin cualquier código de seguridad requerido, código de acceso, número de identificación personal o contraseña, que permitiría el acceso a la cuenta financiera de un residente; '

[k] definido para incluir una 'corporación, institución financiera o operador minorista o cualquier otro tipo de entidad comercial o asociación que, para cualquier propósito, ya sea por recolección automatizada o de otro modo, maneja, recopila, difunde o trata con información personal no pública'.

[l] Definido como el primer nombre / 'primer nombre y apellido del ser humano en combinación con uno o más de los siguientes elementos de datos, cuando el nombre y los elementos de datos no están encriptados:
(a) Número de seguridad social.
(b) Número de licencia de conducir, número de tarjeta de autorización de conductor o número de tarjeta de identificación.
(c) Número de cuenta, número de tarjeta de crédito o número de tarjeta de débito, en combinación con cualquier código de seguridad, código de acceso o contraseña requeridos que permitan el acceso a la cuenta financiera de la persona.
(d) Un número de identificación médica o un número de identificación de seguro de salud.
(e) Un nombre de usuario, identificador único o dirección de correo electrónico en combinación con una contraseña, código de acceso o pregunta de seguridad y respuesta que permita el acceso a una cuenta en línea. '

el procesamiento de datos automatizado cada vez más sofisticado. El SSN se ha convertido con el tiempo en una parte integral de nuestro sistema financiero.

A medida que el uso del SSN por parte del sector privado ha crecido, también lo hace su disponibilidad y valor para los ladrones de identidad ".[30]

El robo de identidad basado en números de seguridad social (SSN)[m] es un problema tan grave en los EE. UU., Varios sitios web del gobierno de EE.UU. tienen advertencias al respecto, como por ejemplo[31]:

• Con el nombre y el número de la seguridad social de una persona, "un ladrón de identidad podría abrir un nuevo crédito y cuentas bancarias, alquilar un departamento",[32]
• acceder a cuentas existentes u obtener beneficios del gobierno a nombre del consumidor.[33]
• 'utilizarlo para obtener otra información personal sobre usted. Los ladrones de identidad pueden usar su número y su buen crédito para solicitar más crédito en su nombre. Luego, usan las tarjetas de crédito y no pagan las cuentas, esto perjudica su crédito. Es posible que no descubras que alguien está usando tu número hasta que te rechacen para obtener crédito, o comiences a recibir llamadas de acreedores desconocidos exigiendo el pago de artículos que nunca compraste ".[34]
• Los ladrones de identidad pueden usar su SSN para obtener su reembolso de impuestos del Servicio de Impuestos Internos (IRS): "Si es elegible para un reembolso, un ladrón puede presentar una declaración de impuestos antes de hacerlo y obtener su reembolso. Luego, cuando lo haga, el IRS pensará que ya recibió su reembolso.[35]

Las empresas continuarán usando SSN

Las empresas pueden solicitar el número de seguro social de una persona[36], ya que dependen habitualmente de los números de seguro social para garantizar una coincidencia exacta de los consumidores con su información dentro de las organizaciones y que la información que utilizan o comparten con otras organizaciones se corresponde con la persona adecuada. Por ejemplo, se usa para "compartir registros de pacientes dentro del sistema de atención médica"[37].

"Muchas empresas sostienen que el SSN es superior a cualquier otro elemento de información actualmente disponible para identificar a los consumidores y vincular la información con ellos. Los comentaristas de diversos sectores de la economía afirmaron que no hay otros identificadores que sean tan confiables, rentables y precisos para la coincidencia de datos como SSN, porque solo el SSN es permanente, único, omnipresente y común en todas las organizaciones"[38].

'Y es posible que se te niegue el servicio si no das el número'[39].

Como era de esperar, el número de seguro social de un ciudadano estadounidense es muy valioso (por ejemplo, en la web oscura)[40]. La Dark Web o internet oscura es el contenido público de la World Wide Web que existe en darknets, redes que se superponen a la internet pública y requieren de software específico, configuraciones o autorización para acceder: Wikipedia, N.dT.). Esto se debe a que es ampliamente utilizado por las empresas y "A lo largo de las décadas, el número de la Seguridad Social se volvió valioso por lo que se podía ganar al robarlo", dijo Bruce Schneier, miembro de la Escuela de Gobierno Kennedy de Harvard. Era el único número disponible para identificar a una persona y se convirtió en el estándar utilizado para todo, desde confirmar a alguien en el consultorio del médico hasta la escuela. . . La falla del número de Seguridad

[m] Según la Comisión Federal de Comercio del gobierno de EE. UU .: "el SSN facilita el robo de identidad, es decir, que es un elemento de datos necesario, si no necesariamente suficiente, para que se den muchas formas de este delito",

Social es que solo hay uno para cada persona, "una vez que está comprometido una vez, ya está listo", Bob Stasio, miembro del Proyecto de Seguridad Nacional Truman y ex jefe de operaciones de la Agencia de Seguridad Nacional Centro de Operaciones Cibernéticas[41].

El robo de identidad a través de SSN ya era un problema en 2008 y la Comisión Federal de Comercio del gobierno de EE. UU. escribió un informe en el que recomendaba[42]:

• 'limitar las circunstancias y los medios por los cuales pueden transmitirse, haría más difícil que los ladrones obtengan SSN, sin obstaculizar su uso con fines legítimos de identificación y coincidencia de datos'

• 'que se tomen medidas para reducir la visualización y transmisión innecesarias de SSN y mejorar la seguridad de los datos. Con respecto a sus propuestas centrales: mejorar la autenticación, reducir la visualización y transmisión innecesarias de SSN, mejorar la seguridad de los datos y exigir notificaciones de incumplimiento, la Comisión recomienda que el Congreso considere establecer estándares nacionales que se delinearán aún más a través de la reglamentación de las agencias. Además, la Comisión recomienda que el Congreso considere otorgarle la autoridad para obtener sanciones civiles por violaciones de estas reglas.

• 'La Comisión recomienda que el Congreso considere la creación de estándares nacionales para la exhibición pública y la transmisión de SSN. La legislación federal establecería un enfoque a nivel nacional para reducir la visualización y transmisión innecesarias de números de seguro social, mientras se abordan las preocupaciones sobre un parche de leyes estatales con diferentes requisitos. Los estándares nacionales deberían prohibir a las entidades del sector privado exponer innecesariamente los SSN. Los estándares precisos deben ser desarrollados en la elaboración de normas por las agencias federales apropiadas (es decir, las agencias que supervisan las organizaciones que rutinariamente transmiten o muestran SSN), y deben incluir, por ejemplo, prohibiciones en contra de:

> o . . transmitir (o requerir que un individuo transmita) un número de seguro social a través de Internet, a menos que la conexión sea segura contra el acceso no autorizado, por ejemplo, mediante encriptación u otras tecnologías que hacen que los datos sean generalmente ilegibles '

Tras la masiva violación de datos de Equifax en 2017, Rob Joyce, asistente especial del presidente y coordinador de ciberseguridad de la Casa Blanca dijo que el uso de números de seguridad social como el principal método para asegurar las identidades de las personas es "un sistema defectuoso que podemos" "Retiraremos ese riesgo después de saber que hemos tenido un compromiso", dijo. "Personalmente sé que mi número de seguro social se ha visto comprometido al menos cuatro veces en mi vida. Eso es insostenible"[43].

Sin embargo, cambiar de sistema de números de seguridad social no es fácil ", dijo Rotenberg." Tendría que haber muchas audiencias y estudios sobre las consecuencias. Es un tema complicado.'[44]

Algunos gobiernos han aprobado leyes para abordar este problema

Mientras tanto, aproximadamente 25 estados de EE. UU. Han aprobado leyes que limitan la exhibición pública y / o el uso de SSN como California[45] y Minnesota[46], que tienen leyes que regulan cómo se pueden transmitir los números de la seguridad social. Especifican que las empresas privadas no pueden requerir:

• una persona para transmitir su número de Seguridad Social a través de Internet, a menos que la conexión sea segura o el número de la Seguridad Social esté encriptado (con algunas excepciones).
• Una persona que usa su número de Seguridad Social para acceder a un sitio web, a menos que también se requiera una contraseña, un número de identificación personal único u otro dispositivo de autenticación para acceder al sitio web.

Esto estaría prohibido según Art 14.6.2 TPP a menos que se use la excepción para una categoría particular de transacciones (o se aplica otra excepción).

Transacciones de salud

En virtud de las transacciones electrónicas de la Ley de HIPAA Ley de Responsabilidad y Portabilidad del Seguro de Salud (una transacción es "un intercambio electrónico de información entre dos partes para llevar a cabo actividades financieras o administrativas relacionadas con la atención médica"[47], por ejemplo, un hospital que envía un reclamo a la compañía de seguro médico para pagar por la operación de un paciente) entre las entidades cubiertas por HIPAA debe usar ciertos estándares[48]. Dado que estas normas (x12) parecen estar cubiertas por la definición de autentificación electrónica en el Art. 14.1 TPP, esto no está permitido por el TPP a menos que se use la excepción para una categoría particular de transacciones del Art 14.6.3 o se aplican a excepciones generales del TPP[49] (difícil de usar[n] , ver más abajo). para salud, ambiente y privacidad.

La Ley de Protección al Paciente y Cuidado de Salud Asequible de los EE.UU. también exige el cumplimiento de las reglas de funcionamiento ("definidas como" las reglas y pautas comerciales necesarias para el intercambio electrónico de información que no están definidas por un estándar o sus especificaciones de implementación"[50]). 'Las reglas de operación establecen ciertos requisitos para las transacciones que están cubiertas por HIPAA. Especifican la información que se debe incluir cuando se realizan transacciones estándar, lo que facilita a los proveedores el uso de medios electrónicos para manejar transacciones administrativas."[51] Esto tampoco está permitido por el TPP a menos que sea una excepción para una categoría particular de transacciones en Art 14.6.3 se usa o se aplican las excepciones generales (difíciles de usar[o], ver a continuación) del TPP[52] para salud, ambiente y privacidad.

Sin embargo, la racionalidad establecida (ver a continuación) la eficiencia y la reducción de costos no es una de las excepciones generales del TPP.

La razón por la cual el gobierno de EE. UU. establece estas normas y reglas de operación nacionales incluyen[53]:
• 'Para reducir el papeleo y agilizar los procesos comerciales en todo el sistema de atención médica'
• 'garantizar que la comunidad de atención médica obtenga los beneficios de las transacciones estandarizadas y los costos administrativos reducidos'.
• 'Las transacciones estándar, las reglas de operación, los conjuntos de códigos y los identificadores únicos permiten que la información se comparta electrónicamente de manera consistente.

---

[n] incorporan las excepciones GATT y GATS de salud y medio ambiente, etc., que los países han tratado de utilizar 44 veces en la OMC y tuvieron éxito una vez. https://www.citizen.org/sites/default/files/general-exception_4.pdf.

[o] Incorporan las excepciones de salud y medio ambiente, etc. del GATT y el AGCS, que los países han tratado de utilizar 44 veces en la OMC y lo lograron una vez, https://www.citizen.org/sites/default/files/general-exception_4.pdf.

• Con los estándares comunes de contenido y formatos, la información se mueve rápidamente a medida que se comparte entre proveedores y planes de salud de manera predecible.
• Estos estándares tienen el potencial de disminuir los costos de salud, el tiempo dedicado a la documentación y la carga administrativa, brindando a los proveedores más tiempo para la atención del paciente.
• Y las comunicaciones rápidas con las aseguradoras pueden ayudar a informar a los pacientes por adelantado sobre la cobertura, los beneficios y los costos de desembolso directo ".
• Reducir los miles de millones de dólares en administración sanitaria que USA gasta cada año al hacerlo más eficiente para que los hospitales y las compañías de seguros, etc. puedan compartir información electrónicamente.[54]
• Que la elegibilidad para el seguro de salud y el estado de las reclamaciones se puede verificar en línea, por ejemplo, los cargos permitidos. La información y la forma en que se transmite es más uniforme, por lo que los hospitales solo pueden usar un tipo de solicitud electrónica para todas las aseguradoras de salud[55]

Los EE.UU. también tiene reglas operativas obligatorias para la transferencia electrónica de fondos (EFT, es decir, el pago que una compañía de seguros paga a la cuenta bancaria del hospital) y el aviso electrónico de remesa (ERA)[56]. ERA es lo que el seguro de salud envía al hospital para explicar para qué es el pago. Las reglas establecen un formato estándar y contenido de datos para EFT y ERA de cada transacción, que automatiza la conciliación de pagos para proveedores y simplifica el proceso. Esto tampoco está permitido por el TPP a menos que se aplique la excepción para una categoría particular de transacciones en el Art. 14.6.3 o las excepciones generales (difíciles de usar[p], vea a continuación) del TPP[57] para salud, ambiente y privacidad. Sin embargo, el razonamiento anterior sobre la simplificación del proceso no es una de las excepciones generales del TPP.

Esto indica que dejarlo al sector privado (como ocurrió antes de las regulaciones de EE. UU.) condujo a la exigencia de múltiples estándares del sector privado, lo que redujo la eficiencia y la interoperabilidad y ocasionó altos costos administrativos. Por lo tanto, el gobierno de EE.UU. pensó que los beneficios superaban los costos al requerir un solo estándar nacional para mejorar la eficiencia y reducir los costos. Este tipo de regulación no sería posible en virtud de las propuestas de comercio electrónico anteriores (excepto las que tienen una excepción para una categoría particular de transacciones, si esta es la única categoría seleccionada). Cualquier excepción de salud que se aplique a estas propuestas (véanse las excepciones a continuación) no sería pertinente ya que el gobierno introdujo estas normas obligatorias para aumentar la eficiencia y reducir los costos, no por razones de salud (aunque las regulaciones se aplican al sector de la salud).

Banca en línea

El problema

La banca en línea debe ser segura. Esto se debe a que, cuando se deja en manos de los bancos, las aplicaciones bancarias y la banca en línea a menudo son sorprendentemente inseguras. P.ej:

• 'En 2014, Ariel Sanchez probó 40 aplicaciones de banca doméstica y descubrió que el 90% incluía enlaces inseguros (que no usaban SSL), el 40% no verificaba la validez de los certificados SSL, el 50% era vulnerable a sitios cruzados secuencias de comandos, y el 40% eran vulnerables al hombre medio en los ataques. . . Las aplicaciones bancarias de hoy deberían ser mucho más seguras, pero yo

[p] Incorporan las excepciones GATT y GATS de salud y medio ambiente, etc., que los países han tratado de utilizar 44 veces en la OMC y tuvieron éxito una vez. , https://www.citizen.org/sites/default/files/general-exception_4.pdf.

no apostaría. . . Sea cual sea el dispositivo que esté utilizando, la mejor solución es el cifrado de extremo a extremo, que se muestra mediante las direcciones "https" y un candado en el navegador[58].

• incluso los bancos británicos en diciembre de 2017 tomaron atajos (supuestamente para ahorrar dinero y esfuerzo) y usar meros http en la página principal del sitio web del banco; sin embargo, los expertos en seguridad señalan que "sin HTTPS un atacante podría teóricamente modificar elementos del sitio web de un banco". Podrían enviar víctimas a un sitio falso de banca en línea y robar su información. "La página de inicio es insegura, por lo que no puede confiar en nada", dijo el Sr. Hunt. "Este es un sitio web bancario. No hay excusas", agregó Stephen Kellett, de la firma de seguridad Software Verify. "Todas las páginas, ya sea que realicen transacciones, la página de inicio, la página de aproximadamente, todo el lote, todas deberían estar seguras. ¿Por qué? Porque todas lanzan a la página de inicio de session (login)"[59].

Los gobiernos ya requieren un cierto nivel de seguridad

Dados problemas como los mencionados anteriormente, varios reguladores financieros ya especifican el nivel de seguridad de las transacciones bancarias en línea. Por ejemplo:

1) Por lo tanto, el banco central de Malasia requiere autenticación de dos factores, etc. para la banca en línea[q].
2) El banco Central de la India especifica que "los bancos que presten servicios de banca móvil deberán cumplir con los siguientes principios y prácticas de seguridad para la autenticación de transacciones de banca móvil:
a) Todas las transacciones de banca móvil se permitirán solo por validación a través de una autenticación de dos factores.
b) Uno de los factores de autenticación debe ser mPIN o cualquier estándar superior.
c) Cuando se utiliza mPIN, es deseable el cifrado de extremo a extremo del mPIN, es decir, mPIN no debe estar en texto claro en ninguna parte de la red.
d) El mPIN se almacenará en un entorno seguro.[60]

Los reguladores financieros en otros países pueden tener requisitos similares.

Entidades financieras

El Departamento de Servicios Financieros del Estado de Nueva York aprobó un nuevo reglamento que entró en vigencia el 1 de marzo de 2017 en respuesta a amenazas de ciberseguridad para la industria de servicios financieros. Sus requisitos incluyen:

• compañías autorizadas bajo la Ley de Servicios Bancarios, Seguros o Servicios Financieros para encriptar información no pública[r] mantenida o transmitida por estas compañías tanto en tránsito a través de redes externas como en reposo (a menos que no sea factible)[61].

---

[q] Para fortalecer aún más la seguridad de los servicios de banca por Internet, todas las instituciones bancarias que ofrecen servicios de banca por Internet deben implementar la autenticación de dos factores para las transacciones bancarias por Internet. El segundo factor de autenticación es complementar el nombre de usuario y el PIN o la contraseña (que es la autenticación de primer factor) mediante el uso de una herramienta de autenticación adicional como el código de autorización de transacción (TAC), certificado digital, tarjeta inteligente o token USB o un cliente característica biométrica propia, como huella digital o patrón de retina. El segundo factor de autenticación es necesario para transacciones de alto riesgo como registrar beneficiarios o beneficiarios nuevos, transferencia de fondos de terceros, pago a partes no registradas, recargas de tiempo de aire prepago, pagos de facturas y cambio de información confidencial como dirección de correspondencia y números de contacto. http://www.bnm.gov.my/files/publication/fsps/en/2006/cp04.pdf

[r] Esto incluye información de salud y nombre + '(i) número de seguro social, (ii) número de licencia de conductor o número de identificación de no conductor, (iii) número de cuenta, número de tarjeta de crédito o débito, (iv) cualquier código de

• Autentificación de múltiples factores[s] para cualquier persona que acceda a las redes internas de empresas autorizadas por la Ley de Servicios Bancarios, Seguros o Servicios Financieros desde una red externa, a menos que la compañía haya aprobado por escrito el uso de controles de acceso razonablemente equivalentes o más seguros.[62]

o Si este es un ejemplo de "partes en una transacción electrónica" (por ejemplo, según la provisión de autentificación electrónica del TPP[63]) depende de cómo se definan "partes" y "transacción electrónica" (no están definidas en el texto TPP). Por ejemplo, si un empleado que inicia sesión de forma remota en la base de datos interna de su banco para trabajar desde su casa es una "parte" diferente del banco y este trabajo a distancia es una "transacción electrónica". Los países del TPP pueden haber acordado qué significan "partes" y "transacción electrónica" en el historial de negociación del TPP[t], sin embargo, esto no se ha divulgado, por lo que solo los gobiernos del TPP saben si este tipo de situación estaría cubierta por el Art. 14.6 TPP.

Datos de tarjeta de crédito / débito

La Comisión Federal de Comercio (FTC)[64] del gobierno de Estados Unidos ha acusado a compañías que no encriptaron datos confidenciales (por ejemplo, información de tarjetas de crédito / débito) en tránsito por actos o prácticas desleales o que afecten el comercio en violación de la Sección 5 (a) de la Ley Federal de Comercio Ley de la Comisión, 15 USC § 45 (a)[65]. Por ejemplo:

• TJX tiene 2.500 tiendas en todo el mundo. Recopiló información de tarjetas de crédito / débito y otra información personal y la transmitió sin encriptar (en texto claro) dentro y entre sus tiendas. Un intruso se conectó sin autorización a las redes de TJX, instaló herramientas de hackers, encontró información personal almacenada en texto claro y la descargó a computadoras remotas a través de Internet. Además, entre mayo y diciembre de 2006, un intruso interceptaba periódicamente las solicitudes de autorización de la tarjeta de pago en tránsito desde las redes en la tienda a la red corporativa central, almacenaba la información en archivos en la red y transmitía los archivos a través de Internet a computadoras remotas. . . La violación comprometió decenas de millones de tarjetas de pago únicas utilizadas por los consumidores en los Estados Unidos y Canadá. Hasta la fecha, los bancos emisores han reclamado decenas de millones de dólares por cargos fraudulentos en algunas de estas cuentas.[66]" La FTC acusó a TJX de 'actos o prácticas desleales en el comercio o que lo afectan en violación de la Sección 5 (a) de la Ley de la Comisión Federal de Comercio, 15 USC § 45 (a)[67] ' y TJX lo arregló.[68]

---

seguridad, código de acceso o contraseña que permitiría el acceso a la cuenta financiera de un individuo, o (v) registros biométricos '

[s] Definido como 'autentificación a través de la verificación de al menos dos de los siguientes tipos de factores de autentificación:
(1) factores de conocimiento, como una contraseña; o
(2) factores de posesión, como un token o mensaje de texto en un teléfono móvil; o
(3) factores de inherencia, como una característica biométrica '.

[t] Esta historia de negociación es vinculante entre las Partes debido al Artículo 32 de la Convención de Viena sobre el Derecho de los Tratados (CVDT) que especifica que 'el trabajo preparatorio' del tratado puede utilizarse para confirmar el significado de un término o determinar el significado de un término cuando es ambiguo u oscuro, https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf . Los países que son parte de la VCLT están obligados por ella. Además, los artículos 31 y 32 de la CVD reflejan el derecho internacional consuetudinario (Corte Internacional de Justicia en Libia contra Chad, ICJ Reports (1994), página 4, párrafo 41) y el derecho internacional consuetudinario es vinculante para todos los países, incluso los que no son parte a la VCLT.

• BJ's opera 150 almacenes y 78 estaciones de servicio en 16 estados del Este de los Estados Unidos. Aproximadamente 8 millones de consumidores actualmente son miembros, con ventas netas por un total de aproximadamente $ 6,6 mil millones en 2003. BJ no proporcionó seguridad razonable para estos datos confidenciales, porque no pudo cifrar la información del consumidor cuando se transmitió o almacenó en computadoras en las tiendas de BJ [69]. "Las compras fraudulentas se hicieron utilizando copias falsificadas de tarjetas de crédito y débito que los bancos habían emitido a clientes que habían usado sus tarjetas en BJ's. Esto fue posible porque los nombres de sus clientes, números de tarjetas y fechas de vencimiento de sus tarjetas se almacenaban en las redes de computadoras de BJ y luego accedieron ilegalmente y se usaronn en 'copias falsas de tarjetas que se usaron para hacer compras fraudulentas de varios millones de dólares'[70]. La FTC acusó a BJ con prácticas desleales y BJ se conformó[71].

Nevada tiene un sistema de protección de privacidad para compañías que hacen negocios en Nevada que aceptan una tarjeta de crédito/débito que les exige cumplir con la versión actual del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCIDSS)[72].

Implicaciones del sector privado para elegir el método de autentificación apropiado para las transacciones con tarjeta de crédito / débito

Las empresas dominantes establecen los estándares y penalizan a quienes no cumplen

El PCIDSS es un estándar del sector privado creado en 2006[73] por American Express, Discover Financial Services, JCB International, MasterCard y Visa Inc[74], que tiene una serie de requisitos que incluyen "cifrar la transmisión de datos de titulares de tarjetas e información confidencial en redes públicas abiertas"[75] y autentificación multifactorial 'para acceso remoto (que se origina fuera de la red de una compañía) donde ese acceso remoto podría dar acceso al entorno de datos del titular de la tarjeta'.[76]

Un restaurante estadounidense administrado por McCombs recibió una multa de US$ 90,000 por Visa y Mastercard por presuntamente violar los requisitos del PCIDSS que se introdujeron cuatro años después de que firmaran su contrato con el banco y solo fueron referidos en un sitio web impreso en los estados bancarios porque lo hicieron banca en línea que no notaron. Aunque fue su banco el que recibió una multa de Visa y Mastercard, los bancos tienen contratos con los minoristas que obligan a los minoristas/restaurantes a pagar a los bancos por las multas que deben pagar a Visa / Mastercard. Esta multa fue impuesta a pesar de que la mayor parte de la actividad fraudulenta reportada involucró números de tarjetas de crédito que nunca se habían usado en el restaurante y el minorista/restaurante no puede apelar (solo el banco puede no tener incentivos para hacerlo ya que simplemente pasan la multa hasta el minorista/restaurante y al banco le cuesta $ 5,000 USD no reembolsables para apelar)[77].

Este controvertido sistema PCIDSS, impuesto a los comerciantes por compañías de tarjetas de crédito como Visa y MasterCard, ha sido calificado como "cercano al engaño" por un portavoz de la Federación Nacional de Minoristas y otros, que dicen que está diseñado menos para proteger datos de tarjetas que para beneficiarse de tarjetas de crédito de las empresas al tiempo que les da poderes ejecutivos de castigo a través de un sistema de cumplimiento obligatorio que no tiene supervisión. "Es como si Visa y MasterCard fueran gobiernos", dijo Stephen Cannon, un abogado que representa a los McCombs. "¿De dónde obtienen la autoridad para ejecutar un sistema de multas y sanciones contra los comerciantes? ... Los McCombs afirman que el sistema PCI es menos un sistema para proteger los datos de las tarjetas de los clientes que un sistema para recaudar ganancias para las compañías de tarjetas a través de multas y multas. Visa y MasterCard imponen multas a los comerciantes, incluso

cuando no hay ninguna pérdida por fraude, simplemente porque las multas "son rentables para ellos", dicen los McCombs"[78].

Por ejemplo, Heartland tuvo que pagar US$139 millones a las compañías de tarjetas de crédito y en honorarios legales cuando se incumplió[79].

Además, dado que Visa y Mastercard tienen el 80% de la cuota de mercado[80], los minoristas y restaurantes, etc. no tienen otra opción, tienen que usar Visa y Mastercard y, por lo tanto, su sistema PCIDSS.

Tal como lo señaló la cadena Michaels (con 1,000 tiendas), el consejo de PCIDSS está configurado para que las compañías de tarjetas de crédito y los bancos retengan todo el poder sobre los mandatos, multas y todo lo demás conectado a PCI. Debido a esto, los mandatos no representan lo que es la "mejor" seguridad, sino lo que es mejor para las compañías de tarjetas de crédito y sus socios de instituciones financieras. . . No es un cuerpo de estándares de la industria. . . Todo esto surge de las reglas que inicialmente crecieron de un monopolista de tarjetas que no tenemos más remedio que hacer negocios o arriesgar la pérdida de una gran parte de nuestro negocio. Sería imposible para un minorista como Michaels sobrevivir sin tomar Visa. Así que, al igual que otros minoristas, nos tragamos las decenas de millones que hemos gastado para cumplir con PCI, en muchos casos gastados innecesariamente, lo que reduce la rentabilidad y aumenta los costos de todo lo que vende el comerciante"[81].

La Federación Nacional de Minoristas de EE. UU., La asociación minorista más grande del mundo que representa "una industria con más de 1.6 millones de establecimientos minoristas en EE. UU., Más de 24 millones de empleados, aproximadamente uno de cada cinco estadounidenses y ventas de $ 4.6 trillones en 2008". La Cámara de Representantes escucha que 'las pautas PCI son onerosas, confusas y cambian constantemente. Muchos minoristas dicen que el cumplimiento básico es como tratar de alcanzar un objetivo que se mueve rápidamente"[82].

Las empresas dominantes establecen un estándar que es difícil y costoso de cumplir

Es difícil y costoso cumplir con PCIDSS ya que incluso una cadena de 4,000 millones de dólares con 1,000 tiendas testificó ante el Congreso de los Estados Unidos: 'Los estándares de seguridad y datos PCI son un conjunto extraordinariamente complejo de requisitos; son muy caros de implementar, confusos para cumplir y, en última instancia, subjetivos tanto en su interpretación como en su aplicación. El programa está plagado de ambigüedad y complejidad"[83].

Una disposición de comercio electrónico que requiere que las partes en una transacción electrónica puedan 'determinar mutuamente los métodos de autenticación apropiados para esa transacción' permite que la ley y las sanciones privatizadas de Visa / Mastercard / American Express continúen como antes y los minoristas / restaurantes tengan pocas opciones ya que casi todos tienen que ofrecer la posibilidad de pagar con Visa / Mastercard / American Express a sus clientes. Por lo tanto, incluso si un restaurante no quería cumplir con el estándar PCIDSS, por lo que no estaba "mutuamente determinado", tiene pocas opciones.

El estándar del sector privado no es lo suficientemente seguro

Como la cadena de tiendas Michaels de US $ 4 mil millones testificó ante el Congreso de los EE. UU .: "PCI declara que todos los datos de las tarjetas de crédito deben estar encriptados. Sin embargo, existe una excepción a este requisito; PCI establece que los datos que viajan a través de una red privada no necesitan ser encriptados. Si bien una red privada es más segura, todavía no elegiría enviar números de

tarjetas de crédito sin cifrar. ¿Por qué? Porque agrega un riesgo innecesario. Sin embargo, las instituciones financieras de las compañías de tarjetas de crédito no aceptan transacciones encriptadas. Nosotros en Michaels hemos pedido, durante los últimos 3 años, la posibilidad de enviar información encriptada al banco. Hasta la fecha, esto no ha sucedido. ¿Por qué es esto un problema? Uno podría preguntarle a los consumidores afectados por la violación de datos de Heartland Payment Systems, o TJX Corporation, por ese asunto. Se ha sugerido que los métodos utilizados en esas infracciones aprovechan este defecto. . . Los delincuentes usaron un `` Caballo de Troya " que leía los datos de la tarjeta de crédito `` en vuelo ". Estos no son los datos almacenados de los que hablé anteriormente, sino los números que fluían por el canal de comunicación para su aprobación. Una razón por la que los ladrones pudieron capturar esta información es porque no estaba encriptada. Si se hubiera cifrado, lo más probable es que no hubieran podido leer los datos"[84].

En 2010, más de un año después de que se planteara este problema en una audiencia en el Congreso de los EE. UU., esto seguía siendo motivo de preocupación en un artículo que analizaba la violación masiva de Heartland cuando los piratas informáticos accedieron a un números de 130 millones de tarjetas de crédito: "Una debilidad potencial radica en el hecho de que los datos debe descifrarse para pasar del sistema de Heartland a Visa y MasterCard, ya que las compañías de tarjetas de crédito solo aceptan datos no cifrados"[85].

Además, existe la preocupación de que el PCIDSS no sea lo suficientemente seguro. Por ejemplo, al Comité de Seguridad Nacional de la Cámara de Representantes de los EE. UU. Le preocupaba que "varias empresas conocidas hayan sufrido infracciones de datos masivas en sus redes informáticas internas, lo que da como resultado el compromiso de los datos sensibles de los clientes. Los delincuentes que perpetraron estas intrusiones atacaron la información de la cuenta de la tarjeta de crédito y débito que tenían los comerciantes o los procesadores de datos de terceros como resultado de transacciones minoristas. . . Sabemos que un porcentaje de los cargos fraudulentos y las empresas ilícitas de estas actividades se utilizan para financiar actividades terroristas en todo el mundo."[86] El Presidente de este Comité" inició una investigación para determinar si los estándares PCI han sido efectivos para reducir el delito cibernético. Los resultados de esta investigación sugieren que los estándares PCI son de fuerza y efectividad cuestionables"[87].

"El esfuerzo para cumplir con PCI es un desafío desalentador para los comerciantes cuya competencia central es la venta de mercancías en lugar de experiencia en seguridad. El costo para los comerciantes más grandes puede ascender a $ 18 millones al año. Muchos creen que si completan esta ardua tarea, serán recompensados con un sistema seguro. Pero la investigación del comité confirma lo que muchos analistas han sabido durante años. En palabras de una compañía de tarjetas de crédito, el pleno cumplimiento del estándar PCI no garantiza que el comerciante o proveedor no sea víctima de una violación de datos.

Tomemos como ejemplo la violación de datos del año pasado de Hannaford Brothers Company. Los hackers instalaron un código malicioso en los servidores de cada una de las tiendas de la cadena Hannaford. El malware intercepta los datos almacenados en la banda magnética de las tarjetas de pago a medida que los clientes los utilizan en el mostrador de caja. Hannaford recibió la certificación de que cumplían con PCI el 28 de febrero de 2008. Pero el 27 de febrero de 2008, según los documentos obtenidos por el comité, se notificó a Hannaford que varios números de tarjetas de crédito de su red fueron robados y utilizados en el mercado negro. En otras palabras, Hannaford estaba siendo certificada como compatible con PCI, mientras que una intrusión ilegal en su red estaba en progreso"[88].

La Federación Nacional de Minoristas de EE. UU., la asociación minorista más grande del mundo, señaló en una audiencia de la Cámara de Representantes de los EE.UU. que "PCI es poco más que un

parche elaborado. . . " Los protocolos PCI han requerido que muchos comerciantes eliminen los buenos programas existentes de seguridad de datos y los reemplacen con diferentes programas de seguridad que cumplen con las reglas PCI que no son necesariamente mejores. Incluso las empresas que han sido certificadas como compatibles con PCI se han visto comprometidas.

Desafortunadamente, los incentivos económicos para las compañías de tarjetas para remediar estos defectos en su sistema han disminuido. A nuestro sector le parece que las compañías de tarjetas de crédito están algo menos interesadas en mejorar sus productos y procedimientos que en reasignar sus costos de fraude. Desde nuestro punto de vista, si retira las capas de PCI, lo verá como lo que realmente es, una herramienta para desplazar el riesgo de los balances de los bancos y las tarjetas de crédito y colocarlo en otros. Es su sistema de tarjeta de pago, y los minoristas, como consumidores, son solo usuarios de su sistema"[89].

Antes de aceptar estas reglas de autentificación electrónica que continúan permitiendo el sistema PCI, ¿han consultado los gobiernos a los minoristas, a los restaurantes / a sus asociaciones industriales, etc.?

Whatsapp

La Oficina del Comisionado de Privacidad de Canadá investigó Whatsapp y su informe de 2013 encontró[90] que:

> • Los mensajes de confirmación de la cuenta de WhatsApp se estaban enviando a través de puertos de tráfico web ordinarios, supuestamente sin cifrado ni protecciones. La ausencia de medidas de seguridad apropiadas, mensajes de confirmación y cualquier información personal adjunta al mismo corría el riesgo de ser interceptada. Una vez interceptado, se puede usar un número de confirmación para acceder y recibir los mensajes de un usuario y / o cualquier otra información personal enviada al número programado '
>
> • 'En el momento en que se inició nuestra investigación, los mensajes enviados usando la aplicación no fueron encriptados. Como tal, los mensajes enviados y recibidos con la aplicación corrían el riesgo de intercepción, especialmente cuando un usuario elegía usar el servicio a través de redes Wi-Fi no protegidas. En el curso de nuestra investigación confirmamos que los mensajes enviados entre los usuarios de la aplicación no eran seguros. Incluso en los casos en que se enviaron datos a través de puertos utilizados para comunicaciones https seguras (SSL / TLS), los datos personales, incluido el contenido de los mensajes de los usuarios y los números de teléfono, fueron claramente visibles. . . En sus representaciones en nuestra oficina, WhatsApp confirmó que los mensajes enviados y recibidos usando la aplicación no estaban encriptados, lo que confirma la necesidad de introducir salvaguardas para garantizar la seguridad de los mensajes instantáneos y cualquier otra información personal adjunta a esos mensajes. En respuesta parcial a nuestras preocupaciones, en septiembre de 2012, WhatsApp comenzó a agregar cifrado de protocolo a su servicio de mensajería móvil. Si se aplica correctamente, el cifrado de extremo a extremo salvaguardaría adecuadamente los mensajes de escuchas o intercepciones. '

Uber

Uber almacenó información del consumidor en un servicio de almacenamiento en la nube de terceros proporcionado por Amazon Web Services ("AWS") llamado Amazon Simple Storage Service (el "Amazon S3 Datastore"). Uber almacena en el Amazon S3 Datastore una variedad de archivos que contienen información personal confidencial, incluyendo copias de seguridad parciales y completas de las bases de datos de Uber. Estas copias de seguridad contienen una amplia gama de información personal de Rider and Driver, que incluye, entre otras cosas, nombres, direcciones de correo electrónico, números de teléfono, números de licencia de conducir y registros de viaje con información de geolocalización precisa.[91]

Uber no requirió autentificación de múltiples factores en el Almacén de datos de Amazon S3[92]. Como resultado de estas y otras fallas, "intrusos accedieron varias veces al almacén de datos de Amazon S3 de Uber utilizando claves de acceso que los ingenieros de Uber habían publicado en GitHub, un sitio de código compartido utilizado por los desarrolladores de software. Primero, alrededor del 12 de mayo de 2014, un intruso accedió al Almacén de datos Amazon S3 de Uber utilizando una clave de acceso que se publicó públicamente y otorgó privilegios administrativos completos a todos los datos y documentos almacenados en el Almacén de datos Amazon S3 de Uber (la "brecha de datos 2014"). El intruso accedió a un archivo que contenía información personal sensible perteneciente a Conductores de Uber, incluidos más de 100,000 nombres no cifrados y números de licencia de conducir, 215 nombres no encriptados y los números de cuenta bancaria y enrutamiento nacional, y 84 nombres no cifrados y números de Seguridad Social[93].

Presumiblemente, Uber enviará información personal confidencial (y copias de seguridad parciales de las bases de datos de Uber) al servicio de almacenamiento en la nube de Amazon para que sean "partes en una transacción electrónica" y estén cubiertas por las reglas de comercio electrónico propuestas, ver más arriba.

Después de **esta infracción de 2014**, el Fiscal General de Nueva York exigió a Uber que cifrara la información de ubicación basada en GPS cuando estaba en tránsito y la adopción de autentificación de factores múltiples, o metodologías de control de acceso protectoras similares[94]. Como las copias de seguridad de la base de datos Uber incluían información de geolocalización[95] y Uber respaldando sus datos en la nube de Amazon son presumiblemente "partes de una transacción electrónica" (ver arriba), entonces el requisito de Nueva York de que esto se encripte parece ser la intervención del gobierno (asumiendo que la 'Parte' se define para incluir a los gobiernos subnacionales[u]) para establecer un estándar de rendimiento y evitar que Uber y Amazon determinen el método de autenticación apropiado para esta transacción. Por lo tanto, este requisito de Nueva York no estaría permitido en virtud de las propuestas de comercio electrónico (a menos que sea la única categoría permitida como excepción en algunas propuestas de comercio electrónico).

Luego, entre el 13 de octubre de **2016** y el 15 de noviembre de 2016, los intrusos ingresaron al Almacén de datos Amazon S3 de Uber utilizando una clave de acceso AWS que se envió a un repositorio privado de GitHub ("la brecha de datos de 2016"). Uber otorgó a sus ingenieros acceso a los repositorios GitHub de Uber a través de las cuentas GitHub individuales de los ingenieros, a las que generalmente acceden los ingenieros a través de direcciones de correo electrónico personales. Uber no tenía una política que prohibiera a los ingenieros reutilizar credenciales, y no requería que los ingenieros habilitaran la autenticación de múltiples factores al acceder a los repositorios GitHub de Uber. Los intrusos que cometieron la violación de 2016 dijeron que accedieron a la página de Uber GitHub usando contraseñas que anteriormente estaban expuestas en otras violaciones de datos grandes, y descubrieron la clave de acceso de AWS que usaban para acceder y descargar archivos del Almacén de datos de Amazon S3 de Uber. Los intrusos descargaron dieciséis archivos que contenían información personal no cifrada del consumidor relacionada con pasajeros y conductores de EE. UU., incluidos aproximadamente 25.6 millones de nombres y direcciones de correo electrónico, 22.1 millones de nombres y números de teléfonos móviles y 607,000 nombres y números de licencia de conducir[96].

Si los empleados de Uber que acceden a los repositorios de GitHub son "partes en una transacción electrónica" (que parecen lo son), entonces el requisito de Nueva York para la autentificación

[u] Se supone a lo largo de esta nota que los gobiernos subnacionales están estrictamente sujetos a estas reglas de comercio electrónico. Si esto es realmente el caso depende del texto en el acuerdo comercial.

multifactorial parece ser la intervención del gobierno (suponiendo que 'Parte' incluye a los gobiernos subnacionales) para establecer un estándar de rendimiento y evitar que los empleados de Uber y Github determinen el método de autentificación apropiado para esta transacción. Por lo tanto, este requisito de Nueva York no estaría permitido en virtud de las propuestas de comercio electrónico (a menos que sea la única categoría permitida como excepción en algunas propuestas de comercio electrónico).

Seguridad de oleoductos

Los ciberataques ya están ocurriendo en oleoductos y gasoductos y sus empresas relacionadas, algunos ya han tenido éxito y los reguladores ya están pidiendo estándares obligatorios. Si los gobiernos no pueden exigir un cierto nivel de seguridad para las transacciones electrónicas (debido a estas reglas de comercio electrónico en los acuerdos comerciales), esto puede dejar a los oleoductos y gasoductos, etc., vulnerables a ataques cibernéticos.

Los ataques cibernéticos en los oleoductos ya están ocurriendo

Los oleoductos y gasoductos ya son a menudo blanco de ciberataques. P.ej:

• el gasoducto trans-Alaska tiene un promedio de 22 millones de ataques cibernéticos por día y "La tasa de ataques cibernéticos se ha duplicado en los últimos cinco años"[97]. "El año pasado, el Departamento de Seguridad Nacional y el FBI emitieron una advertencia de que sofisticados ataques cibernéticos se han dirigido al sector energético de los EE. UU.

El Servicio de Investigación del Congreso (CRS)[v] de EE.UU. en un informe de 2012 sobre la seguridad de los oleoductos observó[98] que:

> • 'Más de 500,000 millas de oleoductos de gran volumen reúnen y transportan gas natural, petróleo y otros líquidos peligrosos en los Estados Unidos. Además, casi 900,000 millas de tuberías de distribución más pequeñas entregan gas natural a negocios y hogares. Esta vasta red de tuberías es integral para el suministro de energía de los EE.UU. y tiene enlaces a plantas de energía, refinerías, aeropuertos y otras infraestructuras críticas. Si bien los oleoductos son un medio de transporte eficiente y fundamentalmente seguro, muchos transportan materiales volátiles, inflamables o tóxicos con el potencial de causar daños públicos y daños al medio ambiente. En consecuencia, los sistemas de oleoductos han llamado la atención como posibles objetivos para el terrorismo u otras actividades maliciosas ".
>
> • la red de gasoductos y tuberías de líquidos peligrosos de los EE.UU. es vulnerable a los ciberataques. En particular, la infiltración cibernética de los sistemas de control de supervisión y adquisición de datos (SCADA)[w] podría permitir a los "hackers" exitosos interrumpir el servicio de tuberías y causar derrames, explosiones o incendios, todo desde ubicaciones remotas.

---

[v] El CRS fue establecido por la legislación en 1914 y realiza investigaciones para los miembros del Congreso de EE.UU. como parte de la Biblioteca del Congreso (una agencia de la rama legislativa del gobierno de EE. UU.), https://www.loc.gov/crsinfo/about/ , https://www.loc.gov/crsinfo/about/history.html , https://www.loc.gov/about/general-information/ .

[w] Los sistemas de control de supervisión y adquisición de datos (SCADA) son control industrial basado en software sistemas utilizados para monitorear y controlar muchos aspectos de la operación de la red para ferrocarriles, plantas y redes eléctricas, sistemas de agua y alcantarillado y redes de tuberías. En el sector de los oleoductos, los sistemas SCADA recopilan datos (por ejemplo, presión de línea) en tiempo real de sensores a lo largo de una red de tuberías,mostrar esos datos a operadores humanos en salas de control de red remotas. Estos operadores pueden enviar comandos computarizados desde estaciones de trabajo SCADA para controlar geográficamente dispersos

• En marzo de 2012, el Departamento de Seguridad Nacional (DHS) informó las continuas intrusiones cibernéticas entre los operadores de gasoductos de gas natural de EE.UU. estas intrusiones han aumentado la preocupación del Congreso sobre la ciberseguridad en el sector de los ductos de los EE. UU.

• "Los cambios en las redes informáticas en los últimos 20 años, los piratas informáticos más sofisticados y la aparición de software malicioso especializado han hecho que las operaciones SCADA sean cada vez más vulnerables a los ciberataques. Esto se debe a las mejoras en la tecnología informática y al desarrollo continuo de comunicaciones y aplicaciones de sistemas de control basados en Internet, los sistemas SCADA se han vuelto mucho más vulnerables a intrusiones y manipulaciones externas. Las debilidades de seguridad específicas de SCADA incluyen la adopción de tecnologías de sistemas de control estandarizados con vulnerabilidades conocidas, mayor conexión a redes externas, conexiones de comunicación inseguras

• 'tales ataques cibernéticos podrían interrumpir potencialmente el servicio del ducto, dañar el equipo de tuberías (por ejemplo, con una presión excesiva) o causar una liberación peligrosa de productos de las tuberías al medio ambiente. Incluso si un hacker no intenta dañar o interrumpir el sistema de tuberías, al obtener acceso o controlar el sistema SCADA, el intruso podría causar daños graves involuntariamente.

• "Los problemas relacionados con SCADA fueron una causa principal o un factor que contribuyó en varios accidentes recientes que tuvieron consecuencias catastróficas". El informe detalla los problemas relacionados con SCADA que han matado a 11 personas, derramado 819,000 galones de crudo en un río y causado $ 45 millones en daños, etc. Si bien estos fueron accidentes, dan una idea de las consecuencias de un ciberataque exitoso en los sistemas SCADA utilizados en las tuberías.
• Recientemente ha habido una serie coordinada de intrusiones cibernéticas dirigidas específicamente a los sistemas informáticos de oleoductos de EE. UU.
• un video de Al Qaeda obtenido en 2011 por el Buró Federal de Investigaciones (FBI, por sus siglas en inglés) supuestamente pedía una "jihad electrónica" contra la infraestructura crítica de los EE. UU.
• "Si el interés propio de los operadores de oleoductos es suficiente para generar el nivel de ciberseguridad apropiado para un sector de infraestructura crítica, está abierto al debate. Si el Congreso llega a la conclusión de que las medidas voluntarias actuales son insuficientes para garantizar la ciberseguridad de los oleoductos, puede decidir dar instrucciones específicas a la CST para desarrollar regulaciones y proporcionar recursos adicionales para apoyarlas '.

Jim Guinn, dirige la empresa Accenture de seguridad cibernética para las industrias de energía, servicios públicos, productos químicos, metales y minería. Guinn dijo que, en lo que a él respecta, las posibles consecuencias de un ataque cibernético mayor deberían ser lo principal para mantener despiertos a los ejecutivos de energía por la noche, si es que aún no lo estan.

"Podría ser desde un derrame, hasta la pérdida del control de la planta, la explosión, la pérdida de vidas", dijo. "No sería diferente a perder una plataforma en el Golfo de México o en el Mar del Norte". . . . "La realidad es que, mientras estos activos estén conectados a las redes y se administren de la manera

---

equipo de oleoductos como válvulas, bombas y estaciones de compresión. El sistema SCADA proporciona información continua sobre las condiciones a lo largo de una tubería, generando alarmas de seguridad cuando las condiciones de funcionamiento caen fuera de los niveles prescritos '.

en que lo están hoy, existe una amenaza real de que puedan ser manipulados de manera malintencionada", dijo Guinn. "Es solo el desafortunado mundo en el que vivimos" "[99].

James Steffes, vicepresidente ejecutivo de Direct Energy Inc., que distribuye electricidad, y también utiliza Energy Services, dijo: "A medida que nos volvemos más digitales, vamos a ver más y más amenazas", dijo Steffes. "Las malas personas tratando de hacer cosas malas" continuarán siendo una amenaza para los servicios basados en la web. "Nunca podremos quitar nuestros ojos de esta bronca porque es solo la naturaleza de un entorno digital".

Los sistemas de gas natural y las redes eléctricas se han ido convirtiendo cada vez más en electrónicos a medida que se actualiza la infraestructura obsoleta. Los hackers están desarrollando una inclinación por los ataques a la infraestructura energética debido al impacto que el sector tiene en la vida de las personas, dijo Scott Coleman, director de mercadeo y gestión de productos de Owl Cyber Defense, que trabaja con los productores de petróleo y gas. Si un hacker cierra una subestación eléctrica, 20,000 personas pueden verse afectadas, dijo.[100]

La piratería sobre ESG

En abril de 2018, el sistema de intercambio electrónico de datos que procesa digitalmente transacciones de clientes para una importante red de oleoductos en los Estados Unidos sufrió un ataque cibernético y se cerró[101]. La empresa de datos cuyos sistemas electrónicos del Grupo de Servicios de Energía (**ESG)** fue hackeada ayudan a los operadores de tuberías a acelerar el seguimiento y la programación de los flujos de gas. La compañía también suministra precios de electricidad y modelos de demanda de los que los proveedores minoristas de energía dependen para facturar a hogares y negocios, y determinar cuánta oferta asegurar para los clientes en los mercados mayoristas[102]. Los sistemas electrónicos que fueron atacados en los recientes ataques cibernéticos ayudan a los clientes a comunicar sus necesidades con los operadores a través de un intercambio de documentos de computadora a computadora, como contratos y facturas"[103].

"Las plataformas de ESG se utilizan" en todo el país "para las transacciones de energía, dijo Harris. "Nadie que esté usando la plataforma de precios ha podido usarla para fijar los precios desde el jueves pasado. Habrá facturas estimadas para algunas de las compañías más grandes ". A falta de los modelos de demanda de Energy Services, los proveedores de energía minorista también podrían quedarse cortos (o largos) en suministros de energía para sus clientes y pueden recurrir a comprar y vender. en los mercados spot para reequilibrar. Eso podría generar grandes oscilaciones en los precios mayoristas si el sistema de Energy Services permanece inactivo durante semanas, dijo Harris. . . Los minoristas de electricidad de Texas "han estado proporcionando soluciones manuales mientras esperan que ESG regrese al servicio"[104]. Esto dificultó las operaciones de al menos cuatro compañías de gas natural[105] con cinco operadores de oleoductos que dijeron que sus sistemas de comunicaciones electrónicas de terceros se cerraron debido a la piratería[106].

"Aunque el ataque cibernético no interrumpió el suministro de gas a los hogares y empresas de EE.UU., subraya que las compañías de energía, desde los proveedores de energía hasta los operadores de oleoductos y los perforadores de petróleo, son cada vez más vulnerables al sabotaje electrónico. También mostró cómo incluso un ataque menor puede tener efectos dominantes, lo que obliga a los servicios públicos a advertir sobre demoras en la facturación y dificulta a los analistas y comerciantes predecir un informe clave del gobierno sobre las existencias de gas"[107].

Steve Grobman, director de tecnología de la compañía de seguridad cibernética McAfee Security, señaló que 'ESG puede que ni siquiera haya sido el objetivo. . . En cambio, el objetivo final de los atacantes pudo haber sido encontrar formas de violar los clientes de ESG. "El nivel de robustez en los sistemas de seguridad de las compañías de petróleo y gas los convierte en objetivos difíciles", dijo Grobman en una entrevista el miércoles. "Buscar objetivos más flexibles, como las empresas de comunicaciones electrónicas, es mucho más fácil de ejecutar"[108]. Por eso es importante que el nivel de seguridad de las transacciones electrónicas para infraestructura crítica como tuberías y redes eléctricas sea lo suficientemente alto y no solo para el sector privado que, como lo ha demostrado ESG, puede elegir un nivel de seguridad demasiado débil, dadas las externalidades (véase más arriba).

Regulaciones que abordan la seguridad del oleoducto

Algunos países han decidido que las normas voluntarias de seguridad en el sector de los oleoductos son insuficientes y, en su lugar, han ordenado la seguridad mediante reglamentos. Por ejemplo, "en 2010, el Consejo Nacional de la Energía de Canadá ordenó las normas de seguridad para las tuberías jurisdiccionales canadienses de petróleo y gas natural, algunas de las cuales son tuberías transfronterizas que sirven a los mercados de exportación en los Estados Unidos. Muchas empresas operan oleoductos en ambos países. Al anunciar estas nuevas reglamentaciones, la junta declaró que había considerado adoptar las normas de ciberseguridad existentes como "guía" en lugar de una norma aplicable, pero "teniendo en cuenta la importancia crítica de la protección de la infraestructura energética", la junta decidió adoptar la Norma en las regulaciones.'[109]

El CRS de EE.UU. señala que "la decisión de Canadá de regular la seguridad del oleoducto puede plantear interrogantes sobre por qué Estados Unidos no lo ha hecho"[110].

Preocupaciones de los reguladores

Mientras que los Estados Unidos todavía tienen seguridad cibernética voluntaria/autorregulación de los gasoductos, ha habido un aumento en los llamados a la regulación obligatoria (incluso desde el ataque ESG). Por ejemplo, la Casa Blanca, los representantes del Congreso y los reguladores han expresado su preocupación por estos riesgos de ciberseguridad y han propuesto regulaciones obligatorias para abordarlos. Por ejemplo:

• 'Una propuesta de la Casa Blanca de abril de 2011 y la Ley de seguridad cibernética de 2012 (S. 2105) obligarían a las regulaciones de seguridad cibernética para sectores de infraestructuras críticas de propiedad privada, como los oleoductos.'[111]

• En respuesta a la piratería sore ESG:

  o "'Estos ataques son un llamado de alerta que debe abordarse como una prioridad para nuestra infraestructura energética obsoleta", dijo en una declaración enviada por correo electrónico el congresista Robert Latta, un republicano de Ohio que sirve en el Comité de Energía y Comercio de la Cámara. 5. "Los malos actores están buscando cualquier forma de debilitar el sector energético estadounidense"[112].
  o Representante James Langevin, copresidente del bipartidista Congressional Cybersecurity Caucus dijo: "Mientras seguimos aprendiendo más sobre los incidentes cibernéticos que afectan a los sistemas empresariales de oleoductos, incluidos los de los Energy Transfer Partners, ya debe quedar claro que cada empresa enfrenta el riesgo de ciberseguridad '[113].

• En junio de 2018, dos reguladores estadounidenses (un republicano y un demócrata[114]) pidieron la autoridad legal, los recursos y el compromiso de implementar normas obligatorias para abordar la seguridad del gasoducto[115].

Plataformas de negociación de acciones inseguras

Un consultor de seguridad encontró que casi todas las 40 principales plataformas de negociación de acciones en línea que investigó tenían algún tipo de vulnerabilidad[116]. Por ejemplo:

• El 64% de las aplicaciones de escritorio que Hernández examinó transmitieron al menos algunos datos, por ejemplo, contraseñas, balances, carteras e información personal sin cifrar,
• La mayoría de las plataformas web examinadas no permitieron la autentificación de dos factores por defecto

Exigir que estas plataformas (que se usan para grandes cantidades de dinero) utilicen encriptación para transmitir información personal confidencial o autentificación obligatoria de dos factores (como hacen algunos gobiernos para la banca en línea, ver más arriba) no estaría permitido en las propuestas de comercio electrónico anteriores (a menos que sea la única categoría permitida como excepción en algunas propuestas de comercio electrónico).

Facebook envía datos a creadores de aplicaciones sin encriptar

Durante años, Facebook envió los datos del usuario sin cifrar a la persona o empresa que creó la aplicación app: "cada vez que el usuario carga la aplicación, Facebook le envía una carga de datos básicos del usuario para facilitar el funcionamiento de la aplicación (se pueden solicitar datos adicionales) por separado cuando sea necesario). Durante años, estas transmisiones incluso se realizaron sin cifrar, hasta que Facebook requirió que las aplicaciones se comuniquen con su servicio a través de una conexión segura."117 Presumiblemente Facebook y el creador de la aplicación serían 'partes de una transacción electrónica', por lo que un gobierno quería información personal del usuario sensible (por ejemplo, información de salud o de identificación) que se enviará encriptada, que requiere que esto no esté permitido por las propuestas de comercio electrónico anteriores (a menos que sea la única categoría permitida como excepción en algunas propuestas de comercio electrónico).

Servicios de análisis de terceros que usan http no cifrado

'Los scripts de reproducción de sesión son provistos por servicios analíticos de terceros diseñados para ayudar a los operadores de sitios a comprender mejor cómo los visitantes interactúan con las propiedades de su web e identificar páginas específicas que son confusas o rotas. Como su nombre lo indica, los scripts permiten a los operadores recrear sesiones de navegación individuales. Cada clic, entrada y desplazamiento se pueden grabar y luego reproducir. . .

"La recopilación del contenido de la página por parte de scripts de reproducción de terceros puede provocar que información delicada, como condiciones médicas, detalles de tarjetas de crédito y otra información personal mostrada en una página, se filtre a terceros como parte de la grabación", escribió Steven Englehardt , un estudiante de doctorado en la Universidad de Princeton,. "Esto puede exponer a los usuarios al robo de identidad, las estafas en línea y otros comportamientos no deseados. Lo mismo es cierto para la recopilación de las entradas de los usuarios durante los procesos de registro y registro mismo".

Englehardt instaló scripts de reproducción en seis de los servicios más utilizados y descubrió que todos exponían los momentos privados de los visitantes en diversos grados. Durante el proceso de creación de una cuenta, por ejemplo, los scripts registraron al menos una entrada parcial escrita en varios campos. Las secuencias de comandos de FullStory, Hotjar, Yandex y Smartlook fueron las más intrusivas

porque, de forma predeterminada, registraron todas las entradas ingresadas en campos para nombres, direcciones de correo electrónico, números de teléfono, direcciones, números de seguridad social y fechas de nacimiento. . .

Otro ejemplo: la página de cuenta para la tienda de ropa Bonobos filtró detalles completos de la tarjeta de crédito, carácter por carácter, tal como fueron escritos a FullStory. Para colmo de males, Yandex, Hotjar y Smartlook ofrecen cuadros de mandos que utilizan HTTP sin cifrar cuando los editores suscritos reproducen las sesiones de los visitantes, incluso cuando las sesiones originales estaban protegidas por HTTPS.'[118]

Presumiblemente, el uso de servicios analíticos de terceros por una compañía como la farmacia Walgreens sería 'partes de una transacción electrónica' y dado que se enviaba sin cifrar (ver arriba), si un gobierno imponía requisitos de encriptación para la transmisión de información personal sobre su residentes (como requiere Massachusetts), o un número de seguro social (como lo requieren California y Minnesota) ingresar al sitio web de Walgreens, esto sería una interferencia gubernamental ilegal según las propuestas de comercio electrónico anteriores (a menos que sea la única categoría permitida como excepción en algún comercio electrónico propuestas o una de las excepciones difíciles de usar, ver abajo).

Informes de una Compañía de crédito (Equifax)

"El 7 de septiembre de 2017, la masiva información de la compañía de crédito Equifax reveló públicamente una violación de los sistemas informáticos de la empresa, que se describió como" uno de los mayores riesgos para la información sensible personal en los últimos años ", lo que expuso datos de más de 145 millones de estadounidenses a delincuentes piratas informáticos. La compañía indicó que un vasto tesoro de datos confidenciales, incluidos números de seguridad social, números de tarjetas de crédito, números de pasaportes y licencias de conducir, podría haberse visto comprometido. El incidente fue la quinta violación de datos reciente de Equifax o sus subsidiarias que puso en peligro la información personal de los estadounidenses"[119].

Esta no fue la única vez que Equifax tuvo problemas de ciberseguridad. Por ejemplo, durante el mismo período:

• "Equifax informó en febrero de 2017 que un problema técnico" comprometía la información crediticia de algunos consumidores que utilizaban servicios de protección contra robo de identidad de un cliente"[120].
• 'En julio, 14 sitios web orientados al público operados por Equifax tenían certificados caducos, errores en la cadena de certificados u otros problemas de seguridad web'[121].
• Para lidiar con el incumplimiento, 'Equifax creó un sitio web, EquifaxSecurity2017.com, e instruyó a los consumidores a visitar para determinar si sus datos se vieron comprometidos'; sin embargo 'según los expertos en seguridad cibernética consultados por el personal de la Senadora Warren, EquifaxSecurity2017.com tuvo vulnerabilidades de seguridad importantes :. . que el diseño y la dirección web del sitio facilitaron a los demás suplantar y recopilar la información de los consumidores. Para demostrar esto, un experto en ciberseguridad creó un sitio web con una dirección web casi idéntica: www.securityequifax2017.com, que se parecía tanto al enlace del sitio web real de Equifax que dirigió a los consumidores al sitio falso varias veces. Además, los expertos consultados por el personal de la Senadora Warren identificaron muchos otros defectos técnicos en el diseño del sitio web. Informaron que el sitio web estaba configurado para ejecutarse en una instalación común de Wordpress, que no incluía las características de seguridad necesarias para proteger la información delicada que los consumidores enviaban y que el certificado de seguridad de Transport Layer Security tampoco realizaba las comprobaciones de revocación adecuadas. lo que habría asegurado que estaba

estableciendo una conexión segura y protegiendo los datos de un usuario. Y luego, el 12 de octubre, Equifax se vio obligado a eliminar una página web donde las personas podían aprender cómo obtener un informe crediticio gratuito cuando un analista de seguridad informaba que los visitantes del sitio estaban siendo atacados por anuncios comerciales emergentes maliciosos. Después de no proteger los datos de los consumidores, Equifax posteriormente creó un sitio web que puso a sus clientes en un peligro aún mayor"[122].

Equifax 'tiene' datos sobre aproximadamente mil millones de personas 'y' administra grandes cantidades de datos únicos ',' pero su ciberseguridad inadecuada 'pone a millones en riesgo de robo de identidad por el resto de sus vidas'[123]. Equifax priorizó el crecimiento de sus ganancias, pero no parecen dar prioridad a la seguridad cibernética."[124] El deseo de las empresas privadas de maximizar los beneficios y, por lo tanto, comportarse de manera que perjudique a los consumidores también se puede ver en cómo Equifax manejó esta falla[125]:

- no hizo pública la falla durante más de un mes (por lo que los hackers pudieron haber utilizado los datos de la tarjeta de crédito robada, etc. durante un mes),
- no reveló el hecho de que también se había accedido a los números de pasaporte,
- cuatro meses después de la falla, solo había notificado (por teléfono o por escrito) a 2,5 millones de los 145 millones de consumidores afectados (el resto tenía que enterarse iendo al sitio web de Equifax para averiguarlo por sí mismos),
- Le cobró a los consumidores congelar su crédito para lidiar con el problema de posible robo de identidad que la negligencia de Equifax había creado (hasta que hubo una protesta pública) y se benefició de otras maneras descritas en el informe de la violación.

Si bien las propuestas de comercio electrónico anteriores dejan a las "partes" de una transacción electrónica decidir qué tan seguro debe ser, en realidad, los consumidores tienen poco poder para influir en la seguridad con que las empresas privadas, como los bancos y las agencias de informes crediticios, manejan sus datos. Por ejemplo, las preocupaciones del consumidor sobre el incumplimiento de Equifax fueron particularmente marcadas porque la empresa, junto con las otras dos grandes agencias de informes crediticios, Experian y TransUnion, ocupan un lugar único en el mundo financiero: obtienen y utilizan cantidades masivas de datos en millones de consumidores, pero los consumidores tienen poco o ningún poder sobre cómo se recopilan estos datos, cómo se usan o cómo se mantienen seguros"[126].

La senadora estadounidense Elizabeth Warren creó el Buró de Protección Financiera del Consumidor, presidió el Panel de Supervisión del Congreso para el Programa de Alivio de Activos en Problemas (TARP, por sus siglas en inglés) después de la crisis financiera de 2008 y fue profesor de la Facultad de Derecho de Harvard[127]. En febrero de 2018 la Senadora Warren escribió un informe sobre la violación Equifax y encontró[128] que:

- 'La información confidencial perteneciente a más de 145 millones de estadounidenses quedó expuesta como resultado de la violación, uno de los mayores y más importantes lapsos de seguridad de datos en la historia'.
- 'Equifax configuro un sistema defectuoso para prevenir y mitigar los problemas de seguridad de datos. La violación fue posible porque Equifax adoptó medidas débiles de ciberseguridad que no protegían adecuadamente los datos de los consumidores. La empresa no priorizó la ciberseguridad y no siguió los procedimientos básicos que habrían evitado o mitigado el impacto de la violación. Por ejemplo, se advirtió a Equifax de la vulnerabilidad en el software de la aplicación web Apache Struts que se utilizó para infringir su sistema, y se envió un correo electrónico al personal para pedirles que corrijan la vulnerabilidad, pero luego no se confirmaron las correcciones. Las

exploraciones posteriores solo evaluaron parte del sistema de Equifax y no identificaron que la vulnerabilidad de Apache Struts se hubieran remediado.
• Equifax omitió numerosas advertencias de riesgos para datos confidenciales. Equifax tuvo una amplia advertencia de debilidades y riesgos para sus sistemas. Equifax recibió una advertencia específica del Departamento de Seguridad Nacional sobre la vulnerabilidad precisa que los hackers aprovecharon para violar los sistemas de la compañía. La compañía había estado sujeta a varias fallas más pequeñas en los años previos a la infracción masiva de 2017, y varios expertos externos identificaron e informaron debilidades en las defensas cibernéticas de Equifax antes de que ocurriera la violación. Pero la compañía no hizo caso, o no fue capaz de escuchar de manera efectiva, estas advertencias ".
• 'La violación fue posible porque Equifax adoptó medidas débiles de seguridad cibernética que no protegían los datos de los consumidores, un síntoma de lo que parecía ser la baja prioridad que los líderes de la compañía les brindaban a la ciberseguridad. El CEO en el momento de la violación, Richard Smith, declaró que a pesar de las ganancias récord en los últimos años, Equifax gastó solo una fracción de su presupuesto en ciberseguridad, aproximadamente el 3 por ciento de sus ingresos operativos en los últimos tres años. Por el contrario, Equifax pagó casi el doble en dividendos a los accionistas. Los expertos en ciberseguridad consultados por el personal de la Senadora Warren indicaron que una gran empresa que posee datos confidenciales, como Equifax, debería tener múltiples niveles de ciberseguridad. . . A pesar de recopilar datos sobre cientos de millones de estadounidenses sin su permiso, Equifax no adoptó plena y efectivamente ninguna de estas cuatro medidas de seguridad ".
• El informe detalla varias debilidades en la ciberseguridad de Equifax
• 'Equifax y otras agencias de informes crediticios se han aprovechado de los consumidores durante años, recogiendo sus datos sin permiso y obteniendo enormes ganancias sin proteger adecuadamente esos datos. **Estas prácticas no cambiarán sin una legislación federal que obligue a Equifax y a sus pares a poner el énfasis apropiado en la protección de los datos de los consumidores ".**
• 'La legislación federal es necesaria para prevenir y responder a futuros incumplimientos. Equifax y otras agencias de informes crediticios recaban datos del consumidor sin su permiso, y los consumidores no tienen manera de evitar que sus datos sean recopilados y retenidos por la empresa, que estaba más enfocada en sus propios beneficios y crecimiento que en proteger la información personal sensible de millones de personas consumidores. Este incumplimiento y la respuesta de Equifax ilustran la necesidad de una legislación federal que (1) establecer multas apropiadas para las agencias de informes crediticios que permiten infracciones graves de ciberseguridad en sus responsabilidades; y (2) **facultar a la Comisión Federal de Comercio para establecer estándares básicos para garantizar que las agencias de informes de crédito estén protegiendo adecuadamente los datos de los consumidores ".**
• 'El Congreso debe facultar a la FTC para establecer requisitos para medidas fundamentales de ciberseguridad en las agencias de informes crediticios'.

"Hubo infracciones en las tres agencias de informes de crédito en los últimos años, y cientos de millones de consumidores se vieron afectados. Cuando las agencias de informes de crédito recopilan datos personales sin el permiso del consumidor, la carga recae en ellas para proteger esos datos. Si no protegen esos datos, deberían ser castigadas. Las demandas de los consumidores no proporcionan la disuasión adecuada para empresas como Equifax. Mientras que el consumidor promedio recupera menos de $ 2 a través de demandas civiles en respuesta a violaciones de datos, Equifax está realmente configurado para hacer dinero con su reciente incumplimiento. **Si nuestras leyes no castigan a empresas como Equifax por su incapacidad para proteger los datos confidenciales de los consumidores, estas compañías continuarán adoptando normas por debajo del estándar.**

Datos de salud

"Los ataques a la ciberseguridad tienen el potencial de producir resultados desastrosos para los proveedores de servicios de salud y la sociedad en general. Es imperativo que los proveedores de atención médica reconozcan la necesidad de abordar las inquietudes de seguridad cibernética y actuar en consecuencia. . . la información médica es realmente valiosa, especialmente cuando se vende en el mercado negro o se usa en relación con otras actividades ilegitimas o ilícitas"[129].

"Las empresas cada vez abren más sus redes a socios comerciales, contratistas externos (incluidos los proveedores de aplicaciones y almacenamiento en la nube) e incluso a sus clientes. Para abordar completamente su riesgo de robo de datos, debe comprender la red de conexiones hacia y desde sus datos confidenciales. . . ¿Qué datos existen en su infraestructura y qué seguridad existe para proteger los datos en tránsito y en reposo?[130] "Estos terceros contratistas pueden transferir los delicados datos de salud a otros, por lo que la directora gerente de BucklySandler, Rena Mears, dijo. "Las empresas deben entender que administrar el riesgo de los datos no es solo un problema de cumplimiento y contrato, sino un desafío estratégico fundamental en el que los datos personales, la propiedad intelectual y los registros transaccionales deben protegerse **de terceras, cuartas o n partes de riesgo**"[131].

Para hacer esto de manera efectiva, las empresas deberían preguntar a los socios potenciales sobre el cifrado específico de datos de las organizaciones en lugar de solo aceptar las trivialidades genéricas de cifrado[132]. Estas podrían incluir preguntas sobre:

- 'Estado del cifrado de los datos en tránsito desde la base de datos al servidor de aplicaciones
- Estado del cifrado de los datos en tránsito desde el servidor de la aplicación al servidor proxy (servidor HTTP)
- Estado de encriptación de los datos en tránsito desde el servidor proxy al cliente del usuario final
- Estado de cifrado de los datos en tránsito desde los servidores de la API a los clientes del usuario final (iOS, Android, etc.)
- Estado de cifrado de las transferencias de archivos de servidor a servidor[133]

Sin embargo, una encuesta a empresas (en general, no solo a compañías de atención médica) encontró[134]:

- "La mitad de los encuestados (49%) confirma que su organización experimentó una violación de datos causada por uno de sus proveedores"
- '73% de los encuestados ve aumentar el número de incidentes de ciberseguridad que involucran a los proveedores;
- '58% de los encuestados dicen que no pueden determinar si las salvaguardas y las políticas de seguridad de los proveedores son suficientes para evitar una violación de datos; '

Además, "los investigadores descubrieron que una dificultad importante es detectar y mitigar los riesgos relacionados con los socios comerciales porque las organizaciones no tienen los recursos ni los procedimientos para verificar las medidas de seguridad del proveedor"[135].

La Ley de Responsabilidad y Portabilidad de Seguros Médicos (HIPAA) de los EE. UU. No exige que los datos de los pacientes se cifren en tránsito (es meramente direccionable[x]) [136]. Cuando se encuestó a hospitales y médicos de los EE.UU., solo el 68.1% de los proveedores acusiosos y menos de la mitad

[x] Lo que significa que la empresa puede elegir no implementar una especificación direccionable basada en su evaluación, pero "debe documentar el motivo y, si es razonable y apropiado, implementar una medida alternativa equivalente", https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf .

(48.4%) de los proveedores no acusiosos están encriptando datos en tránsito. Esto significa que los proveedores que no están cifrando datos están enviando información de salud protegida y otros datos en forma clara, dejando que tales datos sean susceptibles de ser vulnerados mediante escuchas ilegales, olfateos de paquetes u otros medios. Además, la falta de encriptación significa que los datos pueden ser manipulados en tránsito, por lo tanto, hay poca seguridad de que los datos del remitente sean fieles a los datos del receptor. La alteración de dicha información puede tener un efecto adverso en las operaciones clínicas, las operaciones administrativas y / o la atención del paciente ".[137]
Por ejemplo, un correo electrónico que contiene datos confidenciales (nombre, fecha de nacimiento, sexo e información del Beneficiario de Medicare) cubierto por HIPAA se envió por correo electrónico a otro grupo médico sin encriptación al nivel correspondiente.[138]

Por lo tanto, cuando el sector privado elige el nivel de seguridad de las transacciones electrónicas, a pesar de la frecuencia de las infracciones de datos del paciente y las consecuencias potencialmente graves de salud y privacidad, etc., los proveedores de servicios de salud a menudo no encriptan los datos en tránsito. Además, a pesar de la frecuencia de las violaciones de datos causadas por sus proveedores, las empresas no tienen la capacidad de verificar la ciberseguridad de sus proveedores. Por lo tanto, los gobiernos pueden necesitar regular este sector altamente sensible, sin embargo, si se prohíbe la prohibición de propuestas de comercio electrónico (excepto tal vez para una categoría de transacciones), la capacidad de establecer métodos de autentificación puede no ser posible. Vea a continuación la discusión sobre la adecuación de la excepción de salud habitual en los acuerdos comerciales.

Los reguladores estadounidenses ya saben que las regulaciones existentes son insuficientes

La Comisión Federal de Comercio (FTC, por sus siglas en inglés) del gobierno de los Estados Unidos ha declarado que "se necesitan herramientas adicionales" para establecer los requisitos básicos de ciberseguridad y monitorear el cumplimiento de esas normas por parte de las compañías.[139]

El Buró de Protección Financiera del Consumidor (CFPB) del gobierno de los EE. UU. Afirma que "las leyes federales que son aplicables a la seguridad de datos no se han mantenido al día con los avances tecnológicos y de ciberseguridad ... es imperativo que el Congreso tome medidas para garantizar que el marco regulatorio sea adecuado. "Los desafíos planteados por las amenazas de ciberseguridad".[140]

La Administración Trump 'también participa en las discusiones que el Congreso está teniendo sobre los requisitos de protección de datos personales'[141]

Algunas implicaciones cuando se combinan con otras propuestas de comercio electrónico, etc.

Al considerar las implicaciones potenciales de aceptar las propuestas de autentificación electrónica anteriores, es importante considerar el efecto combinado con otras reglas de comercio electrónico, etc. que se proponen en estas negociaciones comerciales. Por ejemplo, otras disposiciones en el TPP /propuestas en los debates de comercio electrónico de la OMC o en otros acuerdos comerciales incluyen:

- Permitir flujos transfronterizos de datos (incluidas restricciones para exigir que los datos se almacenen localmente). Esto generalmente requiere que el país permita que incluso sus datos confidenciales (p. Ej. Registros sanitarios / financieros / fiscales) se transfieran a cualquier país del mundo (que puede tener excepciones de privacidad insuficientes que

permitan vender los datos a anunciantes / bancos / compañías de seguros que puede negar préstamos / seguros bancarios, etc.)[y]. Combinar esto con las reglas de eauthentificación propuestas arriba significaría que los gobiernos no pueden exigir que estos datos confidenciales sean encriptados mientras están en tránsito hacia estos otros países, ni pueden requerir que sean encriptados mientras se almacenan en estos otros países, etc. Esto dejaría los datos sensible (incluidos detalles de tarjetas de crédito, etc.) vulnerables a ser robados en otros países.

• Restricciones para exigir que las empresas tengan presencia local (como una sucursal / oficina / filial, etc.)[z]. Si Uber no tiene una oficina en el país en cuestión, es muy difícil para ese país hacer cumplir sus leyes (incluida la autentificación electrónica, por ejemplo, para exigir el cifrado) a esa empresa (por ejemplo, para demandarlas en los tribunales nacionales por incumplimiento o para hacer cumplir una multa por no cumplir con el nivel de seguridad requerido en las transacciones electrónicas).

Como señaló un profesor de derecho, "las leyes de privacidad y protección del consumidor doméstico pueden volverse impotentes si no se requiere que las firmas financieras extraterritoriales tengan presencia local. Cuando los datos financieros se guardan "en la nube", la información personal y comercial de las personas está sujeta al régimen de privacidad y protección del consumidor del país que aloja el servidor, especialmente problemático cuando el anfitrión es los EE.UU.[142] "Por lo tanto, es importante considerar el implicaciones para las leyes/políticas de un país, etc. del efecto combinado de las reglas propuestas, no solo la propuesta de autentificación de forma aislada.

Eficacia de las excepciones

Excepción de salud / ambiente

No está claro si las excepciones en materia de salud, medio ambiente y privacidad de las normas de servicios de la OMC[143] se aplicarán a las normas de comercio electrónico propuestas en la OMC. En el TPP, las excepciones de salud, ambiente y privacidad en las reglas de servicios de la OMC se aplican al capítulo de comercio electrónico del TPP, por lo que esto también puede ocurrir en otros TLC.

Sin embargo, esta excepción general de la OMC para la salud, el medio ambiente y la privacidad es difícil de usar debido a todas las pruebas que deben aprobarse para utilizarla. Para 2015, los países habían tratado de utilizar esta excepción (y el equivalente de los productos[144]) en la OMC 44 veces y solo tuvieron éxito una vez, sobre el asbesto[145] (amianto, según su clasificación comercial N.dT.).

Excepción de privacidad

Además, la excepción de privacidad en la OMC[146] es aún más difícil de usar porque tiene una frase adicional que muchos expertos legales creen que se auto cancela: solo puede usarse para leyes / reglamentos que ya cumplen con el Acuerdo (en cuyo caso la excepción no es necesaria). Por lo tanto, si esto se copia en un TLC que tenga las disposiciones de eauthentication anteriores, todavía requiere el

[y] Por ejemplo, ver Briefing 3 en https://www.twn.my/briefings_MC11.htm .

[z] Si bien esto se ha propuesto en la OMC en nombre del comercio electrónico, por ejemplo, véase JOB / GC / 97 / Rev.3 en https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx, en los TLC esto puede a menudo estar en el capítulo de servicios, por ejemplo, Art 10.6 del TPP https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/

cumplimiento de las disposiciones de autentificación electrónica anteriores, por lo que es poco probable que se pueda utilizar como una excepción efectiva.

Defensa prudente

La OMC tiene una defensa prudente que también se copia básicamente en algunos TLC como el TPP[147]. Incluso si las preocupaciones anteriores (por ejemplo, robo de detalles de tarjetas de crédito / robo de identidad, etc.) son motivos "prudenciales" para las reglamentaciones (la prudencia generalmente no está definida en el texto, pero puede ser aclarada en la historia de negociación del tratado comercial), esta defensa prudente o prudencial también tiene una frase que muchos expertos consideran como auto cancelada[148] ("Cuando tales medidas no se ajusten a las disposiciones del Acuerdo, no se utilizarán como un medio para eludir los compromisos u obligaciones del Miembro en virtud del Acuerdo"[149]). Por lo tanto, gobiernos como la Unión Europea (UE) y EE.UU. no han confiado en éllo en algunos de sus TLC. P.ej:

• en el TPP, los reguladores financieros de los EE.UU. no parecían pensar que esta defensa prudente fuera suficiente para permitirles exigir que los datos financieros se almacenaran localmente para poder acceder a ellos a tiempo en una crisis financiera[150] (por ejemplo, para desenrollar las posiciones de Lehman Brothers) cuando colapsó y los datos se guardaron en Hong Kong pero los sistemas de TI se apagaron y el personal de TI se fue[151]), aunque se aplica al capítulo de comercio electrónico, insistieron en excluir explícitamente los datos financieros de la prohibición de requerir datos para ser almacenado localmente en el capítulo de comercio electrónico del TPP[aa].

• En algunos TLC de la EU, como el TLC Canadá-UE (CETA)[152] y el Artículo 104 del EPA UE-CARIFORUM, la segunda sentencia de cancelación automática de la defensa prudencial del AGCS ha sido eliminada porque presumiblemente esos gobiernos pensaban que hacía ineficaz a la excepción.[153]

Otras excepciones

No hay excepciones en las reglas de la OMC (o en los TLC que ha revisado este autor) para los derechos de los consumidores más ampliamente o para la reducción de eficiencia/costos, etc., que son algunas de las razones por las que los gobiernos han impuesto estándares para las transacciones electrónicas.

Conclusión

EN tan solo algunas horas de búsqueda en línea un investigador que no es experto en ciberseguridad ha encontrado:

1) empresas privadas que tienen transacciones electrónicas inseguras (que son o pueden necesitar ser reguladas) en una variedad de situaciones que incluyen:

a) hacer una copia de seguridad de sus datos en la nube,

b) webcam del centro de cuidado infantil para que los padres controlen a sus hijos

c) banca en línea

d) aplicaciones

[aa] El Art. 14.1 del TPP: definición de 'persona cubierta' no incluye una 'institución financiera' o un 'proveedor transfronterizo de servicios financieros de una Parte'

e) servicios analíticos de terceros, etc.

2) el gobierno establece estándares para las transacciones electrónicas en:

a) Banca en línea

b) Uso de tarjeta de crédito

c) Transmisión y uso del número de seguridad social en un sitio web

d) Transferencia de información personal[bb] electrónicamente

e) Cuidado de la salud

f) Acuerdos legales (por ejemplo, por agencias nacionales de protección al consumidor o subnacionales generales) que requieren que las empresas (cuya ciberseguridad inadecuada condujo a violaciones de datos) aumenten su ciberseguridad, por ejemplo encriptando datos en tránsito o usando autenticación multifactorial

Los gobiernos están estableciendo estos estándares para evitar el robo de identidad o el robo de dinero, proteger la privacidad, promover la eficiencia y reducir los costos, etc. Los gobiernos han intervenido con regulaciones en estas áreas porque dejarlo al sector privado ha sido problemático (por ejemplo, el sector privado no voluntariamente adoptó estándares suficientemente seguros, o no ha acordado un sistema común de transacciones electrónicas que aumente la eficiencia y reduzca los costos, etc.). Una de las razones por las cuales los gobiernos han intervenido es debido a las fallas del mercado debido a: i) externalidades asociadas con seguridad insuficiente: los costos de una violación de seguridad son asumidos en gran parte por entidades distintas a la compañía que sufrió la violación debido a una seguridad inadecuada; ii) asimetría de la información: los consumidores no tienen forma de saber si una empresa proporciona la seguridad adecuada.[154]

No está claro cuál es el problema percibido que motivó estas propuestas de comercio electrónico y si los beneficios son tan grandes al restringir/prohibir la capacidad del gobierno de establecer estándares en estas transacciones electrónicas que superan los costos de tener que cancelar estas leyes existentes y restringir el espacio de políticas futuras en un campo de tecnología de cambio rápido.

Incluso cuando se permite una excepción, parece limitarse a "una categoría particular de transacciones" (capítulo sobre comercio electrónico del TPP y la propuesta de firma electronica/ autentificación electrónica de la UE en 2017 en la OMC). Esto parece significar que los gobiernos que acepten tal disposición tendrían que elegir una de las áreas anteriores donde podría establecer estándares (esto ni siquiera considera áreas futuras que pueden necesitar regulación, por ejemplo, información genética (ver a continuación)). Además, las propuestas de comercio electrónico de la UE para TLC y 2018 de la OMC no permiten excepciones, siempre se debe permitir que el sector privado establezca los estándares más bajos que quiera (por ejemplo, para ahorrar costos y así obtener más ganancias).

Como se señaló anteriormente, es poco probable que baste con las excepciones generales usuales por razones de salud/privacidad/prudencia.

[bb] Definido como el primer nombre/'primer nombre y apellido del ser humano en combinación con uno o más de los siguientes elementos de datos, cuando el nombre y los elementos de datos no están encriptados:
(b) Número de seguridad social.
(b) Número de licencia de conducir, número de tarjeta de autorización de conductor o número de tarjeta de identificación.
(c) Número de cuenta, número de tarjeta de crédito o número de tarjeta de débito, en combinación con cualquier código de seguridad, código de acceso o contraseña requeridos que permitan el acceso a la cuenta financiera de la persona.

Como se puede ver más arriba, dejar que las "partes en una transacción electrónica" decidan qué tan seguro deba ser puede ser problemático en una transacción de empresa a empresa en la que una o ambas compañías desean reducir costos. Es aún peor cuando una de las "partes" de la transacción es un consumidor (por ejemplo, banca en línea, informes crediticios, pruebas de ADN, compras en línea, etc.) que tiene poco o ningún poder para determinar qué tan segura debe ser la transacción. Las situaciones anteriores ya son problemas del mundo real al dejar que las empresas decidan cuán segura sería una transacción electrónica.

Los ejemplos anteriores son solo algunos de los que se han visto en informes de noticias recientes. Ha habido muchos otros informes sobre la falta de transmisión segura de información personal confidencial por parte de empresas privadas, como cámaras web que monitorean un centro de cuidado infantil[cc] y aplicaciones de citas[dd]. Es probable que haya muchas más circunstancias en que dejar que el sector privado determine el nivel de seguridad puede dar como resultado un nivel de seguridad inferior al requerido para la protección del consumidor, privacidad, etc. a medida que las empresas intentan minimizar los costos.

El ejemplo anterior de Equifax muestra que incluso si no existe una legislación actual que exija que dichos datos se retengan, transmitan, procesen, etc. de manera más segura, ya existe la necesidad de dicha legislación según una senadora estadounidense ampliamente reconocida como experta en protección financiera del consumidor.

Además, a medida que las transacciones electrónicas se generalizan, incluso los datos personales más sensibles (por ejemplo, registros de salud, financieros, etc.) pueden transmitirse electrónicamente con los mayores riesgos que conlleva.

Las leyes que requieren un cierto nivel de seguridad en las transacciones electrónicas entre las partes privadas descritas anteriormente son solo aquellas que se pueden encontrar con poco esfuerzo. Una búsqueda sistemática de todas las medidas (por ejemplo, leyes, reglamentos, directivas, circulares, etc.), en todos los niveles de gobierno, en todos los sectores, ministerios gubernamentales y reguladores es probable que encuentre muchas otras medidas que requieren un cierto nivel de seguridad en las transacciones electrónicas. Como se señaló anteriormente, las leyes nacionales o subnacionales ya exigen que las transacciones electrónicas tengan un cierto nivel de seguridad por razones de protección del consumidor, etc. Conforme al TPP y algunas disposiciones propuestas de autentificación electrónica de la OMC, estas leyes solo se pueden mantener para una categoría de transacciones como máximo.

[cc] El centro de cuidado infantil permitió a los padres de los niños matriculados controlar a sus hijos en el centro de cuidado infantil a través de una cámara web. Sin embargo, esto no usó https, por lo que los datos no fueron encriptados. La Oficina del Comisionado de Privacidad de Canadá recomendó que se use https para esta cámara web, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2011/pipeda-2011-008 /. No está claro si este tipo de situación estaría cubierta por "partes en una transacción electrónica" (donde la intervención del gobierno está restringida en las propuestas de comercio electrónico), ver más arriba.

[dd] Por ejemplo, la aplicación de citas más popular del mundo no usó https para sus fotos, encuentros o coincidencias, por lo que no están encriptados y 'Solo por estar en la misma red Wi-Fi cualquier usuario de la aplicación iOS o Android de Tinder, los investigadores pudieron ver cualquier foto que el usuario hizo, o incluso inyectar sus propias imágenes en su flujo de fotos. Y mientras otros datos en las aplicaciones de Tinder están encriptados con HTTPS, Checkmarx descubrió que aún filtraban suficiente información para separar los comandos cifrados, permitiendo que un pirata informático en la misma red mirara cada deslizamiento hacia la izquierda, deslizara hacia la derecha o coincidiera en el teléfono del objetivo casi tan fácilmente como si estuvieran mirando por encima del hombro del objetivo. Los investigadores sugieren que la falta de protección podría permitir cualquier cosa, desde simple curiosidad voyeurista hasta esquemas de chantaje ', https://www.wired.com/story/tinder-lack-of-encryption-lets-strangers-spy-on-swipes/

Bajo las propuestas de TLC de la UE, todas estas leyes deberían ser eliminadas ya que las propuestas de TLC de la UE no tienen excepciones.

Dada la diversidad de los sectores afectados y la variedad de ministerios que ya regulan / planean regular las transacciones electrónicas (desde regulación financiera, protección del consumidor, aplicación de la ley a la salud, etc.) en varios niveles de gobierno, es importante consultar a todos los ministerios y niveles relevantes de el gobierno y los sectores económicos y sociales afectados antes de decidir si aceptan esta clase de propuesta de comercio electrónico. Por ejemplo, las pequeñas tiendas y restaurantes pueden no querer que las compañías dominantes de tarjetas de crédito tengan el derecho de continuar con sus actuales reglas privatizadas.

Como el informe del gobierno de Minnesota sobre la privacidad de los datos se menciona en una sección titulada Panorama Legal Impredecible (Legal Landscape Unpredictable): "Es imposible predecir cómo será el panorama jurídico relativo a la privacidad y seguridad de los datos en los próximos meses o años venideros. . . Los legisladores federales y estatales continúan lidiando con formas de lograr un equilibrio entre las nuevas tecnologías, el flujo libre de información que se ha vuelto omnipresente para el comercio electrónico, la proliferación de las redes sociales y la protección de la información personal[155]. "El mismo informe enumera 10 proyectos de ley federales en los Estados Unidos como algunos de los que proponen una mayor protección de la privacidad de datos en el Congreso de los EE.UU. cuando los legisladores responden a las violaciones de datos.

Si incluso los gobiernos de los países desarrollados tienen dificultades para seguir la evolución de la tecnología, es aún más difícil para los países en desarrollo y los países menos adelantados (PMA) predecir qué sectores tendrán transacciones electrónicas en el futuro y dónde los gobiernos pueden y necesitan regular. Cuando incluso las reglamentaciones nacionales tienen problemas para mantenerse al día con la velocidad del cambio tecnológico, encerrar en la desregulación / autorregulación corporativa del *laissez faire* en un tratado internacional (que es incluso más lento de enmendar si resulta problemático en un momento de rápido cambio tecnológico) corre el riesgo de estar desactualizado para cuando el acuerdo comercial entre en vigencia.

Es sorprendente que, en un momento en que se encuentran cada vez más ejemplos de ciberseguridad insuficiente de las empresas privadas, y los gobiernos desarrollados, en desarrollo y menos desarrollados están planeando nuevas reglamentaciones para abordarlos, las negociaciones comerciales contemplan una desregulación (total) de este problema, dejando que las empresas privadas establezcan los estándares cuando muchas de esas compañías han elegido niveles inadecuados de ciberseguridad (que causan problemas para los consumidores, etc.) cuando se les deja elegir el nivel de seguridad.

Anexo: posibles futuros problemas de ciberseguridad

Acceso no autorizado / uso de información genética / ADN

El ADN y la información genética deben estar seguros. Puede revelar información sobre su salud, personalidad, historia familiar, etc.[156] y los investigadores ya han demostrado que es posible identificar a algunas personas basándose en datos genéticos anónimos. En 2013, un profesor de MIT publicó un estudio en el que identificó con éxito a personas y sus familiares basándose en datos genéticos "anónimos" en un estudio de investigación, junto con solo su edad y estado.[157] "Incluso cuando parte del genoma se deja de lado (por ejemplo, James Watson no publicó la parte de su genoma que indica si es más probable que desarrolle Alzheimer), que puede predecirse basándose en el ADN circundante.[158]

a. El senador estadounidense Schumer publicó un comunicado de prensa en noviembre de 2017 sobre equipos de prueba de ADN en el hogar que requieren un hisopado de la mejilla o la recolección de saliva, que luego se envía para pruebas genéticas

> i. En los últimos años, los kits de prueba de ADN se han vuelto cada vez más populares. Según los informes de los medios, el mercado de pruebas de ADN valía aproximadamente $ 70 millones en 2015 y se espera que aumente a $ 340 millones para 2022.. .
> ii. Muchos consumidores compran kits de prueba de ADN, de compañías como MyHeritage, Ancestry y otros para aprender más sobre su genética y ascendencia, sin embargo, muchos no se dan cuenta de que su información confidencial puede terminar en manos de muchas otras compañías de terceros. . .
> iii. Schumer señala que cada empresa tiene su propia variación de una política de privacidad y de los Términos de Servicio y que muchas compañías pueden estar vendiendo a terceros los datos genéticos que han reunido. Schumer dijo hoy que está claro que se debe hacer más para proteger la privacidad del consumidor cuando se trata de estos kits de prueba de ADN en el hogar. . .
> iv. Cuando se trata de proteger la privacidad de los consumidores de los servicios de kits de prueba de ADN en el hogar, el gobierno federal está atrasado. Además, poner su información genética más personal en manos de terceros para su uso exclusivo plantea muchas preocupaciones, desde la posibilidad de discriminación por parte de los empleadores hasta el seguro de salud. . . Es por eso que le pido a la Comisión Federal de Comercio que examine seriamente este tipo de servicio relativamente nuevo y se asegure de que estas compañías tengan políticas y estándares de privacidad claros y justos para todo tipo de kits de prueba de ADN en el hogar"[159].

b. El Senador Schumer señaló que "esto es lo que muchos consumidores no se dan cuenta, que su información confidencial puede terminar en manos de compañías desconocidas de terceros", dijo. "No hay prohibiciones, y muchas compañías dicen que todavía pueden vender su información a otras compañías. "" Ahora, esta es información confidencial, y lo que esas compañías pueden hacer con todos esos datos, de nuestra información sensible y profunda, su genética, no está clara y en algunos casos no es ni justa ni correcta", agregó. "Llegó a la conclusión de que las compañías son completamente nuevas y necesitan salvaguardias".[160]

c. Un abogado de protección al consumidor notó que cuando envía su muestra a una compañía de análisis de ADN "Es básicamente como si no tuvieras privacidad, lo están tomando todo"[161]. Las compañías de pruebas de ADN proporcionan sus datos genéticos a otras compañías y no está claro "quiénes son todos esos terceros y qué tipo de reglas implementan las empresas para evitar que esos terceros abusen del acceso a la información genética"[162].

d. Muchos otros han expresado su preocupación por la falta de protecciones de privacidad y seguridad en el mercado de kits de ADN, incluido un ex comisionado asociado de la Administración de Drogas y Alimentos de los Estados Unidos Peter Pitts: "Nunca firmaría los derechos sobre mis genes. . . Tu tampoco deberías hacerlo."[163] La otra cosa que está clara es que las compañías de pruebas genéticas definitivamente están vendiendo información a terceros para investigación médica con el fin de ganar dinero. "Usar esta información para ensayos clínicos es algo bueno", dijo Pitts. "¿Pero quieres que una organización de terceros venda esa información a las compañías farmacéuticas? ¿Qué tan seguros son sus datos en ese entorno de terceros? Usted no lo sabe"[164].

La falta de protección adecuada de la información genética ya ha tenido consecuencias

Aunque EE.UU. tiene la Ley de No Discriminación de Información Genética (GINA, Genetic Information Non-Discrimination Act) que se supone evita que las aseguradoras y los lugares de trabajo discriminen en función de su información genética, las lagunas en la ley significan que los proveedores de seguros de vida, de cuidados a largo plazo o de discapacidad, así como los militares aún pueden tomar decisiones basadas en los hallazgos de su ADN. "GINA en realidad ofrece muy poca protección", dijo Ellen Wright Clayton, abogada y profesora de políticas de salud en la Universidad de Vanderbilt.[165]

"Desde 2008, con la aprobación de la Ley de No Discriminación de Información Genética (GINA, por sus siglas en inglés), el gobierno federal ha prohibido a las compañías de seguro médico negar cobertura a aquellas personas con una mutación genética. Pero la ley no se aplica a las compañías de seguros de vida, cuidado a largo plazo o seguro de discapacidad. Estas compañías pueden preguntar sobre la salud, antecedentes familiares de enfermedades o información genética y rechazar aquellas que se consideran demasiado riesgosas".[166]

"Al principio de esta saga de una década, el proyecto de ley [GINA] incluía todo tipo de seguro", dice Terry. Pero los primeros defensores del proyecto de ley amenazaron con retirar su apoyo si incluía discapacidad, seguro de vida y cuidado a largo plazo,'[167] entonces fueron excluidos de GINA.

La industria de seguros: defiende que el modelo de negocios se derrumbe si las empresas se ven obligadas a aceptar a quienes tienen un alto riesgo de cáncer y diversas enfermedades genéticas en el grupo.

Hay algo de verdad en éste argumento. El Dr. Green del Hospital Brigham and Women's estudió el comportamiento de aquellos que aprendieron a través de una prueba genética que estaban predispuestos a la enfermedad de Alzheimer. Estos pacientes tenían cinco veces más probabilidades de comprar un seguro de cuidado a largo plazo que aquellos en un grupo de control.

Y de manera singular, las aseguradoras de salud pueden compensar su riesgo al recibir primas mensuales de estadounidenses jóvenes y sanos (el "Mandato individual" de la Ley de Asistencia Asequible – Affordable Care Act – requiere que mucha gente obtenga un seguro médico o una multa). Por el contrario, la decisión de comprar un seguro de vida o un seguro de cuidado a largo plazo es opcional. Quienes solicitan pólizas pueden tener razones para creer que necesitan protecciones adicionales"[168].

"California aprobó un proyecto de ley llamado CalGINA que no solo prohíbe la discriminación genética en el empleo y el seguro de salud, sino también en vivienda, educación, préstamos hipotecarios y elecciones. Oregon y Vermont también tienen amplias reglamentaciones que prohíben el uso de información genética en la vida, cuidado a largo plazo y seguro de discapacidad.[169]

A un paciente ya le negaron un seguro de vida porque tenía el gen BRCA1 asociado con un mayor riesgo de cáncer de mama y ovario y un padre con mayor riesgo de cáncer de próstata se rehusó a analizarlo (aunque eso le ayudaría a prolongar su vida) porque le podian negar el seguro de vida.[170]

"El vacio de GINA no solo llamó la atención de los grupos de derechos de los pacientes. Los investigadores médicos también están cada vez más preocupados de que retrase sus ensayos clínicos y estudios.

Green dirige un ensayo aleatorio para estudiar la secuenciación de genes en adultos llamado el proyecto MedSeq, que se basa en que los pacientes acepten almacenar sus datos de secuenciación del genoma en

sus registros médicos. Como informó recientemente en el New England Journal of Medicine, el 25% de los pacientes que rechazaron participar en el estudio citando el temor a la discriminación de las compañías de seguros de vida como su principal razón.

Green espera que más pacientes abandonen los estudios clínicos y las pruebas genéticas a medida que se den cuenta de los inconvenientes.

> "Antes de la aprobación de GINA, mucha gente temía que esta nueva era de pruebas genéticas no incluyera protecciones adecuadas para los pacientes", dice Green. "Pero todavía hay motivos para temer que las empresas discriminen a familias enteras""[171] Al realizar una secuencia de estudio del genoma de los bebés, Green obtuvo una tasa de reclutamiento del 10 por ciento: para obtener 300 familias, tuvieron que pedirselo a 3,000. "Hay muchas razones", dice Green, "pero la tercera más común era la preocupación por la privacidad y la discriminación".[172]

Las empresas de pruebas genéticas de consumidores generalmente no están sujetas a las normas de los Estados Unidos sobre privacidad de datos de salud

Aunque EE.UU. posee la Ley de Responsabilidad y Portabilidad de Seguros Médicos (HIPAA) para proteger la privacidad de los datos de salud, "debido a que las firmas de pruebas genéticas de los consumidores no están generalmente obligadas por HIPAA, el flujo de sus datos básicamente no está regulado", dijo Bob Gellman, un consultor sobre privacidad y seguridad. Eso significa que cualquier destinatario autorizado de que su información podría pasarla fácilmente a otra persona. "Cualquier información en cualquier lugar puede ser pirateada de una forma u otra. Eso es lo simplemente sucede hoy ", dijo Gellman. "Cuantas más personas tienen los mismos datos, más riesgo hay de los datos. Eso es un hecho".[173]

Los piratas informáticos podrían robar datos genéticos

"La información genética es mucho más sensible y la gente (con razón) se preocupa de que pueda ser utilizada en su contra por las aseguradoras, o incluso robada por piratas informáticos."[174] El jefe de investigación en criptografía de Microsoft que se enfoca en el cifrado de ADN señaló que "si no pensamos sobre esto ahora, entre cinco a 10 años la información genómica de mucha gente se usará de formas que no se pretendían"[175].

Los programas comunes de procesamiento de ADN son extremadamente vulnerables a los piratas informáticos

'Los programas comunes de procesamiento de ADN de código abierto son muy vulnerables a los piratas informáticos'[176]. "Los investigadores analizaron versiones de código abierto de uso común de esos programas. Muchos, descubrieron, estaban escritos en lenguajes de programación conocidos por tener problemas de seguridad. Algunos también contenían vulnerabilidades específicas y problemas de seguridad. "Este análisis de seguridad básico implica que la seguridad de la secuencia de procesamiento de datos de secuenciación no es suficiente si los atacantes apuntan", escribieron.[177]

La inseguridad de estos programas tiene implicaciones para la justicia penal: "Greg Hampikian, profesor de biología y justicia penal en Boise State, dijo que las vulnerabilidades más inmediatas que los investigadores destacaron son preocupantes. "Si pudieras irrumpir en un laboratorio de delitos, podrías alterar los datos, pero si puedes acceder a los datos del laboratorio criminal, tienes una ruta mucho más eficiente. Y si los datos se modifican, eso es lo que se usará para testificar en la corte ",

dijo. "Tuvimos accidentes donde se intercambiaron tubos. Si pudieras alterar o borrar maliciosamente, obviamente ese es un gran problema"[178].

Un experto académico que comentaba sobre la falta de seguridad de las empresas de análisis de ADN de los consumidores señaló que "con 23andMe y Ancestry estás contratando tu ADN para ellos, y ¿cómo están manejando la seguridad del ADN? Allí esa información está vinculada a tu nombre ", dijo. Debido a que no está claro cómo se aseguran y utilizan esos datos, le dijo a Gizmodo, incluso recomienda que sus alumnos eviten las pruebas de ADN de los consumidores. "No hay nada más sensible que el ADN de alguien", dijo.[179]

Hay formas más seguras de manejar datos genéticos disponibles

Se encuentran disponibles formas más seguras de manejar datos genéticos, de como encriptarlos.[180]

> Sin embargo, cuando se les deja decidir por sí mismas, las compañías privadas no eligen utilizar estos métodos más seguros (presumiblemente debido a las preocupaciones sobre el costo). Por lo tanto, es posible que los gobiernos tengan que regular para garantizar un cierto nivel de seguridad en la transmisión, el almacenamiento, el procesamiento, etc. de datos personales altamente confidenciales, como la información genética.

[1] https://www.internetsociety.org/globalinternetreport/2016/

[1] https://www.internetsociety.org/globalinternetreport/2016/

[2] Página 98

[3] https://www.ntia.doc.gov/files/ntia/publications/eo_13800_botnet_report_for_public_comment.pdf

[4] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

[5] https://www.internetsociety.org/globalinternetreport/2016/

[6] Véase abajo la sección de oleoductos

[7] https://www.schneier.com/blog/archives/2016/07/real-world_secu.html

[8] https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/

[9] TN/S/W/64 de https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx

[10] JOB/GC/188 de https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx

[11] WT/L/274 de https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S001.aspx.

[12] WT/MIN(17)/60 de https://www.wto.org/english/thewto_e/minist_e/mc11_e/documents_e.htm

[13] Art 8.77.3 http://trade.ec.europa.eu/doclib/press/index.cfm?id=1684

[14] Art 6.3 del capítulo de comercio digital http://trade.ec.europa.eu/doclib/press/index.cfm?id=1833

[15] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories

[16] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories

[17] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories

[18] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories

[19] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories

[20] https://www.wired.com/story/tinder-lack-of-encryption-lets-strangers-spy-on-swipes/

[21] Por ejemplo vea https://www.entrepreneur.com/article/281633

[22] Consulte la tabla de precios de solicitud para todos los métodos HTTP (por cada 10.000) en https://aws.amazon.com/cloudfront/pricing/

[23] https://techcrunch.com/2017/10/30/aws-continues-to-rule-the-cloud-infrastructure-market/

[24] https://www.entrepreneur.com/article/281633

[25] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories

[26] https://www.wired.com/2016/04/hacker-lexicon-what-is-https-encryption/?mbid=BottomRelatedStories

[27] www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

[28] NRS 603A.215.2 https://www.leg.state.nv.us/NRS/NRS-603A.html

[29] https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf

[30] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report

[31] https://oag.ca.gov/idtheft/facts/your-ssn

[32] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report

[33] https://www.ssa.gov/pubs/EN-05-10064.pdf

[34] https://www.ssa.gov/pubs/EN-05-10064.pdf

[35] https://oag.ca.gov/idtheft/facts/your-ssn

[36] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report

[37] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report

[38] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report

[39] https://oag.ca.gov/idtheft/facts/your-ssn

[40] Véa por ejmplo https://www.wcpo.com/money/consumer/dont-waste-your-money/what-your-accounts-are-worth-on-the-dark-web

[41] https://www.bloomberg.com/news/articles/2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go
[42] https://www.ftc.gov/reports/security-numbers-social-security-numbers-identity-theft-federal-trade-commission-report
[43] https://www.bloomberg.com/news/articles/2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go
[44] https://www.bloomberg.com/news/articles/2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go
[45] http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.85.
[46] Minn.Stat §325E.59: Uso de los números de Seguridad Social, https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf escrito por un despacho legal, https://mn.gov/deed/newscenter/press-releases/?id=1045-229996
[47] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview.html
[48] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Transactions/TransactionsOverview.html
[49] Art 29.1 del TPP
[50] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Operating-Rules/OperatingRulesOverview.html
[51] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/Operating-Rules/OperatingRulesOverview.html
[52] Art 29.1 delTPP
[53] https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/index.html
[54] https://www.youtube.com/watch?v=s_1CZYK8qb8
[55] https://www.youtube.com/watch?v=s_1CZYK8qb8
[56] https://www.caqh.org/core/operating-rules-mandate-eft-and-era
[57] Art 29.1 del TPP
[58] https://www.theguardian.com/technology/askjack/2017/jun/22/is-it-safer-to-use-an-app-or-a-browser-for-banking
[59] http://www.bbc.com/news/technology-42353478
[60] https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=8207
[61] Section 500.15 https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf
[62] Section 500.12 https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf
[63] Art 14.6 https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/
[64] https://www.ftc.gov/about-ftc
[65] https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf , por ejemplo, ver queja en https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter, véa también https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges
[66] Queja en https://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter
[67] Queja en https://www.ftc.gov/enforcement/cases-proceedings/072-3055/tjx-companies-inc-matter
[68] https://www.ftc.gov/news-events/press-releases/2008/03/agency-announces-settlement-separate-actions-against-retailer-tjx
[69] https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges
[70] Queja en https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter
[71] https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges
[72] NRS 603A.215.1 https://www.leg.state.nv.us/NRS/NRS-603A.html
[73] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[74] https://www.pcisecuritystandards.org/about_us/
[75] https://www.westpac.com.au/docs/pdf/bb/Guide_to_payment_card_indus1.pdf
[76] https://blog.pcisecuritystandards.org/pci-monitor-2-8-2017
[77] https://www.wired.com/2012/01/pci-lawsuit/
[78] https://www.wired.com/2012/01/pci-lawsuit/
[79] https://www.forbes.com/forbes/2010/0628/entrepreneurs-heartland-payment-visa-mastercard-once-hacked.html#10ea72fe6f32
[80] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[81] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[82] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[83] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[84] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[85] https://www.forbes.com/forbes/2010/0628/entrepreneurs-heartland-payment-visa-mastercard-once-hacked.html#10ea72fe6f32
[86] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm

[87] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[88] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[89] https://www.gpo.gov/fdsys/pkg/CHRG-111hhrg52239/html/CHRG-111hhrg52239.htm
[90] https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-001/
[91] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_analysis.pdf
[92] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_analysis.pdf
[93] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_analysis.pdf
[94] https://ag.ny.gov/press-release/ag-schneiderman-announces-settlement-uber-enhance-rider-privacy
[95] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_complaint_0.pdf
[96] https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_revised_analysis.pdf
[97] https://www.usnews.com/news/best-states/alaska/articles/2018-03-16/trans-alaska-pipeline-fights-22-million-cyberattacks-per-day
[98] https://fas.org/sgp/crs/homesec/R42660.pdf
[99] https://www.usnews.com/news/best-states/alaska/articles/2018-03-16/trans-alaska-pipeline-fights-22-million-cyberattacks-per-day
[100] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[101] http://www.post-gazette.com/powersource/companies/2018/04/02/Cyber-attack-shuts-Energy-Transfer-s-pipeline-data-system-EDI/stories/201804020114
[102] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[103] https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat
[104] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[105] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[106] https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat
[107] https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat
[108] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[109] https://fas.org/sgp/crs/homesec/R42660.pdf, véa https://apps.neb-one.gc.ca/REGDOCS/File/Download/614556 para la decisión canadiense de hacerlo obligatorio.
[110] https://fas.org/sgp/crs/homesec/R42660.pdf
[111] https://fas.org/sgp/crs/homesec/R42660.pdf
[112] https://www.bloomberg.com/news/articles/2018-04-06/cyberattack-wake-up-call-puts-pipeline-industry-in-hot-seat
[113] https://www.bloomberg.com/news/articles/2018-04-04/cyberattack-bleeds-into-utility-space-as-duke-sees-billing-delay
[114] https://www.bloomberg.com/news/articles/2018-06-11/u-s-regulators-urge-better-oversight-for-pipeline-cybersecurity
[115] https://www.axios.com/cybersecurity-threats-to-us-gas-pipelines-call-for-stricter-oversight-09fac6e5-da94-491e-9523-d08ef15237f4.html
[116] https://www.wired.com/story/online-stock-trading-serious-security-holes/, el informe completo en https://ioactive.com/are-you-trading-stocks-securely-exposing-security-flaws-in-trading-technologies/
[117] https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214/
[118] https://arstechnica.com/tech-policy/2017/11/an-alarming-number-of-sites-employ-privacy-invading-session-replay-scripts/
[119] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[120] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[121] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[122] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[123] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[124] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[125] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[126] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[127] https://www.warren.senate.gov/about/about-elizabeth
[128] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[129] http://www.himss.org/sites/himssorg/files/2016-cybersecurity-report.pdf
[130] https://healthitsecurity.com/news/protecting-against-unauthorized-healthcare-data-access
[131] https://healthitsecurity.com/news/are-third-parties-compromising-healthcare-data-security
[132] https://healthitsecurity.com/news/health-data-encryption-questions-to-ask-your-vendors
[133] https://healthitsecurity.com/news/health-data-encryption-questions-to-ask-your-vendors
[134] http://www.marketwired.com/press-release/third-party-vendors-are-key-concern-for-business-data-privacy-survey-finds-2111430.htm

[135] https://healthitsecurity.com/news/are-third-parties-compromising-healthcare-data-security
[136] 45 CFR 164.312e) https://www.law.cornell.edu/cfr/text/45/164.312
[137] http://www.himss.org/sites/himssorg/files/2016-cybersecurity-report.pdf
[138] https://www.hipaajournal.com/hipaa-breaching-email-exposed-bjc-healthcare-patients-data-8334/.
[139] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[140] https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf
[141] https://www.bloomberg.com/news/articles/2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go
[142] http://www.thefutureworldofwork.org/stories/uni-global/tisa-foul-play/
[143] Art XIV https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV
[144] https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXX
[145] https://www.citizen.org/sites/default/files/general-exception_4.pdf
[146] Art XIVc) https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXIV
[147] Art 11.11.1 https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-concluded-but-not-in-force/cptpp/comprehensive-and-progressive-agreement-for-trans-pacific-partnership-text/
[148] Véase por ejemplo http://www.citizen.org/documents/report-prudential-measures.pdf
[149] https://www.wto.org/english/docs_e/legal_e/26-gats_02_e.htm#annfin
[150] http://www.politico.com/tipsheets/morning-trade/2016/02/lew-defends-financial-services-data-carveout-senate-to-vote-on-customs-bill-democrats-weigh-in-on-tpp-212657
[151] http://www2.itif.org/2016-financial-data-trade-deals.pdf?mc_cid=0a36b6ab0c&mc_eid=671b585ee6
[152] http://trade.ec.europa.eu/doclib/docs/2016/february/tradoc_154329.pdf (Art 13.16.1 on p103)
[153] (firmado en 2008: http://ec.europa.eu/trade/policy/countries-and-regions/regions/caribbean/) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:289:0003:1955:EN:PDF
[154] Véase 2016 Global Internet Report of the Internet Society, disponible en: https://www.internetsociety.org/globalinternetreport/2016/
[155] https://mn.gov/deed/assets/legal-guide-to-privacy-and-data-security_tcm1045-133708.pdf
[156] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[157] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[158] https://www.wired.com/story/to-protect-genetic-privacy-encrypt-your-dna/
[159] https://www.schumer.senate.gov/newsroom/press-releases/schumer-reveals-popular-at-home-dna-test-kits-are-putting-consumer-privacy-at-great-risk-as-dna-firms-could-sell-your-most-personal-info-and-genetic-data-to-all-comers-senator-pushes-feds-to-investigate_ensure-fair-privacy-standards-for-all-dna-kits
[160] https://www.nbcnews.com/news/us-news/senator-calls-more-scrutiny-home-dna-test-industry-n824031
[161] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[162] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[163] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[164] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[165] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[166] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[167] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[168] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[169] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[170] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[171] https://www.fastcompany.com/3055710/if-you-want-life-insurance-think-twice-before-getting-genetic-testing
[172] https://www.wired.com/2017/05/house-health-plan-makes-genes-preexisting-condition/
[173] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[174] https://www.wired.com/story/to-protect-genetic-privacy-encrypt-your-dna/
[175] https://www.wired.com/story/to-protect-genetic-privacy-encrypt-your-dna/
[176] https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337
[177] https://gizmodo.com/dna-testing-data-is-disturbingly-vulnerable-to-hackers-1797695128
[178] https://gizmodo.com/dna-testing-data-is-disturbingly-vulnerable-to-hackers-1797695128
[179] https://gizmodo.com/dna-testing-data-is-disturbingly-vulnerable-to-hackers-1797695128
[180] https://www.wired.com/story/to-protect-genetic-privacy-encrypt-your-dna/