REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 11 NÚM. 1 (2022) • PÁGS. 103-120 • DOI 10.5354/0719-2584.2022.60821
RECIBIDO: 21/1/2021 • APROBADO: 8/3/2022 • PUBLICADO: 30/6/2022

DOCTRINA

Situaciones de riesgo moral e incentivos desalineados en ciberseguridad

Moral hazard situations and misaligned incentives in cybersecurity

Sebastián Bilbao Pérez
Abogado, Chile

RESUMEN La seguridad del espacio informático es un asunto no solo técnico, sino que también tiene un componente humano, introducido por quienes diseñan y operan los sistemas involucrados. En tal sentido, los incentivos que recaen sobre estas personas no pueden ser ignorados. Entenderemos que se produce riesgo moral cuando los generados por una de las partes en una transacción son asumidos por la otra, creando un incentivo a actuar imprudentemente. En este escrito se estudian tres casos en los cuales se produce esta situación en materias de ciberseguridad y en que los incentivos de los fabricantes o proveedores de servicios no están alineados con los de los usuarios o consumidores.

PALABRAS CLAVE Riesgo moral, incentivos desalineados, ciberseguridad.

ABSTRACT Security in the cyberspace is not only a technical matter, but it also contains a human element introduced by those who design and operate the systems involved. In this respect, the incentives that befall on those persons cannot be ignored. We understand that a moral hazard arises when the risks generated by one of the parties in a transaction are borne by the other, creating an incentive to act recklessly. In this paper, we analyze three cases in which this situation occurs in a cybersecurity context and in which the incentives of manufacturers or providers of services are misaligned with the ones of users or consumers.

KEYWORDS Moral hazard, misaligned incentives, cybersecurity.

Introducción

La seguridad en el espacio informático y de la información no son fenómenos puramente técnicos, sino que tienen un componente eminentemente humano. Todas las medidas que se puedan imaginar, así como todas las salvaguardas tecnológicas, no podrán ser efectivas sin el conocimiento, la cooperación y la ejecución de los usuarios.

Siendo de tal crítica importancia para nuestra seguridad el comportamiento de los humanos detrás del sistema, es dable preguntar si existen los incentivos adecuados para motivar acciones que mantengan resguardados nuestros sistemas de información. En efecto, el hecho de que «los individuos racionales responden a incentivos» ha sido reconocido como un principio básico de la economía (Mankiw, 2002: 4) que gobierna el actuar de las personas en todo ámbito. Por supuesto, como consecuencia, las decisiones tomadas por quienes mantienen, diseñan e implementan sistemas informáticos también estarán influenciadas por este factor.

Al considerar lo anterior, no es difícil imaginar los incentivos que existen para mantener una organización segura en el espacio informático, pero el propósito de esta obra es identificar situaciones en las cuales los incentivos de aquellos que tienen control sobre los sistemas informáticos que utilizamos día a día no apuntan, necesariamente, a implementar un sistema seguro. Esto porque no es el interés de estos actores invertir activamente en recursos para establecer medidas o bien, desde una mirada más pesimista, porque su disposición es específicamente crearlos de forma insegura. En este sentido, Schneier (2018: 56) ha planteado incluso que «las razones difieren —y las partes involucradas nunca admitirán esto abiertamente— pero, básicamente, la inseguridad está en los intereses de tanto las corporaciones como los gobiernos».[1]

En este análisis será de particular importancia el concepto de riesgo moral. Entenderemos que este se produce en situaciones donde «el problema se da cuando los costos atribuibles a los riesgos de una parte son soportados por otro»[2] (Vagle, 2020: 79). Generalmente, cuando hablamos de ciberseguridad, se tratará de escenarios donde quienes diseñan o administran sistemas pueden tomar actitudes riesgosas, ya que los costos asociados a esto serán asumidos por los clientes o bien por la comunidad en general. Como señala este autor, es importante destacar que las situaciones de riesgo moral son posibilitadas por las asimetrías de información, siendo la parte dominante la que empuja el costo de sus inseguridades sobre la contraparte. En particular, cuando nos referimos a plataformas software y tecnología, esta asimetría es particularmente fuerte. Como expone Vagle, las tecnologías conectadas que usamos día a día como *smartphones* o computadoras están diseñadas para esconder de los usuarios la

1. Esta y todas las traducciones son nuestras: «The reasons differ–and the parties involved will never admit this plainly–but basically, insecurity is in the interests of both corporations and governments».

2. «The problem arises whenever the costs attribuable to one party's risks are borne by another».

complejidad de los intrincados procesos que desarrollan rutinariamente, y este ocultamiento de la forma en que operan estos aparatos crea naturalmente asimetrías de información (Vagle, 2020: 87).

A continuación, se analizan algunos casos en los cuales se produce el fenómeno descrito de riesgo moral en el campo de la ciberseguridad. Si bien no se pretende hacer un estudio taxativo de todas las situaciones que pueden generar tal problemática, pues esa sería una tarea imposible, sí es la intención al menos revisar algunos ejemplos con el fin de obtener conclusiones generales.

Falta de reporte de incidentes de ciberseguridad

Reportar los incidentes de ciberseguridad que una plataforma o una organización sufre parece ser una práctica básica. En efecto, sería una expectativa razonable por parte de los clientes saber cuándo las plataformas que utilizan han sufrido vulnerabilidades, sobre todo si estos sistemas manejan información personal u otros datos sensibles. Por otra parte, resultaría difícil formular estrategias efectivas de defensa y seguridad si no se cuenta con información precisa sobre qué clase de vulnerabilidades o problemas se producen en la práctica. En tales circunstancias, aquellos que manejan estas plataformas parecen ser quienes estarán en la mejor posición para recolectar información sobre tales eventos.

Sin embargo, en múltiples publicaciones y estudios se afirma que los actores relevantes tienen una marcada tendencia a no reportar los incidentes producidos en ciberseguridad. En 2016, Forbes informó que tan solo un poco menos de un tercio de los ciberataques a negocios del Reino Unido eran reportados.[3] Un estudio de ISACA (Asociación de Auditoría y Control de Sistemas de Información) en 2019 concluyó que «las empresas necesitan considerar que muchos incidentes de cibercrimen pueden pasar sin ser reportados, a pesar de las exigencias legales o regulatorias de reportarlos»[4] (ISACA, 2019: 11). Asimismo, una investigación realizada en 2019 por la firma Kaspersky (2019a) revela que el 67% de las empresas no reportan los incidentes de ciberseguridad a los que se ven expuestos.

Con esta evidencia de lo común que es no reportar los problemas (Kaspersky, 2019a) es necesario preguntarse claramente qué motiva esto. El no reportar los incidentes en este ámbito podría plantearse como algo perjudicial para las empresas, pues estas no pueden obtener asistencia de las autoridades en incidentes que no informan. Sin embargo, en la práctica parece ser que existen incentivos más poderosos para mantener silencio que para hacer públicos estos hechos.

3. Dina Medland, «UK study reveals serious underreporting of cyber attacks by business», *Forbes*, 2 de marzo de 2016, disponible en https://bit.ly/3a8uspi.

4. «Enterprises need to consider that many cybercrime incidents may go undereported-despite legal and regulatory requirements to report».

Es posible desarrollar una hipótesis con respecto a por qué las firmas toman estas actitudes cuando se enfrentan a un incidente de seguridad informática. Kaspersky ha concluido que la mayor preocupación de las empresas industriales cuando sufren incidentes de ciberseguridad no son las lesiones, las muertes o los daños ambientales que puedan producirse, sino que los potenciales daños a su reputación (Kaspersky, 2019b). Dicho esto, parece razonable pensar que un incidente que nunca es reportado ni conocido por el público general es incapaz de dañar la reputación de una empresa. Por otro lado, estas pueden sufrir costosas bajas en su valorización bursátil a causa de la revelación; de fallas de seguridad en sus sistemas. Un estudio de 2017 concluyó que, luego de un ciberataque grave, las acciones de una compañía perdían en promedio un 1,8% de su valor en el mercado de forma permanente.[5] Estos podrían parecer, al menos, dos poderosos incentivos para que una entidad prefiera no revelar al público general estas circunstancias.

Esta práctica de no informar los incidentes de ciberseguridad, conducta que va en contra de los intereses de los usuarios de las plataformas y de la comunidad en general, se debe a una situación de riesgo moral. Así, los riesgos producidos por las organizaciones no son soportados mayoritariamente por ellas, sino que por los usuarios de sus plataformas que no pueden conocer los potenciales peligros bajo los cuales realizan las operaciones que confían a terceros. Y también por la sociedad en general que no obtiene información precisa sobre los incidentes de ciberseguridad que se producen y, en consecuencia, diseña estrategias de defensa y seguridad sobre la base de información incompleta.

Como ya se ha mencionado, las condiciones para que un riesgo moral se produzca descansan en las asimetrías de información que permiten a una de las partes en una relación tomar riesgos a la vez que su contraparte asume los costos. Vagle expone un desbalance de información en cuanto a las probabilidades de los costos en cualquier relación en que se comparten riesgos presenta la oportunidad (y tentación) para la parte dominante en términos de información para tomar riesgos en que el costo se desplaza o de otra forma "engañar" el entendimiento común sobre la relación entre las partes[6] (Vagle, 2020: 80).

Estas situaciones precisamente se producen con frecuencia en un entorno de ciberseguridad debido a la naturaleza de los servicios prestados y de las plataformas involucradas. Hoy, tanto en las tradicionales como en los servicios en línea (sistemas de mensajería, bancarios en línea, redes sociales), y como en nuevas aproximaciones

5. CFO, «Cyber attacks can cause major stock drops», 12 de abril de 2017, disponible en https://bit.ly/3abEJ4l.

6. «An information imbalance regarding the probabilities and costs in any risk sharing relationship presents the opportunity (and temptation) for the information dominant party to take cost-shifted risks or otherwise "cheat" the shared understandings of the parties' relationship».

relativas al «internet de las cosas» (refrigeradores, hervidores y aspiradores inteligentes), es difícil para los usuarios saber exactamente qué hacen estos dispositivos o cómo lo hacen (Vagle, 2020: 85) debido a las barreras técnicas involucradas.

Cuando una firma se encuentra en estas situaciones, aquellos ajenos a ella no tienen la visibilidad adecuada para detectar las vulnerabilidades, ya que los ciberataques no son generalmente observables para el público (Amir y otros, 2018: 1.180). Esta poderosa asimetría permite a los actores del mercado esconder la información o al menos no revelarla hasta que se descubra por otros medios, lo cual bien puede no suceder. En efecto, el número de ataques o incidentes que incluso los inversionistas de una compañía pueden descubrir por sus propios medios es pequeño, por lo que, aun cuando existe un riesgo en no revelar tal información, este puede ser evaluado como uno menor (Amir y otros, 2018: 1.181).

Si bien una alternativa es mandatar legalmente el revelar esta información al público, como hemos visto hay investigaciones que sugieren que incluso existiendo tales reglas las obligaciones de informar no son cumplidas (ISACA, 2019). Esto puede ser explicado por el hecho de que la asimetría de información subsiste aun con la obligación legal de informar[7] por lo que los agentes obligados pueden seguir estimando que el problema de ser descubiertos si no revelan esta información es comparativamente bajo si se compara al costo de revelarla. En tal sentido, un programa de vigilancia activo y robusto de seguridad informática o uno de *whistleblowers* o informantes puede ser una solución más efectiva a la hora de asegurar que la información sobre estos episodios sea socializada, ya que esto resuelve la raíz del problema, es decir, las asimetrías de información.

Sobre actualizaciones de seguridad: El caso del internet de las cosas

Incluso si aquellos que desarrollan los dispositivos que usamos y diseñan el software en que confiamos son extremadamente diligentes, parece imposible asegurar que un sistema de seguridad será infalible. Nuevas vulnerabilidades pueden ser descubiertas en el futuro o aquellos que busquen atacarlo pueden crear nuevas tecnologías ofensivas imposibles de prever para quienes lo diseñaron. En ese sentido, proteger nuestros sistemas en internet es una constante carrera entre atacantes y defensores. La respuesta tradicional ha venido, sobre todo en nuestra época interconectada, en las actualizaciones. Schneier ha descrito la práctica de «parchar» nuestro software como el paradigma de seguridad imperante en este marco. Los sistemas deben ser

7. Ejemplos de estas obligaciones son las incorporadas a la legislación australiana, que bajo ciertas condiciones incluye la obligación de reportar incidentes de ciberseguridad en infraestructura crítica (Department of Home Affairs, 2021). La Regla 12 del CERT-In de India, por otro lado, también establece el reporte mandatorio de ciertos incidentes de seguridad específicos (Kharbanda, 2016).

ágiles y resistentes, capaces de superponerse a fallas no anticipadas y a ataques que evolucionan constantemente (Schneier, 2018: 34-35), y el método de constante parchado otorga esas características.

De alguna forma u otra, las miembros de la industria parecen haberse adaptado a este paradigma cuando hablamos de computadores y software tradicional. Un estudio conducido por FireEye, en que se analizó una muestra de 60 vulnerabilidades detectadas entre 2018 y 2019, concluyó que, en promedio, entre que una vulnerabilidad era revelada al público y que una actualización de seguridad remediándola estaba disponible pasaban nueve días, y que en el 59% de los casos estudiados un parche era lanzado el mismo día que la vulnerabilidad era publicada (FireEye, 2020).

Sin embargo, el panorama no es así en todos los entornos. Cuando hablamos del «internet de las cosas», parece que los proveedores no están tan prestos a lanzar actualizaciones para mantener sus productos seguros en el tiempo. La diferencia en resultados se produce porque existen problemas de incentivos desalineados y riesgo moral en el mercado particular, que hacen que las actualizaciones de seguridad no siempre sean desarrolladas oportunamente cuando se trata de remediar vulnerabilidades en estos dispositivos.

Si bien es difícil encontrar un consenso sobre a que nos referimos exactamente cuando hablamos del «internet de las cosas», para efectos de este artículo se entenderá como «cualquier cosa conectada al internet, aunque está siendo crecientemente definida como objetos que se "hablan" entre ellos» (Burgess, 2018).[8] Hoy en día esto incluye toda clase de dispositivos: ampolletas, hervidores de agua, estufas, refrigeradores, automóviles y una infinidad de otros elementos. Se proyecta que para el 2030 el mundo contara con 125 mil millones de «cosas» conectadas a internet.[9]

El llamado «internet de las cosas» se ha infiltrado en cada faceta de nuestras vidas de forma casi invisible, como menciona Schneier, «tu horno es una computadora que calienta cosas. Tu refrigerador es una computadora que mantiene las cosas frías. Tu cámara es una computadora con un lente y un obturador» (Schneier, 2018: 3).[10] Sin embargo, esta transformación silenciosa no ha sido acompañada por un cambio en las percepciones del público general, que no parece incorporar la

8. «The term IoT encompasses everything connected to the internet, but it is increasingly being used to define objects that "talk" to each other. Simply, the Internet of Things is made up of devices —from simple sensors to smartphones and wearables— connected together. Matthew Evans, the IoT programme head at techUK, says». Matt Burgess, «What is the Internet of Things? WIRED explains», *Wired*, 16 de febrero de 2018, disponible en https://bit.ly/3PYfzGM.

9. Techjury, «How many IoT devices are there in 2021? [All you need to know]», *TechJury*, 22 de abril de 2022, disponible en https://bit.ly/3wWg5NT.

10. «Your oven is a computer that makes things hot. Your refrigerator is a computer that keeps things cold. Your camera is a computer with a lens and a shutter».

noción de que efectivamente estos nuevos objetos son computadoras y deben ser protegidos como tales. Y los riesgos son ciertamente reales.

En 2015, se reportó el descubrimiento de vulnerabilidades que permitían ataques contra un refrigerador inteligente Samsung que no contaba con las adecuadas medidas de seguridad, lo que comprometía las credenciales de Google utilizadas en él.[11] El mismo año, Chrysler se vio forzado a realizar un *recall* de 1.4 millones de vehículos que debían parchar para reparar una vulnerabilidad que permitía tomar remotamente el control de un automóvil.[12] En 2016, un *malware,* tal vez por coincidencia llamado *mirai* (palabra japonesa que se traduce como futuro), nos dejaba ver las consecuencias que podía tener un futuro lleno de dispositivos conectados, pero no asegurados. *Mirai* aprovechaba, por ejemplo, vulnerabilidades en *webcams* y, sin que sus usuarios lo supieran, tomaba control de estos para generar una red de *bots* que masificó ataques de denegación de servicio distribuido y que afectó a múltiples plataformas (Vagle, 2020: 97).

Uno de los aspectos que marca la diferencia entre el problema de la seguridad y las actualizaciones en aparatos tradicionales como computadores y este mismo tema en dispositivos del «internet de las cosas», es que sencillamente no existen los mismos incentivos o mecanismos.

En primer lugar, la misma percepción de los consumidores genera un problema. Estos sencillamente no privilegian la seguridad informática en este tipo de productos. Los clientes priorizan la rapidez en el ingreso al mercado y las nuevas funcionalidades, características en las que no son relevantes las inversiones en protección (Morgner y otros, 2019: 1). Por lo demás, según estos mismos autores, existe efectivamente una asimetría de información entre los productores y los consumidores, ya que estos últimos tampoco cuentan con las herramientas para evaluar si el dispositivo inteligente que pretenden adquirir es seguro. En conjunto, estos factores solo pueden llevar a que, para satisfacer a los compradores y asegurar el éxito comercial, la seguridad no es relevante y, en consecuencia, no existen incentivos comerciales para invertir en esta.

Por otro lado, existe tanto entre consumidores como desarrolladores una cultura que da preferencia a la innovación por sobre la actualización. Esta falta de atención a la actualización, un elemento crítico para la seguridad informática frente a amenazas que evolucionan constantemente, crea riesgos desproporcionados. La visión que pone la innovación por sobre la actualización genera «un claro desbalance basado en las asimetrías de información entre los fabricantes y los usuarios, en cuanto los

11. Jennifer Abel, «Hackers can steal Gmail passwords from Samsung "smart" refrigerators», *Consumer Affairs*, 25 de agosto de 2015, disponible en https://bit.ly/3a7e20u.

12. Andy Greenberg, «After Jeep hack, Chrysler recalls 1.4M vehicles for bug fix», *Wired*, 24 de julio 2015, disponible en https://bit.ly/3t1WUjd.

fabricantes empujan los costos de dispositivos pobremente mantenidos y asegurados sobre los usuarios» (Vagle, 2020: 93).[13]

Por último, hay múltiples actores involucrados en la fabricación de este tipo de aparatos y sus intereses no siempre van al mantenimiento de su seguridad. Cuando una compañía sin experiencia en materias informáticas decide implementar un pequeño computador en su último producto, no forma una robusta división para manejar el asunto, sino que lo hace contactado a un tercero, quien le suministrará estos componentes (Schneier, 2018: 39). Así, los artículos de una compañía se vuelven «inteligentes» gracias a chips fabricados por terceros que operan con bajos márgenes y su seguridad sencillamente no es una ventaja competitiva en su mercado. Quienes fabrican el producto buscan recortar sus costos lo máximo posible, la marca que pondrá su nombre a la postre solo se asegurará de que funcione y finalmente nadie tiene ningún incentivo ni la capacidad para realizar actualizaciones de seguridad una vez que este fue lanzado.[14]

Recapitulando, existe una asimetría de información en cuanto los usuarios no tienen la capacidad para medir la protección de la tecnología que adquieren incrustada en los dispositivos. La falta de interés de ellos en este punto, combinada con los procesos involucrados en la generación de estos productos, crea escenarios en los cuales no hay un real incentivo para invertir en ciberseguridad en ninguno de los que intervienen en la cadena de comercialización y son, finalmente, los usuarios los que asumen el costo del riesgo generado al utilizar sistemas inseguros.

Sobre aplicaciones móviles

El uso de teléfonos móviles inteligentes ha cambiado realmente nuestra sociedad. Estos dispositivos se distinguen de sus antecesores porque son cada vez más similares a una computadora de bolsillo, incorporando cada año nuevas funcionalidades y acercándose cada vez más a la versatilidad de los equipos de escritorio. Y su adopción se ha dado a un ritmo sorprendente: entre 2005 y 2016 los teléfonos inteligentes pasaron de estar presentes en el bolsillo del 5% de los estadounidenses a encontrarse en un 81% de ellos,[15] y en países como Corea del Sur han alcanzado un 95% de penetración en 2019.[16]

13. «A clear imbalance of risk based on information asymmetries between manufacturer and user, where manufacturers are pushing the costs of poorly mantained and secured devices onto the users».

14. Bruce Schneier, «The internet of things is wildly insecure–and often unpatchable», *Wired,* 6 de enero de 2014, disponible en https://bit.ly/3N2P9BM.

15. Comscore, «U.S. Smarthphone penetration surpased 80% in 2016», 3 de febrero de 2017, disponible en https://bit.ly/3ap4yhb.

16. KBS Radio, «S. Korea smartphone penetration highest in the world at 95%», 6 de febrero de 2019, disponible en https://bit.ly/3wURPKV.

Convirtiéndose nuestros teléfonos móviles en computadoras de bolsillo parece evidente que solo podemos aprovechar su gran potencial mediante el uso de aplicaciones, aquel software que instalamos con el fin de que puedan cumplir con distintos propósitos más allá del solo realizar llamadas. Los usuarios adquieren estas aplicaciones, regularmente, a través de ecosistemas cerrados como Play Store de Google o App Store de Apple. Sin embargo, no parecen existir por parte de quienes crean muchas de estas, reales incentivos para invertir en seguridad debido a una situación de riesgo moral.

En términos de información relativa a la seguridad de los productos, las personas se encuentran en una clara desventaja con respecto a los proveedores de sus aplicaciones, ya que el consumidor promedio «no entiende términos de uso, los niveles de permisos de privacidad o como localizar información referida a la seguridad de una aplicación»[17] (Smith, 2019: 86). Esta asimetría se ve reforzada en cuanto los usuarios, a falta de mejores opciones, suelen evaluar la seguridad de una aplicación sobre la base de factores como el número de descargas (Smith, 2019: 89-90), lo que no tiene relación con si una aplicación es segura o no, y evitan involucrarse mayormente en estas materias si no están planteadas en términos claros y simples (Smith, 2019: 90), aunque frecuentemente no lo estén. Esta no es una buena combinación en cuanto, como expone Schneier «la falta de información combinada con la complejidad de los sistemas quita poder a los consumidores y casi definitivamente los lleva a pensar que los dispositivos son más seguros de lo que en realidad son» (Schneir, 2018: 134).[18] Por supuesto, esto permite a los proveedores de aplicaciones tomar riesgos de seguridad que las personas no siempre son capaces de detectar y que no asumirán, pues será la información de ellas la que se encontrará en peligro.

Y existen ejemplos en los cuales el no poder distinguir claramente si una aplicación es segura ha traído consecuencias para millones de personas. Walgreens, una conocida cadena de farmacias en Estados Unidos, reportó en marzo de 2020 que su aplicación permitía a unos usuarios ver los mensajes privados que otros enviaban.[19] En 2018, una vulnerabilidad en la aplicación MyFitnessPal de Under Armour posibilitó la filtración de la información de aproximadamente 150 millones de usuarios en circunstancias que su desarrollador fue inconsistente al encriptar los datos (que incluían contraseñas) en sus servidores, por lo que no todos estaban debidamente protegidos.[20]

17. «Does not understand user agreements, privacy permission levels, or how to locate information about an app's security».

18. «The lack of information combined with the complexity of the systems is disempowering to consumers, and almost certainly lulls them into thinking that devices are more secure than they are».

19. Jessica Davis, «Walgreens reports data breach from personal mobile messaging app error», *HealthITSecurity*, 2 de marzo de 2020, disponible en https://bit.ly/3m7YP2a.

20. Lily Hay Newman, «The Under Armor hack was even worse than it had to be», *Wired*, 30 de marzo de 2018, disponible en https://bit.ly/3lWDGaZ.

A pesar de las consecuencias, el hecho de que las personas no estén en condiciones de evaluar debidamente si un producto es seguro o no, produce una situación similar a la explorada en relación con los dispositivos de «internet de las cosas». Si bien no es el interés de los desarrolladores que sus aplicaciones sean conocidas como inseguras, en cuanto el usuario no puede distinguir aquellas seguras de las inseguras y el desarrollador no asume el riesgo, los esfuerzos se enfocan en la funcionalidad y no en la seguridad (Smith, 2019: 87).

Conclusiones

Luego del análisis de los casos expuestos, es claro que existen circunstancias en las cuales se producen problemas de riesgo moral en el campo de la ciberseguridad. La posición en la que suelen encontrarse los usuarios frente a aquellos que manejan o diseñan los sistemas es de desventaja en cuanto a información. Esta clara asimetría posibilita que se produzcan los riesgos morales y el efecto sobre los clientes es claro. Aquellos que están en control se arriesgan y ponen en peligro a los consumidores sin que estos últimos puedan conocerlo. Las consecuencias de esto no pueden ser subestimadas, pues no se trata aquí solo de que ellos estén en una posición arriesgada, sino de que estos riesgos son tomados por un tercero sin el consentimiento o siquiera el conocimiento de los usuarios. Los resultados de esto son evidentes a la luz de los casos expuestos en cada apartado. Frente a esta situación, por supuesto, la pregunta es: ¿qué podemos hacer?

Al enfrentar este tipo de problemas es fácil caer en la tentación de pensar en la ciberseguridad como un fenómeno puramente técnico que puede ser afrontado de una forma directa y, en algún sentido, simple. Sin embargo, la experiencia y el estudio de los casos propuestos nos ha mostrado que es un fenómeno de una naturaleza al menos dual, tanto humano como técnico. Incluso, cuando se considera que, por ejemplo, el 90% de las fugas de datos en Reino Unido en 2019 fueron causados por problemas humanos antes que técnicos[21], no parece descabellado llegar a la conclusión de que es un asunto incluso más humano que técnico. En tal sentido, para enfrentarnos como un todo a la problemática de la ciberseguridad parece crítico hacerlo desde la ley, la economía, la sicología y la sociología (Schneier, 2018: 99).

Al observar que estos problemas de riesgo moral se apoyan fundamentalmente en las asimetrías de información presentes, lo razonable sería atacar directamente esos desbalances. Si los proveedores de servicios no pueden aprovechar la ventaja que les da la falta de información de los usuarios, no podrán entonces empujar el costo de la falta de seguridad de sus productos sobre los últimos. La solución, entonces,

21. Michael Hill, «90% of data breaches due to human error in 2019», *Info-Security Magazine*, 6 de febrero de 2020, disponible en https://bit.ly/3m2GvXS.

parecería obvia en una primera aproximación: más información. Sin embargo, como veremos, esta es una respuesta incompleta.

Existen múltiples formas en las que se puede proceder. En el caso de aquellos actores que no reportan sus incidentes de ciberseguridad puede plantearse el imponer la obligación de reportarlos. Sin embargo, como hemos visto (ISACA, 2019: 11), puede que esta no sea una solución efectiva en sí. Después de todo, si las sanciones no son lo suficientemente fuertes o si las asimetrías de información se mantienen haciendo poco probable el ser descubierto, puede ser que los incentivos a no reportar sigan siendo más fuertes.

En los casos de la falta de incentivos para mantener seguros los dispositivos del «internet de las cosas» y establecer medidas fuertes de protección en las aplicaciones móviles, pareciera ser, una vez más, que la solución es brindar más información confiable a los usuarios sobre los estándares aplicados. Así, invertir en seguridad se convertiría en un asunto tan importante como el invertir en nuevas funcionalidades. En tal sentido, Schneier ha propuesto el «ser transparente» como uno de los principios fundamentales para asegurar nuestros dispositivos (Schneier, 2018: 108). Sin embargo, hablar simplemente de entregar más información es demasiado amplio y no dice nada sobre la forma en que debe ser presentada, siendo este un aspecto igualmente relevante (Sunstein y otros, 1998: 1.533-1.534).

Conviene detenernos aquí un momento para analizar cómo, en ciertas ocasiones, el entregar información no es suficiente para eliminar las asimetrías de información. El trabajo de Sunstein y otros sugiere que, no solo la información en sí es relevante, sino que también la forma en que esta es presentada puede afectar en gran medida cómo las personas toman decisiones (Sunstein y otros, 1998: 1534-1535).

Por un lado, no será lo mismo para las personas que la información sea presentada con un lenguaje técnico y complejo o que ella sea presentada de una forma simplificada y amigable. En el primer caso, la entrega de la información puede sencillamente no ser efectiva, en cuanto si la persona no puede entender los elementos que se le entregan, no estamos realmente eliminando las asimetrías. A modo de ejemplo, de acuerdo a Bashir y otros (2015: 2), los usuarios tienen dificultades para comprender las políticas de privacidad que aceptan porque su lenguaje suele ser excesivamente complejo. En tal caso, las políticas de privacidad no son una herramienta efectiva para entregar información a los usuarios. Por otro lado, la forma en que esta es presentada puede ser diseñada de forma de favorecer la toma de decisiones en un sentido o en otro (Sunstein y otros, 1998: 1535).

En tal sentido, considerar los intereses de quienes están encargados de presentar la información es también relevante en cuanto la forma en que será comunicada es determinada por ellos y, evidentemente, la compartirán buscando resultados alineados con sus propios intereses (Sunstein y otros, 1998: 1535).

Con respecto a las dificultades que significa entregar información de forma demasiado compleja, Smith recalca que remediar las asimetrías en este campo no es sen-

cillo, en cuanto la seguridad es un asunto complejo, dinámico y con matices (Smith, 2019: 92) y, en consecuencia, puede no ser efectivo presentarlo sin un proceso que haga la información más fácil de entender. De esta forma, se han propuesto sistemas de calificación en los cuales los productos indican a los consumidores —mediante señales sencillas como una etiqueta (Schneier, 2018: 135) o un ícono (Smith, 2019: 92)— si un producto cumple o no con ciertos estándares de seguridad.

Para finalizar se advierte que, habiendo enfrentado estos problemas de incentivos desalineados, se observan respuestas matizadas que no parecen corresponder a un análisis perfectamente lineal de los estímulos involucrados. Y es que, como hemos visto, al abordar la seguridad como un asunto humano, es importante recordar que esto no es igual a decir que se trata simplemente de un asunto de incentivos analizados de forma perfectamente racional. La figura proveniente de la teoría económica del Econ, aquel actor racional que siempre maximiza su utilidad, no se corresponde a la realidad, pues «no vivimos en un mundo de Econs. Vivimos en un mundo de humanos» (Thaler, 2017: 32), y sería un error operar con esa figura en mente al diseñar estrategias de ciberseguridad.

Los humanos, que nos encargamos cada día de darle forma a nuestras propias acciones y políticas de ciberseguridad, mostramos regularmente en nuestras decisiones racionalidad imperfecta (Sunstein y otros, 1998: 1.477), errores en nuestras percepciones de los riesgos incluso cuando contamos con información sobre los mismos (Sunstein y otros, 1998: 1.542) y, en ocasiones, mostramos otros sesgos en nuestros razonamientos (Sunstein y otros, 1998: 1.545) que nos pueden llevar a errores. También la literatura sugiere que las personas demuestran una capacidad de autocontrol imperfecta, lo que puede llevar a potenciales infractores de reglas a romperlas aún si económicamente eso parece no hacer sentido (Sunstein y otros, 1998: 1.538-1.539). No se pretende sugerir que ni los consumidores ni los agentes del mercado actúan de forma irracional. Como hemos visto, debemos tener en cuenta los incentivos involucrados en nuestros sistemas si queremos evitar problemas como los estudiados. Sin embargo, al buscar soluciones a conflictos de incentivos desalineados no se debe olvidar considerar también, en el diseño de políticas de ciberseguridad, esas particularidades del razonamiento humano: tanto los incentivos involucrados como las imperfecciones en los razonamientos. Sobre todo si buscamos lograr lineamientos y acciones realmente efectivas.

Para cerrar esta sección, si bien no es el foco de este artículo extenderse sobre materias como la responsabilidad, cabe preguntarse si, desde una perspectiva jurídica, el hecho de brindar más información no trasladaría a los usuarios parte de la responsabilidad sobre la seguridad de los productos. Después de todo, se podría argumentar que, contando con la información adecuada, los riesgos fueron tomados de forma voluntaria. En términos breves, al menos en cuanto nos refiramos a dispositivos del «internet de las cosas» la respuesta parece clara. Los problemas que describimos suelen producirse en el marco de relaciones de consumo, en que se entiende que es

el productor o proveedor el que debe entregar garantías sobre la seguridad[22] de los bienes o servicios que comercializa. El otorgar información clara y precisa sobre los riesgos involucrados solo sería cumplir con lo dispuesto en la actual Ley 19.496 en cuanto al derecho de los consumidores de ser informado.[23] En este sentido, no parece que el brindar información altere sustancialmente las reglas de responsabilidad ya presentes. Con respecto a situaciones que no puedan subsumirse en la ley del consumidor, la respuesta no es clara y es probablemente un asunto que deba ser definido de acuerdo con las reglas comunes de responsabilidad por los tribunales competentes.

Propuestas normativas

Para finalizar, nos referiremos a herramientas legislativas que ayudarían a remediar efectivamente las asimetrías de información que causan los problemas de riesgo moral descritos considerando los incentivos involucrados. Si bien corresponden a normas aplicadas en áreas regulatorias no necesariamente asociadas a la ciberseguridad, responden a solucionar las mismas falencias informativas, por lo que su aplicación a los problemas es factible.

En cuanto a los dispositivos inteligentes o del «internet de las cosas» puede ser útil adoptar medidas similares a las que se aplican a los aparatos eléctricos, de acuerdo con el numeral 14 del artículo 3 de la Ley 18.410, que crea la Superintendencia de Electricidad y Combustibles. Este dispone un mecanismo mediante el cual los aparatos que se sujeten a la regulación deben contar con una etiqueta de consumo energético. El Decreto 64 de 2013, del Ministerio de Energía, define tales etiquetas de consumo como una

> «etiqueta informativa de productos relacionados con la energía, con la especificación de una serie de características técnicas y energéticas, que proporciona datos a los consumidores para que puedan adquirir estos productos con la información adecuada desde el punto de vista energética».

Destacamos aquí que la misma regulación aclara que el propósito de la etiqueta es entregar información a los consumidores.

La situación de los dispositivos del «internet de las cosas» es comparable a la de los aparatos eléctricos. Es difícil para los usuarios conocer si un producto es seguro

22. El artículo 3, literal d, de la Ley 19.496, que establece normas sobre protección de los derechos de los consumidores, dictamina que es un derecho de los consumidores la seguridad en el consumo y establece el deber de evitar los riesgos que puedan afectarles.

23. El artículo 3, literal b de la Ley 19.496, que establece normas sobre protección de los derechos de los consumidores, dictamina que es un derecho de los consumidores de obtener información veraz y oportuna sobre los productos o servicios que adquieren en el marco de una relación de consumo.

a simple vista, así como es difícil para el consumidor común saber si un aparato es energéticamente eficiente o no por sus propios medios. De la misma forma, así como quienes los usan son los que soportan los riesgos de esas deficiencias, son los usuarios de artículos energéticos poco eficientes los que pagan los costos de la energía que consumen. Asimismo, si se mantiene la asimetría de información y se compite en el mercado simplemente en precio, ni los productores de dispositivos del «internet de las cosas» ni de artefactos eléctricos tendrán mayores incentivos para hacer que sus artefactos sean más seguros o eficientes.

El sistema chileno da solución a la asimetría de información en el mercado de los aparatos eléctricos a través de la mencionada etiqueta de consumo. Estas son generadas de acuerdo con un procedimiento específico establecido en la regulación correspondiente, por lo que no se deciden simplemente de acuerdo con las preferencias de los productores o distribuidores de los productos regulados. Más importante, estas etiquetas presentan la información de forma sencilla haciéndola accesible. De nada serviría presentar números complejos sobre consumo energético; después de todo, ninguna asimetría de información se soluciona cuando esta no puede ser adecuadamente interiorizada por quien la recibe. El sistema de etiquetas de consumo utiliza simbología intuitiva que hace fácil saber cuándo un producto es eficiente y cuando no.

Un sistema similar puede ser adoptado en los dispositivos del «internet de las cosas». Los productores o distribuidores de los productos tendrían la obligación de someter a evaluación los estándares y una etiqueta sobre estos debería, obligatoriamente, ser añadida antes de ser comercializados. Esta etiqueta simplificada daría información vital a los clientes sobre el nivel de seguridad presente en los productos que adquieren. Si bien es cierto que la forma en que evaluamos los estándares de ciberseguridad cambia constantemente, por lo que tal sistema de evaluación no estaría exento de ciertas complicaciones (es imposible asegurar que un sistema que parece seguro en un primer análisis lo seguirá siendo en el futuro), cuando menos transmitiría a los usuarios información sobre si los estándares básicos de seguridad existentes, cuando el producto fue certificado, están siendo cumplidos.

Un sistema como este también puede ser aplicado para remediar los problemas descritos relativos a la seguridad de aplicaciones, en cuanto un aviso sobre su calificación daría información concreta sobre que riesgos se asumen, resolviendo la asimetría de información.

En resumen, un sistema de etiquetas de calificaciones de seguridad como el presente en la ley chilena con respecto a aparatos electrónicos ayudaría a disminuir las situaciones de riesgo moral en ciberseguridad, siempre y cuando se cumplan dos condiciones en este sistema, que: i) la información sea presentada de forma simple y accesible, de modo que los usuarios puedan fácilmente entenderla e incorporarla en su toma de decisión; y ii) el sistema debe ser regulado de forma detallada, ya que

la forma en que la información es presentada puede influenciar en cómo la misma es entendida.

Ya que los distribuidores o productores de los aparatos del «internet de las cosas» tendrán un incentivo para convencer a los consumidores de que sus productos son seguros, es fundamental estandarizar la forma en que la información es presentada para evitar confusiones derivadas del formato. Por lo demás, es esencial también la intervención de terceros que certifiquen de forma independiente la seguridad de los productos por las mismas razones que el formato de las etiquetas no puede ser dejada al arbitrio de los regulados.

Como se ha explicado con respecto al reporte de incidentes de ciberseguridad, la asimetría de información se presenta en cuanto es la organización que tiene vulnerabilidades en su sistema o sufre un incidente la que está en mejor posición para conocer estos problemas. Estos mismos actores pueden tener un incentivo para no publicar tal información o activamente esconderla. Esto genera una situación de riesgo moralen la que no se socializan las amenazas o incidentes, lo que no permite formular estrategias sólidas de seguridad y produce que los usuarios sigan operando bajo una falsa impresión de protección. Esto puede ser remediado mediante la implementación de un robusto programa de incentivos y protección de los informantes o *whistleblowers*.

Un informante es aquel actor de una organización que revela información con respecto a actividades irregulares dentro de la misma a personas o entidades que puedan enfrentar el problema (Keil y otros, 2010: 789). Son precisamente estos actores los que, con la protección e incentivos adecuados, pueden hacer pública o llevar ante las autoridades competentes información a la que sería difícil de acceder para aquellos fuera de su organización. Esto podría dar solución al problema de asimetría y, en consecuencia, también el riesgo moral al no existir la posibilidad de empujarlo sobre los usuarios.

Tanto en Reino Unido como en los Estados Unidos podemos encontrar ejemplos de esta clase de programas que tienen como fin resolver la falta de acceso a la información por parte de aquellos ajenos a una organización. La Securities and Exchange Comission de Estados Unidos, por mandato de Ley Dodd-Frank de 2010, cuenta con un programa que ofrece recompensas a aquellos que brinden información original que lleve a la persecución exitosa de ciertos delitos, siempre y cuando se logren sanciones superiores a un millón de dólares norteamericanos (Givati, 2017: 117). La Public Interest Disclosure Act de 1998 ofrece protección de carácter laboral en Reino Unido, en la forma de normas antirepresalias, a aquellos empleados que revelan información sobre ciertas actividades ilegales.

Las mismas necesidades que motivan los programas de informantes en los ejemplos abordados, esto es, el lograr acceder a información que de otra forma sería difícil de alcanzar, aplican a nuestros entornos de ciberseguridad. Esto es particularmente bien ejemplificado por el siguiente caso.

En 2020, el gobierno norteamericano sufrió episodios de accesos no autorizados a sus sistemas de información a través de vulnerabilidades en SolarWinds, uno de sus proveedores. El ataque se materializó escondiendo un código malicioso en las actualizaciones del software proporcionado por SolarWinds, en lo que se conoce como un ataque de cadena de suministro.[24]

Fueron las circunstancias de este incidente las que llevaron a miembros de la comunidad a sugerir que el gobierno norteamericano incorporara legislación federal para proveer protecciones específicas a los informantes de vulnerabilidades o incidentes de ciberseguridad (Hammer y Zuckerman, 2021). Esto, pues según ha sido reportado, la administración de SolarWinds en 2017 fue informada por un empleado sobre las vulnerabilidades de su sistema, advertencia que no fue atendida. Complementa esta circunstancia el hecho de que el ataque fue descubierto y hecho público luego de que FireEye, una corporación dedicada a la ciberseguridad y que utilizaba software de SolarWinds, descubrió que estaba siendo víctima de ataques y determinó el origen de estos en actualizaciones del software de SolarWinds.[25]

Este ejemplo es particularmente importante, pues ilustra de forma clara cómo este episodio fue en parte causado por asimetrías de información, y cómo estas podrían haber sido solucionadas por un robusto programa de informantes relativo a incidentes o riesgos de ciberseguridad. En primer término, el hecho de que un empleado haya dado aviso de que los estándares de la compañía no eran los adecuados revela que esta poseía información que sus clientes no tenían. Esta, como lo hemos analizado, es una muestra de riesgo moral. SolarWinds había sido notificada internamente sobre las falencias de seguridad de sus sistemas (tenía información a la que el público no tenía acceso, configurando la asimetría de información) y, por otro lado, no tomó medidas concretas al respecto. De hecho, el empleado que advirtió, Ian Thorton-Trump, renunció un mes después de presentar esta información a la administración de SolarWinds en cuanto sus sugerencias no fueron tomadas en cuenta, permitiendo que el riesgo fuera soportado por sus clientes en circunstancias que estos no podían conocerlo.[26]

Un programa de informantes que hubiera ofrecido protecciones a un empleado que representaba los referidos riesgos o que hubiera ofrecido incentivos para socializarlos efectivamente, tal vez, hubiera motivado una respuesta más expedita de SolarWinds y hubiera prevenido que el ataque se produjera. Sin embargo, los tribunales

24. Reuters, «IT company SolarWinds says it may have been hit in ‹highly sophisticated› hack», 13 de diciembre de 2020, disponible en https://reut.rs/3NLXSIu.

25. CSO, «The SolarWinds hack timeline: Who knew what, and when?», 4 de junio de 2021 disponible en https://bit.ly/3NPNC1M.

26. DailyMail, «SolarWinds was warned THREE YEARS ago that it was prone to a cyberattack–as it's revealed russian hackers also breached major tech and accounting firms, a hospital system and a university», 21 de diciembre de 2020, disponible en https://bit.ly/3x1hFwZ.

norteamericanos en repetidas ocasiones han rechazado solicitudes de extender las protecciones actualmente vigentes a casos en que empleados han sido objeto de represalias por levantar asuntos relativos a ciberseguridad (Hammer y Zuckerman, 2021), lo que en la práctica ha significado un desincentivo a reportar riesgos o incidentes.

El incidente en sí mismo tal vez pudo haber sido prevenido si el empleado de SolarWinds, que en primer término sonó las alarmas, hubiera gozado de un mayor estándar de protección legal o de incentivos para llevar el asunto ante las autoridades competentes, sin embargo, este no fue el caso.

Dadas las particularidades de este problema, en que es difícil simplemente mandatar a los actores involucrados a revelar incidentes de ciberseguridad o incluso problemas detectados (pues son ellos los que suelen tener la mejor posición para acceder a tal información y existe, como hemos visto, un incentivo a esconderla) y pareciera que la solución más efectiva es un sistema de informantes en que actores dentro de las organizaciones tienen las adecuadas protecciones e incentivos para revelar riesgos o incidentes ya materializados. Es importante notar aquí que no solo los incidentes de ciberseguridad que se han materializado deben ser cubiertos por este sistema, sino que también debe cubrir vulnerabilidades y peligros presentes, porque las mismas razones por las que se produce una situación de riesgo moral, en cuanto a incidentes no reportados, pueden reproducirse con respecto a riesgos o vulnerabilidades no informadas.

Referencias

Amir, Eli, Shai Levi y Tsafrir Livne (2018). «Do firms underreport information on cyber-attacks? Evidence from capital markets». *Review of Accounting Studies*, 23: 1177-1206.

Bashir, Masooda, April Lambert, Carol Hayes y Jay Kesan (2015). «Online privacy and informed consent: The dilemma of information asymmetry». *Proceedings of the Association for Information Science and Technology*, 52: 1-10.

Department of Home Affairs (2021). «Security of critical infrastructure Act 2018». Disponible en https://bit.ly/3m7yAsq.

FireEye (2020). «Think fast: Time between disclosure, patch release and vulnerability exploitation-intelligence for vulnerability management, part two». Disponible en https://bit.ly/3amUKUW.

Givati, Yehonatan (2017). «Of snitches and riches: Optimal IRS and SEC whistleblower rewards». *Harvard Journal of Legislation*, 55 (1): 105-142.

Hammer, Dallas y Jason Zuckerman (2021). «SolarWinds breach shows why cybersecurity whistleblowers need protection». *Bloomberg Law*. Disponible en https://bit.ly/3Q6WrXc.

ISACA, (2019). «ISACA state of cybersecurity 2019, part 2: Current trends in attacks,

awareness and governance». Disponible en https://bit.ly/3PR2mPR.

Kaspersky (2019a). «El 67% de las empresas no reporta los incidentes de ciberseguridad». Disponible en https://bit.ly/3N32Pg9.

Kaspersky (2019b). «The state of industrial cybersecurity 2019». Disponible en https://bit.ly/3t4RTGR.

Keil, Mark, Amrit Tiwana, Robert Sainsbury y Sweta Sneha (2010). «Toward a theory of whistleblowing intentions: A benefit-to-cost differential perspective». *Decision Sciences,* 41 (4): 787-812.

Kharbanda, Vipul (2016). «Incident response requirements in indian law». *The Centre for Internet and Society*. Disponible en https://bit.ly/3NSV1O5.

Mankiw, Gregory (2002). *Principios de economía*. Madrid: McGraw-Hill/Interamericana de España, S.A.U.

Morgner, Philipp, Christoph Mai, Nicole Koschate-Fischer, Felix Freiling y Zinaida Beneson (2019). «Security update labels: establishing economic incentives for security patching of IoT consumer products». Disponible en https://arxiv.org/abs/1906.11094.

Schneier, Bruce (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. Nueva York: W.W Norton & Company.

Smith, Margaret (2019). «Information asymmetry meets data security: The lemons market smartphone apps». *Policy Perspectives*, 26.

Sunstein, Cass, Jolls Christine y Richard Thaler (1998). «A behavioral approach to law and economics». *Stanford Law Review*, 50: 1471-1550.

Thaler, Richard (2017). *Portarse mal*. Ciudad Autónoma de Buenos Aires: Paidos.

Vagle, Jeffrey (2020). «Cybersecurity and moral hazard». *Standford Technology Law Review*, 23 (1): 71-113.

Agradecimientos

Se agradece su asistencia y revisiones a los miembros del cuerpo académico del Diplomado de Ciberseguridad de la Facultad de Derecho de la Universidad de Chile.

Sobre el autor

Sebastián Bilbao Pérez es abogado. Licenciado en Ciencias Jurídicas y Sociales por la Universidad de Chile. Diplomado en Ciberseguridad y en Protección de Datos Personales, por la Universidad de Chile. Su correo electrónico es sbilbao@ug.uchile.cl. https://orcid.org/0000-0002-1274-9516.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

DIRECTOR

Daniel Álvarez Valenzuela

(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).