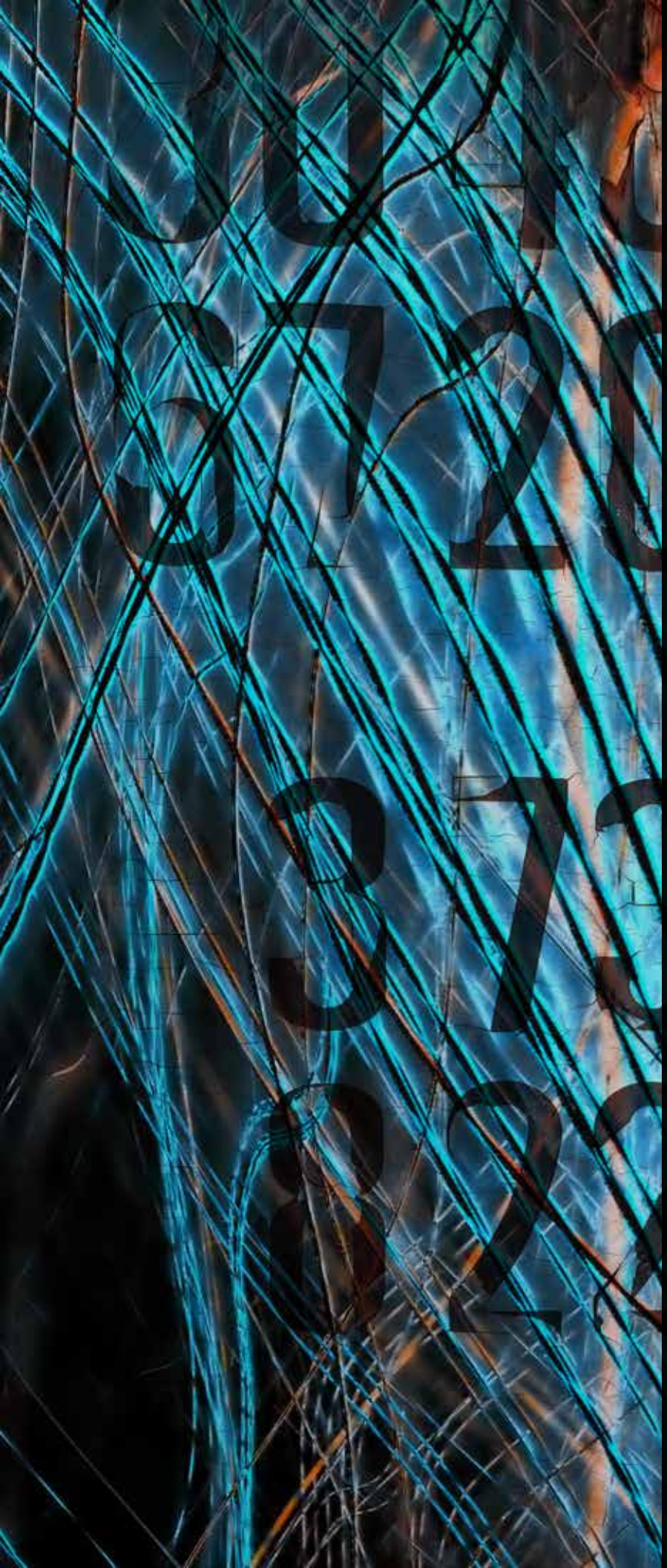


LA ECONOMÍA DIGITAL

EN CHILE 2016

INFORME
PRELIMINAR

CENTRO DE ESTUDIOS
DE LA ECONOMIA DIGITAL,
CÁMARA DE COMERCIO
DE SANTIAGO

CAMARA DE COMERCIO DE SANTIAGO

EQUIPO DE INVESTIGACIÓN ECONOMÍA DIGITAL EN CHILE 2016

GEORGE LEVER, Director Centro Economía Digital
YERKA YUKICH, Secretaria Ejecutiva Centro Economía Digital
MARÍA DEL PILAR CRUZ, Economista Senior CCS

AGRADECIMIENTOS ESPECIALES

Jasna Seguic y Marcos Christensen de comScore; Carolina Gutiérrez de Criteo; Milena Flament y Osbaldo Franco de eMarketer; Patricio Majluf y Max Valenzuela de Google; Raul Arrieta de Gutiérrez y Arrieta; Olga Britto de IAB Colombia; Marie Clare Puffett de IAB Europa; Gabriel Richaud de IAB México; Graciela Rubina de IAB Perú; Marie France Bourgeois de IAB Uruguay; Beatriz Muñoz y Marco Tapia de Ipsos; Luz García y Pamela Arellano del Ministerio de Economía; Juan Luis Núñez y Matías Staeger de Fundación País Digital; Rubén Aros de Taisa; Daniel Halpern de TrenDigital; Francisco Milian de VISA.

LA ECONOMÍA DIGITAL

EN CHILE 2016

INFORME

PRELIMINAR

CENTRO DE ESTUDIOS
DE LA ECONOMIA DIGITAL,
CÁMARA DE COMERCIO
DE SANTIAGO

CAMARA DE COMERCIO DE SANTIAGO

CAPÍTULO 01

LA ECONOMÍA DIGITAL EN EL DESARROLLO ECONÓMICO DE CHILE

Hace unas décadas atrás el mundo digital o de alta tecnología era sólo parte de las creaciones literarias encarnadas en clásicos como la Máquina del Tiempo, Odisea en el Espacio o en la Saga de la Fundación de Asimov. Ocupaba fundamentalmente el campo de la ficción, representando lo inalcanzable e inconmensurable.

Por vías impensadas, lo que entonces era ficción, hoy se ha hecho parte de una realidad concreta, que abarca las más diversas esferas del quehacer humano, robusteciendo la acumulación de capital en sus más variadas formas. La era tecnológica en el siglo XXI ha penetrado de manera transversal a la sociedad y a la economía, impulsando no sólo la trasferencia de datos e información, sino también el desarrollo del comercio, la banca, la industria, la educación, la medicina y las ciencias, modificando en forma radical el interactuar de individuos, empresas y gobiernos y transformando mercados. Ha permitido reducir los costos de búsqueda, de replicar contenidos, de innovar, de instaurar la economía del aprendizaje, integrando a través de redes digitales a los consumidores y mercados del mundo.

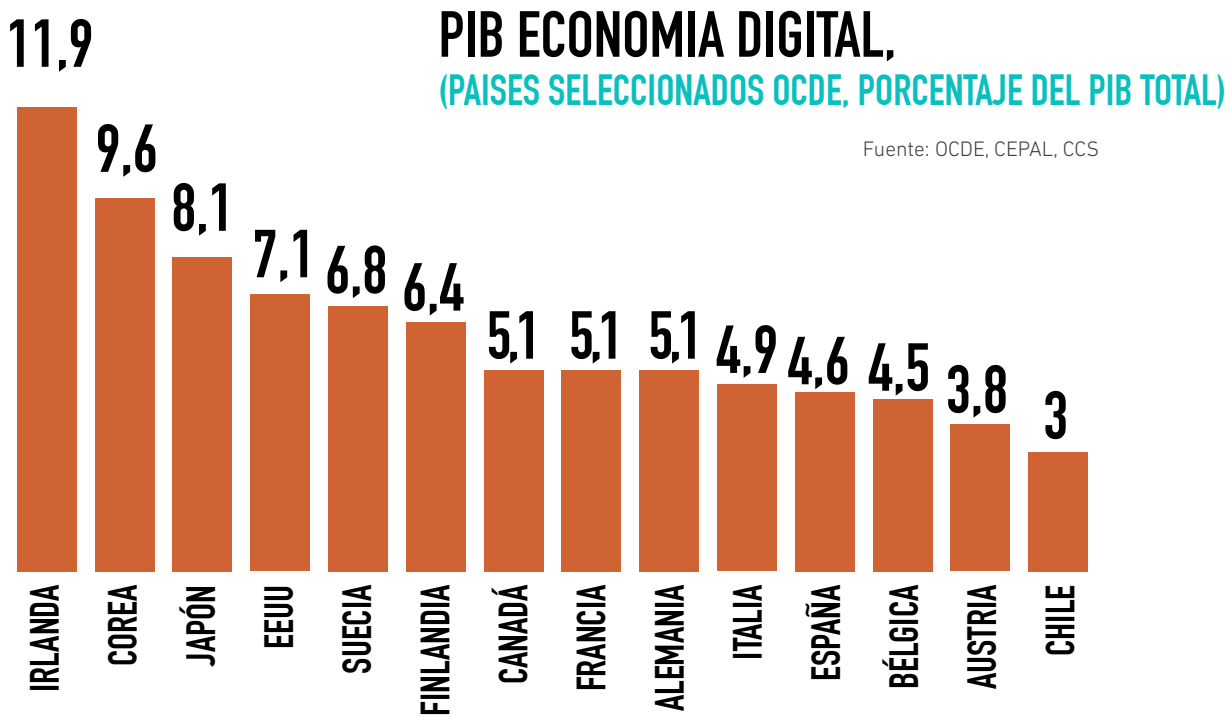
La tecnología, a final de cuentas, nos ha sorprendido porque incluso ha ido en direcciones inesperadas. Ha contribuido a hacer más rápido, mejor o con menos esfuerzo, lo mismo que se hacía antes, pero también a abrir nuevos caminos, plantear nuevos problemas y dar nuevas respuestas, acelerando aún más el mismo proceso de progreso técnico. La era de las redes y la inteligencia artificial florecen en forma exponencial, disparando los estándares de la ficción a conceptos como la singularidad tecnológica, que apunta a que hacia mediados de este siglo un solo computador excederá el poder cerebral de todos los seres humanos juntos.

A estas alturas, no hay áreas grises, ya que definitivamente las economías que no se adhieran seriamente a las tendencias del mundo digital corren el riesgo de quedar rezagadas del desarrollo que tendrá el resto del mundo. El universo de los partícipes de la e-economy, es decir, las empresas, los consumidores y gobiernos, están sometidos a la fuerte presión de administrar la ola de trasformaciones digitales para mejorar sus niveles de eficiencia y sobrevivir a los cambios disruptivos.

En estas circunstancias, el efecto de catalizador en la economía mundial ya no es posible de pasar por alto. Estudios recientes ratifican que el ecosistema digital tiene un importante efecto en impulsar el desarrollo de los países, señalando que un crecimiento de 20% en la inversión en tecnologías de la información tiene la capacidad para elevar en un punto porcentual el crecimiento del PIB, o equivalentemente, en un tercio el crecimiento mundial[1]. Esto muestra el enorme poder que ha alcanzado la economía digital, que ha emergido en un relativamente breve lapso de tiempo, de no más de 15 o 20 años.

Las mediciones respecto del tamaño de la economía digital indican que en Chile representa alrededor del 3% del PIB[2], similar al que tiene la industria alimenticia, el sector silvoagropecuario o los servicios de electricidad, agua y gas. Hacia el año 2020 su incidencia continuará expandiéndose hasta alrededor de 4,5%.

En los países avanzados, tales como Japón, Estados Unidos y la EuroZona, la economía digital es del orden de 7% al 8% del PIB, y hacia fines de la década podría acercarse a un 12%.



[1]Fuente: Índice de Conectividad Global 2015 (ICG), Huawei, McKinsey&Company.
[2]Fuente: Índice País Digital.

DIFICULTADES DE MEDIR LA ECONOMÍA DIGITAL Y SUS EFECTOS EN LA PRODUCTIVIDAD

El consenso especializado coincide en definir el ecosistema de la economía digital como aquel conformado por la infraestructura de telecomunicaciones, la industria de tecnologías de comunicación e información (en software y hardware) y las actividades económicas y sociales desarrolladas a través de internet, como por ejemplo, el comercio electrónico, contenidos digitales y medios de información.

El exorbitante avance de este nuevo hábitat tecnológico y sus difusas fronteras ha hecho difícil medirlo y evaluar sus impactos en el resto de la economía. La percepción de la población es que estos avances han contribuido en forma muy importante al bienestar, pero sin duda la métrica tradicional no está siendo capaz de identificar con precisión su impacto en el PIB. El riesgo de ello es errar en las grandes decisiones estratégicas, ya que lo que medimos afecta nuestro campo de opciones[3], y lo que no medimos también. La importancia de las mediciones precisas es que colaboran con las buenas políticas.

Uno de los aspectos más complejos de cuantificar es el valor agregado de los múltiples servicios o aplicaciones disponibles en Internet y para los cuales no existe un precio de transacción. Son servicios gratuitos entregados a través de las redes, como Google, Wikipedia, YouTube y Facebook, entre otros. Mientras el consumo de estos servicios digitales crece y se expande aceleradamente en áreas tan diversas como educación, esparcimiento, comercio, arte y literatura, se toma conciencia de lo difícil y gravitante que es medir su contribución al consumo o a la inversión en capital humano.

El consumo de lo gratuito es difícil de capturar en la medición de Cuentas Nacionales (PIB), que utiliza transacciones monetarias como base de medida. La paradoja además es que estos servicios gratuitos se han tornado muy poderosos y pueden estar incluso compitiendo con servicios sustitutos sí afectos a pago, amenazando su competitividad y viabilidad en el tiempo. Tales casos se han observado, por ejemplo, en la industria de telefonía tradicional y el surgimiento de operadores gratuitos como Skype y WhatsApp.

Mediciones para Estados Unidos respecto del PIB atribuible a estos servicios gratuitos por internet han concluido que representan algo menos de un 1% del PIB de esa economía[4]. Para poder efectuar los cálculos, han estimado el valor de estos servicios digitales en forma indirecta, utilizando como medida de precio el espacio de tiempo que los consumidores están dispuestos a asignar a su consumo. La investigación arrojó que el tiempo utilizado en Internet por los cibernautas en EEUU ha crecido a tasas del orden de 36% desde 2005 en adelante, llegando a aproximadamente 8 horas promedio por semana. Estas preferencias revelan cuan elevados han llegado a ser los beneficios obtenidos de estos servicios digitales, aunque por ahora no sabemos exactamente su contribución al PIB y a la productividad multifactorial.

---

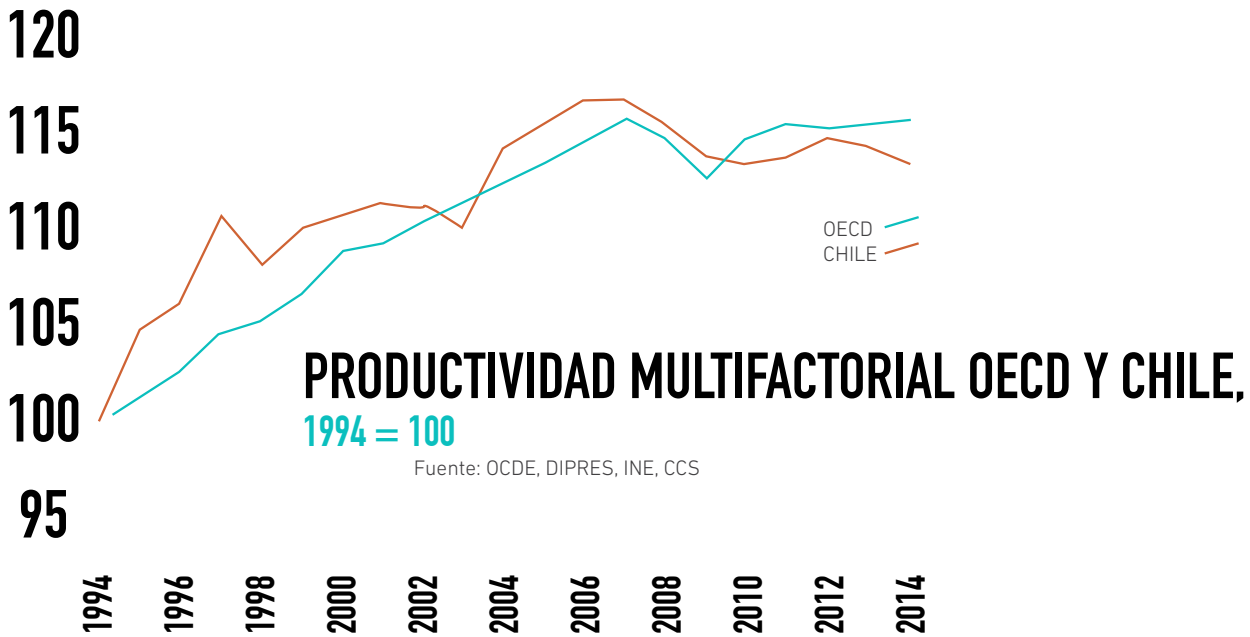
[3] Joseph Stiglitz: El fetichismo del PIB
[4] The Attention Economy: Measuring the Value of Free Digital Services on the Internet. Erik Brynjolfsson, MIT and Center for Digital Business.

LA COMPLEJIDAD DE MEDIR LA INVESTIGACIÓN Y DESARROLLO EN LA ERA DIGITAL

El desarrollo tecnológico va inequívocamente de la mano con el énfasis que dan las empresas a la investigación y desarrollo (I+D), y por ello también su medición se ha hecho absolutamente necesaria. Recientemente los países europeos iniciaron el tratamiento del gasto en I+D como inversión, respondiendo a los estándares dictados por las Naciones Unidas. Chile se apronta también para producir este mismo estándar de cuentas, lo que podría contribuir a elevar los montos de formación bruta de capital en, estimativamente, alrededor de 1%.

El impacto de la economía digital en el acervo de conocimiento e inteligencia, llama también a poner atención sobre la inversión en intangibles como lo es el capital gerencial, estratégico y directivo. La era digital impactará de manera singular la forma cómo las economías acumulan capital, migrando desde las plataformas eminentemente tangibles como maquinarias, equipos y construcciones, hacia plataformas intangibles, representadas por marcas, confianza o accountability. Antecedentes para la economía norteamericana indican que la inversión en intangibles en la actualidad representa alrededor el 13% del PIB y la inversión en tangibles, sólo un 7%. En 1977 la situación era inversa, la inversión en tangibles era la predominante, un 9% del PIB, y la intangible era sólo un 5% ó 6% del PIB,

Los importantes problemas de estancamiento de productividad por los que atraviesa el mundo en la actualidad parecen no comprenderse bien, frente a los enormes avances en materia tecnológica y digital. Esto ha plantado el desafío de lograr detectar y medir a tiempo las enormes transformaciones que vive la economía y la sociedad, no solo para saber cuál es el grado de avance económico que finalmente conlleva la era digital, sino también para aguzar la orientación de las grandes políticas y definiciones estratégicas a las que llama.



PRODUCTIVIDAD MULTIFACTORIAL OECD Y CHILE,

1994 = 100

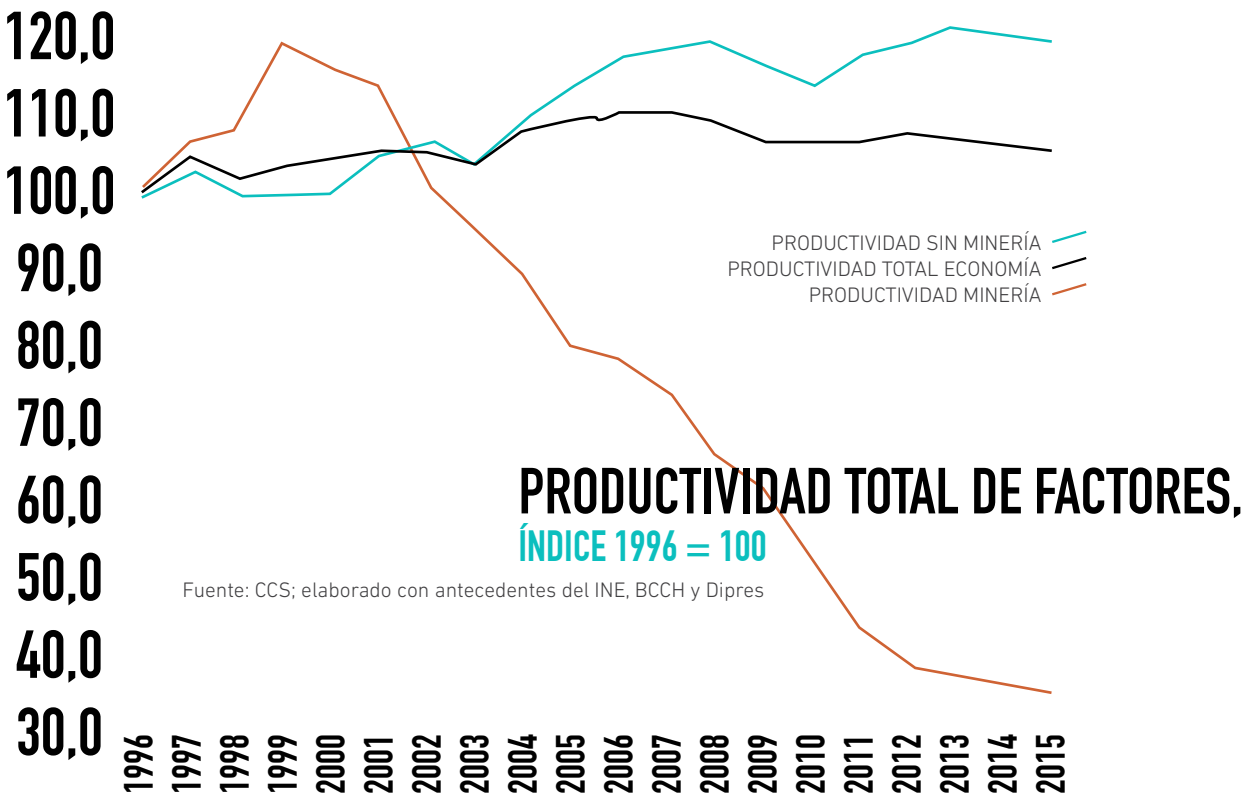
Fuente: OCDE, DIPRES, INE, CCS

A partir de la paradoja de la productividad popularizada en los ochenta por el Nobel de economía Robert Solow ("podemos ver la era de la computación en todas partes, menos en las estadísticas de productividad"), la discusión en torno al impacto de las TICs en el crecimiento ha estado presente en el debate micro y macroeconómico.

La aparente paradoja, no obstante, parece haber sido resulta por el mismo desempeño de la productividad total de factores (PTF) en Estados Unidos durante los noventa. Entre 1995 y 2000, la PTF aumentó a una tasa promedio del 1,5% anual en ese país, dejando atrás los pobres registros apenas superiores al medio punto porcentual anual de la década anterior.

La explicación más comúnmente aceptada es que el fuerte cambio tecnológico debe ir asociado a la acumulación de capital intangible necesario para potenciar las ganancias en productividad. Este capital intangible, a su vez, se desarrolla a partir de los cambios institucionales, organizacionales y culturales requeridos para que el sistema económico y social saque real partido del nuevo acervo tecnológico, cosa que ocurrió en EEUU a partir de los noventa.

La actual paradoja de productividad que viven países menos avanzados, como los latinoamericanos, se explica al menos en tres factores: primero, en la fuerte caída de la productividad de los sectores exportadores de materias primas (el caso de la minería en Chile); segundo, la falta de estrategias nacionales agresivas en materia de innovación; y tercero, en el rezago en la construcción del capital intangible necesario para activar el potencial digital. Esto no significa que estos países aún no hayan percibido beneficios del acceso a las tecnologías digitales. De hecho, en algunos de ellos (como en Chile) la productividad no minera ha mostrado avances, con ejemplos interesantes en sectores de relativa intensidad en el uso de TICs, como el financiero, comercio y telecomunicaciones, entre otros.



PRODUCTIVIDAD TOTAL DE FACTORES,
ÍNDICE 1996 = 100

Fuente: CCS; elaborado con antecedentes del INE, BCCH y Dipres

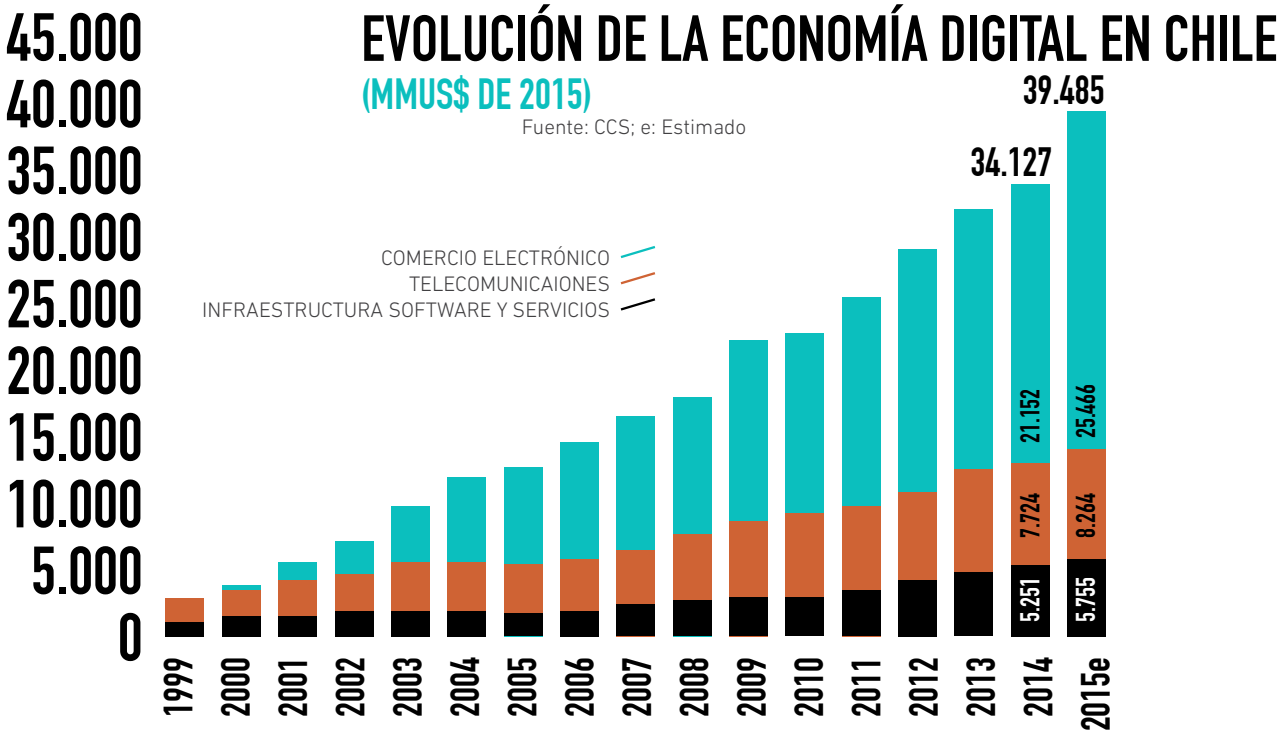
CAPÍTULO 02

EVOLUCIÓN DE LA ECONOMÍA DIGITAL EN CHILE

Tal como se comentó en el capítulo anterior, las metodologías de medición de la economía digital se encuentran en pleno desarrollo a nivel internacional. Algunos países han desplegado esfuerzos por estimar cuentas satélite para las TICs (caso de Chile en 2005), mientras que otros han buscan los instrumentos adecuados para medir la dimensión transaccional del sector.

Desde fines de los años noventa, la CCS ha construido una serie que mide la Economía Digital chilena como la suma de las ventas de infraestructura TIC, software, servicios, telecomunicaciones y comercio electrónico.

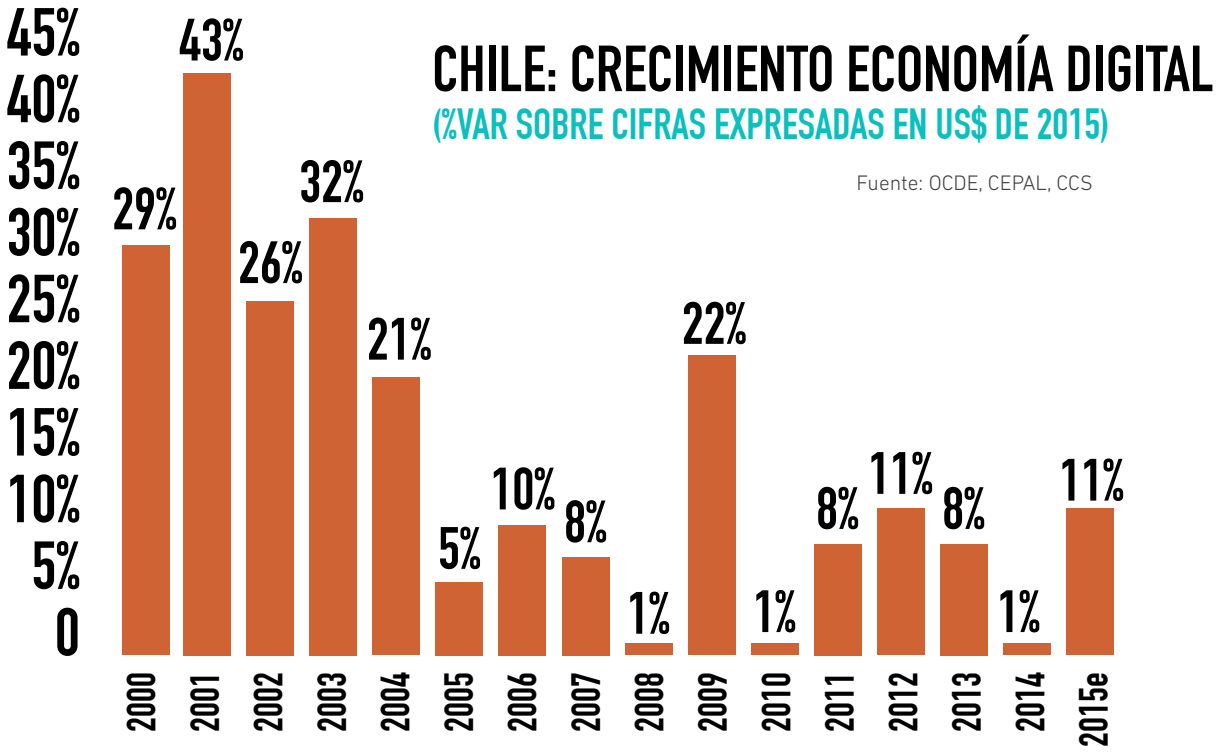
De acuerdo a estas estimaciones, la Economía Digital habría alcanzado ventas totales por casi US$ 40 mil millones en 2015, un 11% por sobre lo registrado el año anterior[1]. Tal como ocurre desde mediados de la década pasada, su principal componente transaccional está dado por el comercio electrónico, con ventas que superan los US$ 25 mil millones y que representan un crecimiento del 15%. Gran parte de estas ventas provienen, a su vez, de las transacciones B2B, entre empresas y entre éstas e instituciones públicas.



[1] Todas las variaciones se miden sobre los montos expresados en dólares de 2015.

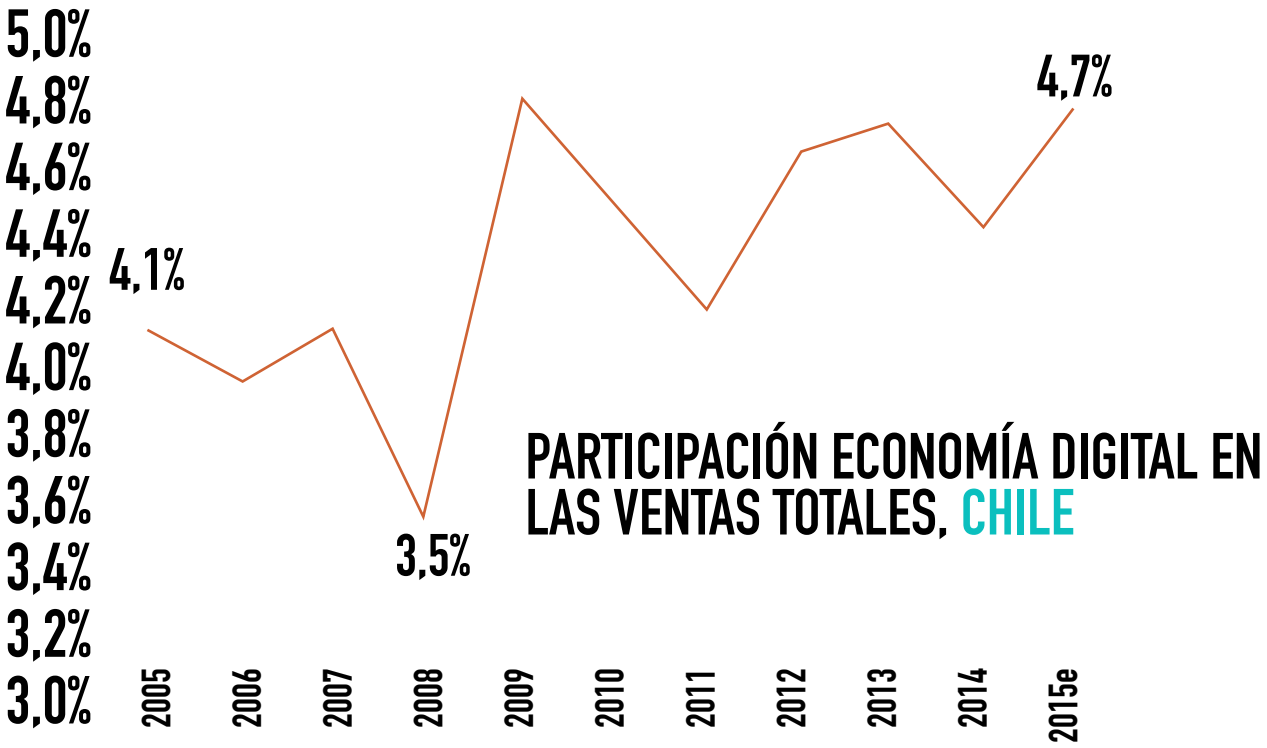
El segmento de telecomunicaciones, que ha sufrido grandes transformaciones en su composición (desde telefonía fija hacia móvil, de comunicaciones de voz a tráfico de datos y servicios cloud), alcanzó ventas estimadas cercanas a los US$ 8.300 millones; mientras que los ingresos por infraestructura, software y servicios superaron los US$ 5.700 millones. Ambos segmentos, a diferencia del comercio electrónico, mostraron crecimientos de un dígito, estimados en 3 y 5 por ciento, respectivamente.

En los últimos años, el crecimiento de la economía digital ha tendido a converger (no exenta de volatilidad) hacia tasas en torno al 10%, primer síntoma de consolidación luego del vertiginoso ritmo observado durante la primera mitad de la década pasada, por sobre el 20% anual.



De acuerdo a los datos recopilados en la Cuenta Satélite de Tecnologías de Información y Comunicación en Chile, desarrollado por el Ministerio de Economía, el INE, la Subsecretaría de Telecomunicaciones, el Ministerio de Educación y CORFO, el Producto Interno Bruto generado por el sector TIC alcanzaba a US$ 3.199 millones en 2004, monto que representaba el 3,4% del PIB total del país. Como se mencionó en el capítulo anterior, las cifras más recientes publicadas por la OCDE, en tanto, sitúan esta participación en torno al 3%, muy por debajo de países como Irlanda (12%), Corea (10%), Japón (8%) y Estados Unidos (7%).

Según las estimaciones del tamaño de la Economía Digital de la CCS, en 2004 el peso del sector dentro de las ventas totales en la economía alcanzaba a alrededor de un 4 por ciento. Diez años después esta participación avanza hacia el 5 por ciento, si bien las dificultades de medición de las múltiples nuevas actividades basadas en digital hacen pensar que su tamaño y relevancia es evidentemente mayor.

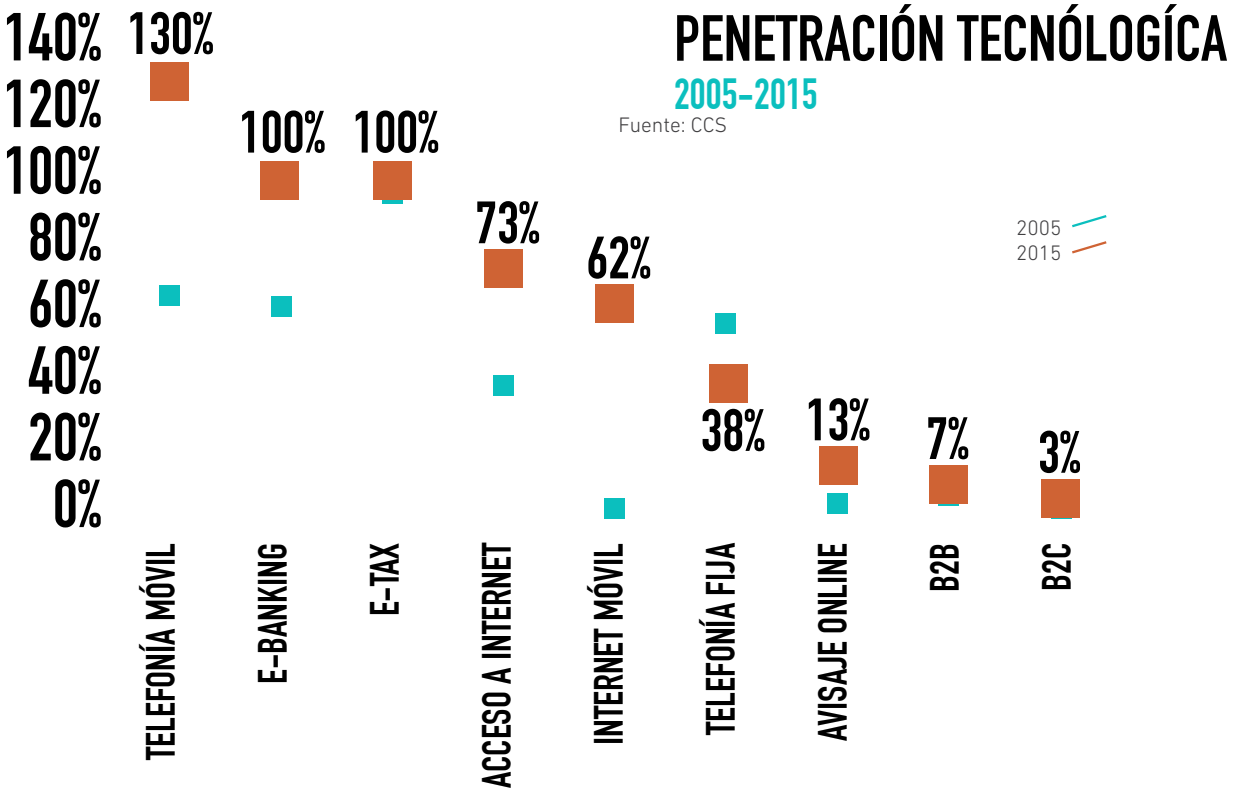


PARTICIPACIÓN ECONOMÍA DIGITAL EN LAS VENTAS TOTALES, CHILE

La observación de los últimos diez años entrega abundante información que ayuda a comprender la dinámica de los cambios provocados por la convergencia de las tecnologías de información y comunicación. Por ejemplo, en 2004 la telefonía móvil superaba por primera vez a la fija en penetración y el 2005 ya llegaba al 65% de la población. La sustitución de las comunicaciones fijas por las móviles fue un proceso que tardó aproximadamente quince años. En su momento, fue evaluado como una de las transformaciones más notables y veloces del mercado de las comunicaciones. Después de todo, a la telefonía fija le había tomado más de 120 años alcanzar el mismo logro (60 por ciento de la población). Diez años después, la telefonía fija se ha retirado hasta por debajo del 40% de la población, mientras que el número de suscripciones móviles equivale al 130% de los habitantes.

Un proceso aún más rápido es el que ha experimentado la Internet móvil, que se aproxima al 60% y que casi con certeza superará a la conectividad fija en el corto plazo.

La declaración de impuestos por Internet, un adelanto emblemático y precoz del gobierno electrónico nacional, ya alcanzaba al 96% de los contribuyentes en 2005. Cuatro años antes, apenas superaba el 40 por ciento. Debido a su temprana adopción, que lo llevó a ser uno de los primeros modelos en madurar, los avances en términos de penetración han sido obviamente modestos en la última década, llegando a superar el 99,5% de adopción en el último año. En este caso, el modelo de adopción está marcado por la estructura del mercado, en el que existe un solo operador (el Servicio de Impuestos Internos), con capacidad para generar los estándares transaccionales, lo que facilita su masificación.



La banca electrónica es otro modelo que ha logrado madurar en términos de adopción. Iniciada a fines de los noventa, en el año 2000 ya alcanzaba al 20% de los cuentacorrentistas y a fines de esa década al 100%. A diferencia del modelo tributario, en este caso conviven varios operadores, la mayoría de gran tamaño. Pese a ello, también se trata de una industria que es capaz de generar estándares que tienden a tener rápida adopción en la demanda. En ambos casos, el canal físico, lejos de agregar valor, impone costos a los usuarios (tiempo, desplazamientos, filas en caja, etc.)

Esta última característica, que acelera la migración de determinados servicios al canal online, tiende a generar barreras en otros, como en el caso del comercio electrónico, obligado a competir con el fuerte arraigo de los hábitos de compra al canal físico, que une la experiencia de consumo con la recreacional. Esto explica en parte las aparentemente bajas tasas de penetración de las compras online sobre las totales, que en Chile alcanzan al 3 por ciento. Si se mide como porcentaje de consumidores que realiza compras online, no obstante, esta penetración sube al 20 por ciento y escala al 30% como porcentaje de los usuarios de Internet.

El marketing digital es otra área que ha avanzado con velocidad en los últimos años. Su participación en el gasto publicitario aumentó desde apenas un 1 por ciento en 2005 a más del 13 por ciento en 2015. Al medirlo en términos de gasto, sin embargo, se pierde de vista el bajo costo relativo del marketing digital en relación a otros canales, como la televisión. Es decir, con la misma inversión monetaria es posible desarrollar más acciones de marketing en el canal online.

Más significativo aún es el hecho de que en la actualidad prácticamente no existen acciones de marketing que no consideren el canal digital. El arrollador avance de la conectividad móvil, además, garantiza un despliegue aún más agresivo del marketing digital en los próximos años.

CAPÍTULO 09

ASPECTOS LEGALES DE LA ECONOMÍA DIGITAL

El desarrollo de nuevas tecnologías sigue sorprendiendo con sus avances año a año. El mundo digital se ha vuelto complejo, diversificado y la vez especializado, ofreciendo nuevos campos de operación para proveedores de bienes y servicios.

Este crecimiento ha gatillado que en la industria se conciban nuevos modelos de negocios impulsados, principalmente, por las ventajas que ofrecen las nuevas tecnologías. Así, por ejemplo, ha aumentado la contratación por medio de plataformas electrónicas, configurándose el modelo de negocios conocido como *e-commerce.* Luego su evolución incluso ha traspasado la barrera de los computadores conquistando la tecnología móvil a través de *smartphones y tablets* concibiéndose como nuevo modelo el *m-commerce.*

Con este fenómeno de crecimiento, se produce, de una parte, que la actividad judicial, legislativa y regulatoria esté siempre varios pasos atrás, y que sea en gran parte, la regulación via contractual, el modo inmediato de abordar el acelerado desarrollo tecnológico, y la mitigación de las brechas con el derecho tradicional. De otra parte, la inmensidad de variables tecnológicas que surge día a día hace que la tarea de abordar todo el desarrollo tecnológico para su estudio y análisis se vuelva casi imposible.

En las páginas que siguen, se analiza, desde una perspectiva jurídica, conforme a la normativa vigente, aquellos desafíos legales, ventajas y riesgos a tener en consideración para aplicar buenas prácticas a propósito de algunos de los temas digitales que consideramos como más relevantes para la industria este año.

Merece, por lo tanto, ser desarrollado desde una perspectiva legal dentro de este Informe de Economía Digital 2015, los siguientes temas: Protección de Datos, *Cloud Computing, Internet de las Cosas, Drones* y Sistemas de Pago Electrónico.

PROTECCIÓN DE DATOS PERSONALES

El desarrollo de las tecnologías de la información y comunicación ha posibilitado el tratamiento automatizado de la información en volúmenes que hasta hace muy poco no parecía posible. Junto a ello, el paso desde grandes sistemas de procesamiento de información in house hacia sistemas de cloud computing han permitido la reducción de los costos, la eliminación de las fronteras territoriales permitiendo que cualquier persona pueda comenzar a tratar información relacionable y consultable en tiempo real. Así, información que aisladamente parecía no tener gran relevancia pasó a configurarse como un elemento que permite alcanzar resultados sustancialmente diferentes sobre el conocimiento de las personas. El moderno procesamiento de información permite delinear estructuras y construir perfiles personales que por medio de la simple observación de un sujeto nunca hubiera sido posible.

Por lo anterior es que la protección de datos personales ha pasado a ser parte del pensamiento moderno de los derechos humanos, dando pie a la que se reconfigure el alcance de la privacidad. Fundamentalmente porque el tratamiento de datos personales aparece como unos de los principales contaminantes de la libertad a partir de la segunda mitad del siglo XX. El alcance originario del derecho a la privacidad, en su expresión de tutela negativa, derecho a ser dejado sólo, ha evolucionado para dar paso a una tutela dinámica en que el derecho se caracteriza más bien por la posibilidad que tiene el titular de controlar el uso que otros hacen de las informaciones que me afectan, por poder realizar las elecciones vitales sin la interferencia del control público y la estigmatización social, por tener la libertad en las propias elecciones existenciales, por tener el control sobre las propias informaciones y a determinar libremente las modalidades de construcción de la propia esfera privada y el derecho a no ser simplificado, transformado en objeto, valorado fuera del propio contexto.

ALCANCE DEL DERECHO A LA PROTECCIÓN DE DATOS

El derecho a la protección de datos consiste en la protección jurídica que se otorga a los individuos respecto de la recogida, almacenamiento, utilización, transmisión y cualquier otra operación realizada sobre los datos concernientes a su persona, a fin de cuidar que su tratamiento se realice con lealtad y licitud de manera que no se afecte indebidamente derechos del titular de los datos personales objeto de dicho tratamiento.

La protección se origina, entre muchas otras razones, en la constatación de la posibilidad cierta de tomas de decisiones arbitrarias en contra de las personas a partir de datos registrados en sistemas manuales y automatizados de tratamiento de información. Ello incluso lleva a que en casos concretos las personas no ejerzan ciertos derechos por temor a que tales actuaciones queden registradas en un sistema como dato personal y por ende susceptible de ser conocidos y utilizados con los consecuentes riesgos y/o menoscabos para el mismo o sus relacionados en cuanto a sus oportunidades de desarrollo personal.

NATURALEZA JURÍDICA DEL DERECHO A LA PROTECCIÓN DE DATOS

Este derecho se ha ido configurando en el mundo desarrollado como un derecho humano instrumental en el sentido de que aquello realmente protegido no son los datos sino la persona titular de ellos. Dicho de otro modo, lo que se otorga es un estatuto de garantía a los datos personales para que su tratamiento sea efectuado bajo las condiciones necesarias para dar un adecuado nivel de protección a quienes son titulares de los mismos. Se reconoce así que el tratamiento de datos es necesario para posibilitar el intercambio económico y la mejora en la prestación de los servicios (públicos y privados), pero asimismo se evidencia la importancia de que el tratamiento se realice bajo estándares de seguridad y calidad, que son los que permiten resguardar los derechos de los afectados por el tratamiento de este tipo de datos.
Es importante tener presente que este derecho ampara toda información relativa a persona determinada o determinable, sobre la base de que no existen datos carentes de interés, pues cualquiera de ellos, al ser sometidos a un proceso de tratamiento y ser cruzados con otros datos, pueden perfectamente cobrar mayor relevancia.

De este modo, el derecho a la protección de datos se configura asociado a la autodeterminación, la cual, para estos efectos, se configura como autodeterminación informativa que consiste en el derecho de todo individuo a controlar la obtención, tenencia, tratamiento, uso y transmisión de los datos relativos a su persona.

En ningún caso se trata de un derecho absoluto sino que, como todos los derechos, tiene las restricciones necesarias para hacerla compatible con los derechos de terceros y, en general, con los intereses de la sociedad. De hecho la protección de datos personales no deber prohibir ni entorpecer el tránsito de los datos, sino que ha de configurar el marco de condiciones y estándares de calidad que permitan la libre circulación de éstos en forma segura.

ESTÁNDAR INTERNACIONAL

Definir el estándar que debe cumplir nuestro país en materia de protección de datos pasa por establecer cuál es el parámetro que los países y asociaciones que forman parte de nuestra esfera de influencia nos exigen para poder integrarnos realmente con ellos. Sea simplemente porque se le mire bajo un prisma de utilitarismo comercial o bien porque nos interesa realmente incrementar los niveles de protección de los derechos fundamentales.

Para el análisis de este punto resulta necesario considerar los principales instrumentos normativos de nuestro entorno de referencia habitual y al de las asociaciones a las que pertenecemos o deseamos incorporarnos. Así, habrá que estar a las directrices, recomendaciones y normas de la Organización para la Cooperación y el Desarrollo Económico, la Unión Europea, la Organización de las Naciones Unidas y la Asociación de Países del Asia Pacífico.

De la revisión de dichos instrumentos es posible advertir que existe una significativa coherencia y consistencia respecto a los elementos que han de configurar el estándar de protección de datos que ha de satisfacer nuestro país.

Para fijar el estándar de protección de datos que ha de cumplir Chile, habrá que tener especial consideración por la normativa proveniente de la Unión Europea y especialmente la Directiva 95/45/CE y el Reglamento General de Protección de Datos. Ello por cuanto dicha normativa es la que impone una mayor exigencia a nuestro país y, consecuentemente, al satisfacer dicho estándar nuestro país queda en condiciones de de dar cabal cumplimiento a los requisitos que nos impone todo nuestro entorno de referencia, no sólo la Unión Europea.

De lo que se trata es que Chile cuente con un Sistema de Protección de Datos, entendiendo que éste es un sistema complejo de protección de las personas que, junto con establecer y plasmar principios, implanta mecanismos que permiten tutelar la efectividad de su cumplimiento. De este modo, es indispensable que la regulación no sólo consagre derechos, sino que permita, además, hacerlos efectivos de manera sencilla, con bajos costos transaccionales y en sede administrativa. El Grupo de Trabajo de Protección de la Unión Europea ha sostenido que las normas de protección de datos sólo contribuyen a la protección de las personas si efectivamente se cumplen en la práctica, por lo que resulta necesario considerar no sólo el contenidos de las normas aplicables a los datos personales, sino también el sistema utilizado para asegurar la eficacia de dichas normas.

Así, los objetivos de un Sistema de Protección de Datos son básicamente tres:

A. Ofrecer un nivel satisfactorio de cumplimiento de las normas. Para ello la atención debe centrarse en que los responsables del tratamiento de datos personales conozcan clara y precisamente cuáles son sus obligaciones. Por otra parte, que los titulares de datos tengan claridad respecto de sus derechos y de los medios disponibles para asegurar su cumplimiento. Finalmente, es necesario que el sistema de protección considere sanciones efectivas que permitan disuadir las malas prácticas e ilícitos en la materia.

B. Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos. Esto está orientado a que los interesados deben tener la capacidad de hacer valer sus derechos con rapidez, eficacia y sin que los costos asociados aparezcan como un desincentivo para actuar. En este punto la Unión Europea considera indispensable la existencia de un mecanismo institucional que permita investigar las denuncias de manera independiente.

C. Ofrecer vías adecuadas de recurso a quienes resulten perjudicados por la no observancia del cumplimiento de las normas. Esto se centra en que el afectado debe poder obtener una resolución judicial o un equivalente jurisdiccional que reconozca la infracción y que eventualmente ordene el pago de las indemnizaciones e imponga las sanciones.

SITUACIÓN ACTUAL

El tratamiento de los datos personales se encuentra regulado en Chile por la Ley 19.628 sobre protección de la vida privada. Sin embargo, la normativa tiene graves defectos que han avalado la contaminación de las libertades personales por el inadecuado tratamiento de los datos personales.

Los defectos normativos no son otra cosa que la consecuencia de una ley que en su origen tenía por objeto, contribuir a disminuir el riesgo país, al asociarse el tratamiento de los datos con un instrumento orientado al orden público económico. Es así como la ley más que implementar un sistema de protección de datos personales lo que hizo, principalmente, fue regular el uso del dato económico. El resultado ha sido la instauración de un marco jurídico altamente permisivo, débil en cuanto a las posibilidades de control que pueden realizar tanto los titulares de datos como terceros y limitado en cuanto a la posibilidad de aplicar sanciones a las infracciones a los deberes que la ley establece.

Si bien en un primer momento ello resultó de utilidad para el mercado, por cuanto proliferaron las más variadas bases de datos, hoy en día estamos ante un mercado que no asegura datos de calidad, que deja sistemáticamente en riesgo los mismos derechos que vino a proteger, además de afectar directamente a las personas titulares de dichos datos.

Con ello, todo el sistema de derechos establecidos en la Constitución y las leyes se ha debilitado, lo que se hace más evidente y grave a medida que avanzan las posibilidades tecnológicas. Socialmente se ha convertido casi en un hecho aceptado el que las personas se puedan ver afectadas por decisiones arbitrarias tomadas por organismos públicos y/o privados en base a datos que constan en alguna parte y que no reflejan la verdadera situación de la persona.

Así, se ha llegado al extremo de ver casi con naturalidad el uso abusivo que se hace de los datos de las personas, lo que se agrava más aún con los resultados judiciales que dejan al descubierto que la ley no es capaz de amparar los derechos de los titulares de datos, tanto por problemas sustantivos como procedimentales.

Finalmente, la falta de Chile con sus compromisos con la Unión Europea evidencia un entorpecimiento de las relaciones comerciales con dicho bloque y hace poco realista convertir al país en un centro de servicios globales. Adicionalmente, Chile no informa avances sustantivos a la OCDE sobre la materia, pese a los compromisos adquiridos en el año 2008.

Las principales deficiencias que tiene la normativa vigente son:

A. Ausencia de consagración del principio de finalidad en el tratamiento de datos personales. Se trata de uno de los principios esenciales que permiten salvaguardar que los datos personales sean realmente utilizados sólo para los objetivos para los cuales fueron recolectados, y que por lo demás es la causa en cuya virtud el titular de éstos libremente consintió en su entrega. Junto a este vacío normativo el artículo 4° inciso final de la ley permite que las personas jurídicas privadas puedan tratar datos personales sin autorización del titular para su uso exclusivo, el de sus asociados y el de las entidades a las que están afiliadas, ya sea con fines estadísticos, de tarificación u otros de beneficio general de aquellos. Esta norma acarrea uno de los mayores riesgos del tratamiento de datos, pues permite que por la vía de la asociación se vulneren todas las normas y principios que pretendidamente protege la ley.

B. Existencia de conceptos que generan dificultades interpretativas y que han servido para vulnerar la protección de datos personales. Por ejemplo, lo que ocurre con el concepto de "fuente accesible al público", el que adolece de un defecto sustancial: radicar en el titular del registro o banco de datos la facultad de dejar o no abierto a público un registro, con el consecuente riesgo cierto de fraude al espíritu de la ley, especialmente en lo que dice relación con la posibilidad de realizar tratamiento de datos sin autorización del titular de los datos en aquellos casos en que la fuente es de esta naturaleza.

C. Falta de claridad respecto de quién es el responsable del tratamiento de datos personales. La ley define al responsable del registro o banco de datos como la persona natural o jurídica privada, o el respectivo organismo público, a quien competen las decisiones relacionadas con el tratamiento de los datos de carácter personal. Sin embargo, no se hace cargo de definir al responsable del tratamiento de datos, que es la persona que toma las decisiones operativas respecto del banco de datos y en quien debiera radicar la responsabilidad directa por el uso indebido de los datos personales.

D. Deber de información en el tratamiento de datos personales. Éste persigue que los titulares de datos personales sean informados de los posibles tratamientos de datos que puedan afectarles para los efectos de que puedan ejercer los derechos que les otorga la ley. La legislación nacional no regula esta materia, lo que es un elemento básico y esencial de la protección de datos personales.

E. Falta de registro de banco de datos privados. Se trata de una forma de materialización del deber de información en el tratamiento de datos personales, donde por intermedio de un registro de carácter universal cualquier persona puede consultar sobre los tratamientos de datos que se hacen de ella. En nuestro país, no obstante que las bases de datos del sector público deben estar inscritas en un registro que mantiene el Registro Civil, no han sido incorporadas al mismo la gran mayoría de las bases de los obligados, careciendo aquél, en consecuencia, de validez y confianza. Adicionalmente, no existe el mandato de registro de las bases de datos privadas.

F. Ausencia de sanciones por infracción a la normativa. La ley carece de un régimen sancionatorio por el incumplimiento de las obligaciones que impone, lo que redunda en que las vulneraciones a la misma quedan impunes y, consecuentemente, no hay presencia de mecanismos disuasivos ni correctivos por no tratar los datos de acuerdo a las exigencias mínimas que se imponen para asegurar la vida privada. También resulta gratuito, por ejemplo, no cumplir con la obligación de registro de las bases de datos públicas en el Registro Civil.

G. Recurso de habeas data atrofiado. La forma que ha tomado este recurso en la ley ha traído como consecuencia que, pese a la existencia de un recurso especial para garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y bloqueo de los datos personales, aquel no haya sido utilizado, prefiriendo los operadores jurídicos recurrir por intermedio del recurso de protección a los tribunales de justicia invocando la vulneración de un derecho fundamental, normalmente la privacidad. Las dificultades que presenta el recurso de habeas data son muchas, pero sólo con fines enunciativos podemos aseverar que tiene problemas para el titular de los datos personales en lo que significa la determinación del tribunal competente, el desigual tratamiento procesal que tienen las partes en el proceso lo que trae implícita la vulneración del debido proceso y la bilateralidad de la audiencia; finalmente, no se establece un plazo de prescripción de la acción con lo que se afecta la seguridad jurídica.

H. Ausencia de una autoridad de control. El hecho de no contar con una autoridad independiente que se encuentre permanentemente velando por el cumplimiento de la ley tanto por parte de los organismos públicos como privados, que tenga la posibilidad de aplicar sanciones por el incumplimiento y que tenga un fuerte rol de promoción de la protección de datos personales, es un vacío que, quizás formalmente, aparece como la mayor dificultad de Chile de cumplir el estándar internacional exigido.

I. Recogida y tratamiento de datos para marketing directo. La ley considera que para los efectos de realizar marketing directo es posible tratar datos personales sin autorización del titular, otorgándole a éste el derecho de oponerse cuando sea con fines de publicidad. Ello ha conducido a que en nuestro país nos encontremos desbordados por el spam o correo electrónico no deseado.

ESFUERZOS LEGISLATIVOS

En el Congreso Nacional es posible encontrar más de una cincuentena de proyectos de ley destinados a modificar la Ley 19.628 o reformar la Constitución para que se reconozca el derecho a la protección de datos personales.

A situarse en el año 2015, parece necesario relevar especialmente dos esfuerzos legislativos. Por una parte, el Proyecto de Ley Boletín 9384-07 que reforma la Constitución para consagrar el derechos a la protección de datos personales y, por otra, el trabajo pre legislativo realizado por la Subsecretaría de Economía durante el año 2014 para la elaboración de un Proyecto de Ley sobre Protección de las Personas del Tratamiento de Datos Personales.

PROYECTO DE LEY BOLETÍN 9384-07

Se trata de un proyecto de reforma constitucional que tiene por objeto consagrar constitucionalmente el derecho a la protección de datos.

Sin duda se trata de un proyecto de ley que busca que Chile siga la senda del reconocimiento constitucional de la protección de datos personales, tal como lo han hecho, entre otros, Argentina, Bolivia, Brasil, Colombia, Ecuador, España, México, Perú, Uruguay y Venezuela.

El proyecto de ley incorpora un nuevo inciso segundo al artículo 19 Nº 4 de la Constitución

estableciendo el derecho de todas las personas a acceder a sus datos personales y a obtener, en la forma que determine la ley, su rectificación, complementación y cancelación, si éstos fueren erróneos o afectaren sus derechos. Es decir, de manera muy sencilla otorga consagración constitucional al derecho y, al mismo, tiempo constitucionaliza los derechos de acceso, rectificación, cancelación y oposición, derechos que forman parte del contenido esencial de la protección de datos en el derecho comparado.

Ahora bien, la constitucionalizarían de los derechos de acceso, rectificación, cancelación y oposición, amenazan con sobrecargar el sistema judicial al no existir mejor mecanismo en el ordenamiento jurídico nacional para el restablecimiento de los derechos de los titulares de datos.

TRABAJO PRE LEGISLATIVO PARA LA ELABORACIÓN DE UN PROYECTO DE LEY SOBRE PROTECCIÓN DE LAS PERSONAS DEL TRATAMIENTO DE DATOS PERSONALES.

El Ministerio de Economía, Fomento y Turismo elaboró un Ante Proyecto de Ley de Protección de las Personas del Tratamiento de Datos Personales que fue sometido a Consulta Ciudadana. Si bien ésta no tenía carácter vinculante para la autoridad, fue anunciada como un mecanismo que permitiría perfeccionar el Ante Proyecto con propuestas que emanen directamente de actores relevantes de la Industria, la Sociedad Civil, la Academia y los ciudadanos individualmente interesados en participar de ella.

Se invitó a la ciudadanía a participar activamente en esta Consulta Ciudadana a través del sitio web institucional, desde el 28 de julio hasta el 22 de agosto de 2014.

En paralelo al desarrollo de la Consulta Ciudadana, la Subsecretaría de Economía constituyó una mesa multiparte en la cual participaron activamente la Asociación de Bancos e Instituciones Financieras, la Asociación Chilena de Empresas de Tecnologías de la Información, la Cámara Chileno Norteamericana de Comercio, la Cámara de Comercio de Santiago, la Cámara Nacional de Comercio, el Comité de Retail Financiero, la Asociación de Aseguradoras de Chile, el Centro de Estudios en Derecho Informático de la Universidad de Chile, el Instituto Chileno de Derecho y Tecnologías, la ONG Derechos Digitales y la Fundación Proacceso. Adicionalmente, participaron las empresas Google y Microsoft como invitadas.

El trabajo prelegislativo buscó que quedaran recogidas de la mejor forma las diferentes opiniones vertidas en la Consulta Ciudadana y en las reuniones de la mesa multiparte.

Como es natural en un proyecto de estas características no fue posible lograr unanimidad, pero sí un alto grado de consenso respecto a las diferentes materias que debe abordar un proyecto de ley que sirva de marco para el tratamiento de la información, con miras a asegurar la libre circulación de la información con pleno respeto a los derechos de los titulares de datos.

De este modo, el texto del proyecto trabajado se orientó a crear un Sistema de Protección de Datos que importe un nuevo acuerdo nacional que, junto con proteger a las personas, logre asegurar la libre circulación de la información.

Respecto a los aspectos sustantivos del proyecto, se consensuó que debían ser los principios internacionales de la protección de datos, recogidos fundamentalmente en la Resolución de Madrid, las Directrices de la OCDE relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales y el Marco de Privacidad de APEC. Adicionalmente, se consideró el texto del Reglamento de la Unión Europea que se encontraba en revisión en el Parlamento Europeo.

La Autoridad de Protección de Datos se la concibió, de acuerdo al estándar internacionalmente exigido, como un órgano autónomo, independiente, de carácter técnico y especializado destinado a promover y garantizar el derecho de las personas de proteger y controlar los datos personales que le conciernen, dictar instrucciones generales para la correcta aplicación de la ley, fiscalizar el cumplimiento de las normas sobre tratamiento de datos personales y ejercer la potestad sancionatoria. Uno de los aspectos más relevantes del trabajo tuvo que ver con el gobierno de éste órgano, habiendo unanimidad, dada las competencias que debe ejercer, respecto a que sea un órgano colegiado en que participen los diferentes poderes públicos en su generación, con un severo régimen de incompatibilidades e inhabilidades, sólo compatible con actividad académica; con dedicación exclusiva para sus miembros y, con un patrimonio conformado por los recursos que le asigna la ley de presupuestos.

En lo que relativo al régimen de sanciones, se estimó la conveniencia de diferenciarlas según gravedad y con criterios que permiten una aplicación diferenciada dentro de la respectiva clase en función de elementos objetivos. Al mismo tiempo, la conveniencia de tener una diferenciación entre las sanciones que se aplican a los particulares y los órganos del Estado. Para los primeros, parten en la amonestación escrita y llegan a multas de hasta 10.000 UTM, siendo todas a beneficio fiscal. Para los órganos del Estado, por su parte, se establece un régimen orientado a hacer responsable directamente al Jefe Superior del Servicio, con multas y hasta la suspensión en el cargo.

MEDIOS DE PAGO ELECTRÓNICOS

¿QUÉ SON LOS MEDIOS DE PAGO?

El avance de Internet como plataforma especial para el comercio ha traído como consecuencia un desarrollo vertiginoso del comercio electrónico, abriendo nuevos horizontes para proveedores de bienes y servicios.

Este avance acarrea que los sistemas de pago deban evolucionar permitiendo a los consumidores pagar a través del mismo medio por el cual celebran sus contratos.

Un sistema de pago electrónico, permite y facilita la aceptación de pagos para las transacciones en línea a través de internet.

Los sistemas de pagos electrónicos, realizan la transferencia del dinero (transferencia de información en realidad) entre compradores y vendedores en una acción de compra-venta electrónica, generalmente, a través de una entidad financiera autorizada por ambos.

Esta evolución incluso ya ha traspasado la barrera del computador, llevando al comercio electrónico *e-commerce* a aparatos móviles como *Smartphone y tablets* ampliando la noción al *m-commerce.*

Las maneras en que se instrumentalizan los medios de pago electrónico son muy variadas, a continuación se caracterizarán aquellos instrumentos más relevantes en el comercio electrónico.

1. TARJETAS BANCARIAS

Tradicionalmente por razones de capital y de fe pública, han sido los bancos los emisores y operadores de tarjetas. La tarjeta es el instrumento de pago electrónico por excelencia, es el más popular y extendido de las formas de pago empleados en el comercio electrónico y hasta fechas muy recientes, los esfuerzos han ido destinados a ofrecer seguridad y confiabilidad a su uso. Sus manifestaciones más típicas corresponden a pagos de transacciones hechas por medio de tarjeta de débito y de crédito con cargo a las cuentas bancarias del titular.

En Chile la emisión y operación de tarjetas de Crédito y Débito, se encuentra reguladas por disposiciones del Banco Central de Chile, Capítulos III.J 1, y 2 del Compendio de Normas Financieras y la Superintendencia de Bancos e Instituciones Financieras en su recopilación actualizada de Normas, Capítulo 8-3 para Crédito y 2-15 para Débito, sin perjuicio de otras circulares[1].

[1] Nos referimos exclusivamente a tarjetas abiertas de carácter bancario

En un esquema clásico de transacción con tarjeta de crédito o débito, participan los siguientes actores:

A. EMISOR: Persona jurídica, generalmente un banco, que concede a un cliente una determinada tarjeta. El Banco tiene la facultad de emitir y poner en circulación una tarjeta, por cuanto en forma previa ha suscrito un contrato con una organización internacional de medios de pago que le ha otorgado la licencia[2], o bien son tarjetas de su propia emisión[3].

B. ADQUIRENTE: Persona Jurídica, generalmente un banco, que afilia al Establecimiento Comercial para que acepte las tarjetas como medio de pago[4].

C. TARJETAHABIENTES O TARJETADEBITANTES: Titular o Usuario de una tarjeta de crédito o débito.

D. ESTABLECIMIENTO COMERCIAL: Acepta que el pago de sus bienes o servicios, sean realizados con las tarjetas emitidas por el Emisor.

Eventualmente, pueden existir otros participantes:
- Operador: Quien se encarga de realizar los servicios administrativos que requieran los emisores, tales como el Rol Emisor, Adquirente o ambos, la afiliación de los establecimientos comerciales y la relación con las Marcas Internacionales, por cuenta y riesgo de su mandantes[5].
- Marcas Internacionales
- Prestadores de Servicios de Redes.

2. TARJETAS MONEDERO

Dentro de las tarjetas bancarias, están también las Tarjetas Monedero o Pre pago, estas son tarjetas emitidas por una entidad bancaria que incorporan un chip en el cual puede ser almacenado, previo pago en la entidad bancaria emisora, un valor monetario que, a su vez, puede ser descontado fraccionaria o completamente en cualquier comercio que posea un lector de este tipo de tarjetas.

El sistema de tarjetas se fundamenta en la existencia de una transacción donde existe presencia física de la tarjeta crédito / debito, actualmente en una clave secreta que sólo el usuario debe conocer, y redes privadas a nivel nacional que permiten que fluya la información, y un sistema contractual que involucra a todos los que participan en la operación, suscribiéndose numerosos y complejos contratos entre todos los participantes.

---

[2] Son las denominadas marcas internacionales de tarjetas de crédito y/o débito, por ejemplo VISA (crédito) - VISA Electron (débito), MasterCard (crédito) MasterCard Maestro (débito), American Express (tarjeta de gasto, inicialmente no otorgaba crédito para el pago de consumos), Diners (tarjeta de crédito), etc.[3] Nos referimos exclusivamente a tarjetas abiertas de carácter bancario

[3] Nos Transbank en Chile y por cuenta de sus Bancos socios y emisores de tarjetas, ha puesto en circulación el sistema de pago con débito, denominado RedCompra.

[4] En Chile, la afiliación de los establecimientos de comercio la realizan las empresas emisoras, y las empresas operadoras, de conformidad al Nº I.4, del Capítulo III. J.1.

[5] En nuestro país el Rol Adquirente lo realiza la Sociedad de Apoyo al Giro Bancario Transbank S.A., quien afilia a los establecimientos comerciales que ingresan al sistema, procesa las transacciones realizadas y paga a los comercios en la época convenida. Asimismo, actúa por cuenta de los Adquirentes frente a las Marcas Internacionales. El Rol Emisor lo realiza principalmente la empresa Nexus, también Sociedad de Apoyo al Giro Bancario.

Las Tarjetas Monedero se presentan como una posible solución al problema de los micropagos, es decir, pagos de pequeñas cantidades cuyo abono por tarjeta tradicional genera unos costos excesivamente altos para el denominadas marcas internacionales de tarjetas de crédito y/o débito, por ejemplo VISA (crédito) - VISA Electron (débito), MasterCard (crédito) MasterCard Maestro (débito), American Express (tarjeta de gasto, inicialmente no otorgaba crédito para el pago de consumos), Diners (tarjeta de crédito), etc.
Transbank en Chile y por cuenta de sus Bancos socios y emisores de tarjetas, ha puesto en circulación el sistema de pago con débito, denominado RedCompra.

En Chile, la afiliación de los establecimientos de comercio la realizan las empresas emisoras, y las empresas operadoras, de conformidad al Nº I.4, del Capítulo III. J.1.

El Rol Adquirente, por su parte, lo realiza la Sociedad de Apoyo al Giro Bancario Transbank S.A., quien afilia a los establecimientos comerciales que ingresan al sistema, procesa las transacciones realizadas y paga a los comercios en la época convenida. Asimismo, actúa por cuenta de los Adquirentes frente a las Marcas Internacionales. El Rol Emisor lo realiza principalmente la empresa Nexus, también Sociedad de Apoyo al Giro Bancario.

La principal ventaja de este medio de pago es que permite realizar pagos pequeños, tal y como si se tuviera un monedero real, gozando de anonimato, todo ello sin necesidad de portar físicamente el dinero.

Existen monederos recargables y desechables, únicos y multipropósito, estos últimos permiten combinar en forma segura y en una misma tarjeta, diversos productos o servicios tanto financieros como no financieros.

Los Monederos Electrónicos, representan una gran ventaja financiera frente a los cajeros automáticos: no requieren la inmovilización del dinero líquido, ya que el depósito es soportado por cada uno de los usuarios en su tarjeta y con cargo a su cuenta.

Actualmente en Chile solo pueden operar Monederos electrónicos los bancos, y su regulación se encuentra en el Capítulo III.J.3 del Compendio de Normas del Banco Central de Chile.

Sin embargo, se encuentra en trámite un Proyecto de Ley, que permitiría a Entidades no bancarias constituirse en Emisores y Operadores de tarjetas de Prepago, constituyendo un avance sobre esta materia.

3.TRANSFERENCIAS ELECTRÓNICAS DE FONDOS

Hoy nos resulta habitual que una persona realice una transferencia de fondos desde su computador a otra cuenta distinta del mismo u otro banco, transacción que, además, en Chile tiene la particularidad de ser inmediata. Naturalmente por el computador no viaja el dinero sino solo información.

Las Transferencias Electrónica de Fondos (TEF) en línea, requieren la existencia de un banco originador y de un banco receptor. Como existen múltiples emisores y receptores, no parece viable que cada banco celebre acuerdos individuales con el resto, de los bancos, por lo que existe switch de comunicaciones (una infraestructura segura) que es capaz de recibir, registrar y distribuir diversas instrucciones e información originada en los bancos emisores hacia bancos receptores destinadas a perfeccionar y materializar las operaciones recibidas. Con la información de las TEF efectivamente cursadas por los bancos, el switch determina e informa a su vez los saldos diarios a pagar a cada uno de los bancos involucrados, pagos que cada banco realiza hacia el final del día en el Sistema de Liquidación Bruta en Tiempo Real del Banco Central de Chile.

La regulación específica de las TEF, se encuentra en el Capítulo 1-7 de la Recopilación Actualizada de Normas de la Superintendencia de Bancos e Instituciones Financieras.

4. DINERO ELECTRÓNICO, LA IRRUPCIÓN DE *BITCOINS*

El dinero no es otra cosa que la representación de un valor abstracto, admitido para la realización de intercambios y respaldado por una autoridad pública. En el supuesto del dinero electrónico esta representación, en lugar de papel, estaría contenida en bits y, concretamente en cupones criptográficos.

Hoy el mayor desarrollo de este modelo de medio de pago se encuentra en los denominados *bitcoins.*

Bitcoin es la primera moneda digital descentralizada, son monedas digitales que se puedan enviar por Internet. Comparado con otras alternativas, *Bitcoin* ofrece varias ventajas:

• son transferidos directamente de persona a persona a través de la red, sin pasar por un banco u otro intermediario. Esto acarrea, que las comisiones sean menores, que puedan usarse en cualquier país, que las cuentas no sean bloqueadas y que no haya pre-requisitos ni limitaciones arbitrarias.

• Eequieren de una billetera electrónica, es decir, un software que se instala en el computador o en el dispositivo móvil. Esta billetera genera una dirección única y específica para el usuario, misma que necesitará compartir si desea hacer transacciones. Cada billetera tiene una clave privada, que se usa para hacer firmas digitales y que verifican identidad y evitan que se hagan alteraciones a las transacciones.

• Las transacciones con Bitcoins son verificadas usando un registro público compartido, llamado blockchain, que mantiene absolutamente todas las transacciones que se hacen, sin excepción. El blockchain asegura que un usuario efectivamente tiene la cantidad de *Bitcoins* que pretende gastar.

Una transacción con esta moneda virtual es en realidad una transferencia de una cantidad entre dos billeteras o direcciones de *Bitcoin.*

Las transacciones son trasmitidas y confirmadas en la red mediante un proceso llamado Mining, un sistema distribuido que se usa para confirmar e incluir transacciones en el blockchain, manteniendo un orden cronológico y distribuye el proceso en diversos equipos de cómputo. Parte de lo que hace este sistema es implementar varios niveles de seguridad que evitan la manipulación o alteración de las transacciones que se llevan a cabo.

La red de *Bitcoins* se mantiene segura gracias a los denominados "mineros", éstos son individuos recompensados por medio de *Bitcoins* por su trabajo verificando transacciones. Una vez que estas transacciones son verificadas se almacenan permanentemente en la red.

Bitcoin es un gran avance para las empresas ya que les permite reducir las comisiones por sus transacciones (desintermediación bancaria), no tiene costos y resulta fácil comenzar a aceptar Bitcoins, no hay reembolsos fraudulentos y se obtiene, además, un negocio adicional de la comunidad *Bitcoin.*

Adicionalmente, Bitcoin está siendo de aceptación universal como medio de pago, es un pago garantizado que no depende de la existencia de fondos en una cuenta ni la concesión de crédito de un tercero, no hay costos para el usuario y es anónimo no queda ni rastro de las personas que lo utilizan.

A simple vista es fácil reconocer las ventajas que el dinero electrónico, ofrece como modo de articulación del cumplimiento del pago. No obstante, también presenta dificultades que no deben ser obviadas: El registro de las transacciones, la confianza en el emisor, eventuales fraudes, y seriedad en las empresas emisoras, entre otros.

5. PAGOS MÓVILES

El uso y generalización del teléfono móvil en estos últimos años ha llevado a algunas empresas (telefónicas, bancarias, de servicios) a desarrollar sistemas de pago basados en el habitual teléfono móvil.
Las modalidades más usuales son:

- sistema de pago basado en tarjetas prepago (a imagen de las populares tarjetas telefónicas)

- un pago en cargo indirecto a la tarjeta de crédito del usuario, previa confirmación telefónica del pago.

En el primer caso, el usuario adquiere una tarjeta prepago en cualquiera de los establecimientos autorizados por la compañía prestadora del servicio y elige el Comercio y el producto deseado, presionando el icono de la empresa que suministra el servicio de pago. En ese momento se inicia una conexión segura con la empresa suministradora del servicio de pago, la cual solicitará al usuario que introduzca las cifras del código secreto incluido en la tarjeta prepago. De esta forma, la empresa suministradora del servicio de pago conocerá el importe total del cual el usuario es acreedor, procediendo a autorizar el pago si el precio del bien o del servicio es inferior al saldo remanente en la tarjeta prepago.

Este sistema tiene ventajas indudables: Es seguro, confidencial, anónimo y completamente electrónico. No obstante también presenta inconvenientes: el comercio puede estar limitado a la afiliación que haya realizado la empresa que suministra el servicio, y sólo es una solución válida y eficaz al problema de los micropagos pero haciendo imposible el pago de bienes y servicios de valor elevado.

En el segundo caso, el pago de bienes y servicios de costo elevado puede ser solventado mediante un pago móvil, aun cuando la operación no se realiza únicamente en la red. En efecto, es necesario convertirse en titular de una tarjeta de crédito, recibir un Código o PIN (Número de Identificación Personal), y confirmar vía teléfono los pagos deseados, para que la empresa autorice y lo haga efectivo.

Esta segunda modalidad, si bien hace posible el pago de importes elevados, presenta serios inconvenientes:

- Es una solución que sigue sin ser global. El usuario sólo tiene la posibilidad de contratar con los comercios adheridos a la empresa prestadora del servicio de pago.

- No es confidencial. Todos los intervinientes en el pago conocen el precio y el bien o el servicio contratado.
- No es anónimo, pudiendo el banco elaborar un perfil de los gustos y hábitos del comprador.

6. SISTEMAS DE PAGO POR CORREOS ELECTRÓNICOS

Son sistemas de pago online relativamente recientes, que permite la transferencia de dinero entre usuarios que tengan correo electrónico[6].

Aprovechan el correo electrónico que es la aplicación más difundida de la Red; no requieren software especiales ni exigen afiliación de ningún tipo; permiten la privacidad ya que no viajan datos sensibles por la Red.

Estos sistemas permiten la recepción y envío de dinero en Internet de forma rápida y segura entre comprador y vendedor. Para ello se tiene la posibilidad de registrarse en su sitio web y obtener servicios como suscripción a pagos periódicos, realizar el pago desde una cuenta bancaria, o incluso que el dinero se deposite en la propia cuenta del Operador del sistema.

Este tipo de pago tiene un costo también en forma de cobro de comisión al comercio pero, generalmente no al consumidor online.

CONCLUSIONES

En general los mayores desafíos legales a los que se enfrentan los medios de pago electrónicos, consisten en permitir la privacidad y confidencialidad de los datos, el anonimato en la transacción, la seguridad y confiabilidad en el uso de la información, costos razonables para el usuario a la hora de realizar sus pagos, y en una solución oportuna y accesible a la hora de resolver disputas

[6] PayPal es la solución más conocida e importante.

CLOUD COMPUTING

¿QUÉ ES EL CLOUD COMPUTING?

Cloud Computing es un servicio de almacenamiento que permite subir documentos, fotos, videos y otros archivos a un sitio web para compartir con otros o para actuar como una copia de seguridad, procesando y recuperando datos. A estos archivos se puede acceder desde cualquier ubicación o cualquier tipo de dispositivo (computadores, teléfonos, tablets, etc.).

Desde una perspectiva empresarial, ofrece una forma de acceder al software sin tener que comprarlo. Además, al no requerir de la capacidad de memoria del disco duro del computador personal, no hay necesidad de realizar inversiones en infraestructura sino que utiliza aquella que pone a su disposición el prestador del servicio, garantizando que no se generen situaciones de falta o exceso de recursos, así como el mayor costo asociado a dichas situaciones.

Desde la perspectiva de las comunicaciones, el Cloud Computing ofrece una forma eficiente para transferir datos de un lugar a otro facilitando el trabajo colaborativo global y para apoyar el comercio electrónico. En este sentido, se trata de una tecnología que se adapta perfectamente al crecimiento de una economía globalmente interconectada. El proveedor del servicio puede encontrarse, prácticamente, en cualquier lugar del mundo proporcionando los servicios optimizando sus propios recursos.

Una vez registrado en una cuenta, normalmente se crea una carpeta en el equipo y todos los archivos alojados en esa carpeta se copian en los servidores del proveedor. Los cambios realizados en estos archivos son copiados en forma automática y quedan inmediatamente accesibles desde otros dispositivos que pueda tener. La mayoría de los servicios ofrecen un servicio limitado gratis, debiéndose pagar por aquellas versiones que permiten mayor o incluso espacio de almacenamiento ilimitado.

Para comprender el funcionamiento del Cloud Computing es fundamental comprender los tres niveles en que puede ser proporcionado el servicio.

1. INFRAESTRUCTURA COMO SERVICIO. Este nivel entrega una infraestructura de procesamiento completa al usuario, quien dispondrá de una o varias máquinas virtuales en la nube con las cuales, por ejemplo, podrá aumentar el tamaño de disco duro en unos minutos, obtener mayor capacidad de proceso y únicamente pagar por aquellos recursos que utilice. Este nivel puede ser visto como una evolución de los Servidores Privados Virtuales que ofrecen actualmente las empresas de hosting.

2. PLATAFORMA COMO SERVICIO. Con este nivel se entrega una plataforma de procesamiento completa al usuario, plenamente funcional y sin necesidad de comprar y mantener el hardware y software. Por ejemplo, un desarrollador web necesita un servidor web que sirva sus páginas, un servidor de bases de datos y un sistema operativo. Este nivel proporciona todos estos servicios.

3. SOFTWARE COMO SERVICIO. Este nivel se encarga de entregar el software como un servicio a través de Internet siempre que lo demande el usuario. Se trata del nivel más bajo que permite el acceso a la aplicación utilizando un navegador web, sin necesidad de instalar programas adicionales en el ordenador o teléfono móvil.

Respecto de los modelos en que puede funcionar el servicio de Cloud Computing se pueden agrupar de la siguiente manera:

• **NUBES PÚBLICAS:** son aquellas en las que todo el control de los recursos, procesos y datos está en manos de terceros. Múltiples usuarios pueden utilizar servicios web que son procesados en el mismo servidor, pueden compartir espacio en disco u otras infraestructuras de red con otros usuarios.

• **NUBES PRIVADAS:** aquellas creadas y administradas por una única entidad que decide dónde y cómo se ejecutan los procesos dentro de la nube. Supone una mejora en cuanto a la seguridad y privacidad de los datos y procesos, ya que los datos sensibles permanecen en la infraestructura informática de la entidad, mientras que controla qué usuario accede a cada servicio de la nube. Sin embargo, la entidad sigue siendo la encargada de comprar, mantener y administrar toda la infraestructura hardware y software de la nube.

• **NUBES HÍBRIDAS:** coexisten los dos modelos anteriores. Por ejemplo, una empresa hace uso de una nube pública para mantener su servidor web mientras que mantiene su servidor de bases de datos en su nube privada. De este modo, se establece un canal de comunicación entre la nube pública y privada mediante el cual los datos sensibles permanecen bajo estricto control mientras que el servidor web es administrado por un tercero. Esta solución disminuye la complejidad y coste de la nube privada.

• Se apunta, además, a un cuarto modelo, las nubes comunitarias, que son compartidas entre varias organizaciones que forman una comunidad con principios similares (misión, requerimientos de seguridad, políticas y cumplimientos normativos). Puede ser gestionada por la comunidad o por un tercero.

Por último, conviene precisar que existen diversos modelos de proveedores de servicios de *Cloud Computing*. El panorama actual dirige a los usuarios hacia dos posibles soluciones. La primera sería contratar un *Cloud Hosting* y la segunda sería utilizar los servicios específicos de *Cloud Computing* ofertados por grandes empresas.

1. LOS SERVICIOS DE *CLOUD HOSTING* son similares a los servicios ofrecidos por empresas de hosting tradicional. La diferencia principal es que en un servicio en la nube se paga por lo que se utiliza y se puede ampliar o disminuir los recursos del sistema. En un sistema de *hosting* tradicional es necesario saber qué capacidad de procesamiento se va a necesitar e incluso qué versión del sistema operativo se va a utilizar antes de contratar los servicios.

2. LOS SERVICIOS DE *CLOUD COMPUTING* ofertados por las grandes empresas del sector informático permiten obtener una mayor personalización en la solución informática contratada. Dado que esta opción brinda más funcionalidades también requiere un mayor conocimiento técnico por parte del contratante para aprovechar al máximo sus características.

VENTAJAS DEL CLOUD COMPUTING

• **MOVILIDAD:** Los datos de una empresa, al quedar alojados en la nube, pueden ser consultados por los empleados desde cualquier lugar.

• **FOCALIZACIÓN:** *Cloud Computing* permite a las compañías centrarse en su negocio principal. En vez de hacer una alta inversión tecnológica en sistemas, una empresa podría invertir en su infraestructura industrial o física o en capital humano para proseguir sus planes de expansión.

• **ECOLOGÍA:** *Cloud Computing* es un medio respetuoso con el medio ambiente. Usar la nube en una empresa reduce la huella de carbono al ahorrar recursos y componentes que pasan a almacenarse de componentes físicos a virtuales. Se ahorra también en consumo de energía con sus beneficios al medio ambiente.

VENTAJAS ECONÓMICAS DEL *CLOUD COMPUTING*

El *Cloud Computing* ofrece ventajas a las organizaciones del sector privado, especialmente a las PYMEs, y a las dependencias y entidades el sector público. En particular, el estudio "ahead of the Curve" del Boston Consulting Group encontró, a nivel mundial, que las PYMEs que utilizan el Cloud Computing se distinguen de aquellas que no porque incrementan su facturación 15 puntos porcentuales más rápido y crean puestos de trabajo casi dos veces más rápido.

Rackspace, por su parte, **ha publicado un estudio sobre los ahorros de costos gracias al Cloud Computing, realizado a empresas y empresarios de EEUU y Reino Unido.**

Según este estudio, nueve de cada diez empresas están de acuerdo con que **el paso a la nube se ha traducido en un ahorro de costos.** De acuerdo a los datos de la encuesta, **el *Cloud Computing* permite ahorrar dinero,** ayudando a aumentar la competitividad y ofreciendo interesantes oportunidades para empresas de todos los tamaños.

Para la elaboración de esta encuesta se analizaron más de 1.300 empresas de EEUU y Reino Unido, mediante entrevistas con los ejecutivos de estas empresas. El 88% de éstos indicaron que **habían ahorrado** dinero gracias a la utilización de la nube, y habían **mejorado la eficiencia** de sus infraestructuras, pudiendo así centrarse en la estrategia y la innovación.

Por otra parte, el 56% de los encuestados dijo que el Cloud Computing había **incrementado las ganancias de la empresa,** mientras que algo menos de la mitad (49%) cree que la computación en nube ha **ayudando a hacer crecer su negocio.**

Conforme a una investigación realizada por el Centre for Economics and Business Research, que buscaba cuantificar los beneficios económicos que la **informática en la nube o** *Cloud Computing* tendría para las empresas españolas, indicó que esa reducción, entre 2010 y 2015, alcanzará los 22 mil millones de euros.

Las principales ventajas de carácter económico que brinda el Cloud Computing son:

1. REDUCE LOS COSTOS: Los propietarios de pequeñas y medianas empresas no tienen que invertir grandes cantidades de dinero en equipos o softwares para ejecutar las aplicaciones que utilizan en sus negocios, lo que disminuye considerablemente sus gastos.

2. PERMITE TENER MENOS PERSONAL: Los propietarios de negocios no necesitan contratar profesionales para configurar e implementar los softwares necesarios para sus actividades. Este ahorro salarial podría ser incluso mayor que los ahorros de equipamiento. Además, los costos operacionales son sólo una parte del continuo gasto de mantenimiento, por lo que en realidad los ahorros se extienden a lo largo del tiempo.

3. FLEXIBILIZA LOS GASTOS: En principio, el servicio es prepagado, es decir, las empresas pueden pagar sólo por lo que han utilizado. Sin embargo, a medida que el negocio prospera, los clientes pueden fijar un costo mensual, similar a un plan de telefonía, conforme a sus necesidades.

4. PERMITE OPTAR A NUEVAS TECNOLOGÍAS: Permite a los propietarios de negocios experimentar con nuevas tecnologías a un precio moderado. Éstas suelen ser muy costosas y, aunque algunos empresarios tienen el presupuesto necesario para adquirirlas, la inversión resulta muchas veces exagerada.

RIESGOS Y PROBLEMAS DEL CLOUD COMPUTING

El uso de servicios de Cloud Computing ofrece un gran número de ventajas pero presenta también, por sus características, riesgos específicos que deben afrontarse con una adecuada elección del prestador. Debe analizarse que las condiciones de prestación tengan en cuenta los elementos que permitan que el tratamiento de datos se realice sin merma de las garantías que le son aplicables.

1. FALTA DE TRANSPARENCIA
Es el prestador quien conoce los detalles del servicio que ofrece. De allí se manifiesta la necesidad de conocer qué, quién, cómo y dónde se lleva a cabo el tratamiento de los datos que se proporcionan al proveedor para la prestación del servicio. Si este último no da una información clara, precisa y completa sobre todos los elementos inherentes a la prestación, la decisión adoptada por el responsable no podrá tener en consideración de forma adecuada requisitos básicos como la ubicación de los datos, la existencia o no de subencargados, los controles de acceso a la información o las medidas de seguridad. De esta forma, se dificulta al usuario la posibilidad de evaluar los riesgos y establecer los controles adecuados.

2. FALTA DE CONTROL
Como consecuencia de las peculiaridades del modelo de tratamiento en la nube y en parte también de la ausencia de transparencia en la información, la falta de control del responsable se manifiesta, por ejemplo, ante las dificultades para conocer en todo momento la ubicación de los datos, las dificultades a la hora de disponer de los datos en poder del proveedor o de poder obtenerlos en un formato válido e interoperable, los obstáculos a una gestión efectiva del tratamiento o, en definitiva, la ausencia de control efectivo a la hora de definir los elementos sustantivos del tratamiento en lo relativo a salvaguardas técnicas y organizativas.

3. CONOCIMIENTO DEL RESPONSABLE DEL TRATAMIENTO.
El mismo contratista puede desconocer la localización precisa de sus datos y no disponer del control directo de acceso a los mismos, de su eliminación y de su portabilidad, ya que la información no está físicamente en su poder.

Por la protección de datos personales resulta esencial la identificación del responsable del tratamiento, dado que esto garantiza que haya una persona que tiene asignadas una serie de obligaciones concretas derivadas del tratamiento y, por lo tanto, hay alguien a quien le es exigible el cumplimiento de estas obligaciones.

4. PROTECCIÓN DE DATOS.
Los problemas principales que enfrentan los proveedores de servicios en la nube y otros que necesitan para transferir datos a través de las fronteras son la forma de garantizar el cumplimiento leyes, reglamentos y códigos de buenas prácticas respecto de protección de datos.

Al optar por almacenar archivos en la nube es necesario recordar que éstos estarán realmente almacenados en servidores controlados por el proveedor de servicios. Quien, a su vez, podría estar utilizando los servicios de *Cloud Computing* de otra organización.

Para ello habrá que comprobar que la seguridad y disponibilidad del servicio sea el adecuado para los tipos de archivos que se desea cargar.

Los diferentes modelos de servicio de *Cloud Computing,* impactan directamente sobre una cuestión clave en la definición del derecho a la protección de datos de carácter fundamental: la autodeterminación informativa.

Este es un derecho activo de control sobre el conjunto de informaciones relativas a una persona.

El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre sus datos personales, el cual no vale nada si el afectado desconoce cuáles de estos datos están poder terceros, quiénes son estos terceros y con qué finalidad tienen sus datos.

Éste es, por lo tanto, uno de los mayores inconvenientes detectados con relación al *Cloud Computing:* la pérdida efectiva de control sobre los datos, dado que, más allá de los vínculos contractuales o de suscripción con las empresas que prestan estos servicios, desaparece el vínculo o la certeza sobre la ubicación física de la información y las condiciones de procesamiento y, en consecuencia, pueden quedar afectadas las garantías de confidencialidad y de seguridad de la información situada en la nube.

5. TERRITORIALIDAD
La protección del derecho fundamental a la protección de datos de personales, se puede ver vulnerado en situaciones de multiterritorialidad y movimiento internacional de datos, propio del *Cloud Computing,* acarreando dificultades para resolver de manera efectiva las posibles vulneraciones.

6. POSIBLES COLISIONES DE DERECHOS DE PROPIEDAD INTELECTUAL Y SEGURIDAD
El *Cloud Computing* puede ser un entorno poco seguro para poner contenidos sujetos a Propiedad Intelectual de consumo típicamente lineal (películas, música, libros) a disposición de terceros *on demand* o retransmitir linealmente *(streaming)* puesto que la aceptación "pirata" de la transmisión o puesta a disposición del contenido da lugar a una copia "pirata" que puede ser comercializada.

Se pone a disposición la información al Proveedor de Servicios, lo cual configura un tratamiento de dato por un tercero, lo que puede dar lugar a una cesión de datos no consentido.

CÓMO ENFRENTAR LOS RIESGOS CONFORME A LA NORMATIVA CHILENA

Como ya se ha comentado, los principales riesgos que se manifiestan con el uso de los servicios de *Cloud Computing* se manifiestan en materia de protección de datos personales. ¿Cómo está preparado Chile para enfrentar estos riesgos?

Para enfrentar estos riesgos, y así desarrollar buenas prácticas en el uso del *Cloud Computing,* es necesario que los proveedores de este tipo de servicio presten especial atención a la normativa vigente respecto de la protección de datos de carácter personal, específicamente a las reglas de la ley 19.628 sobre protección de la vida privada.

ARTÍCULO 4°. *El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.*
La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.
La autorización debe constar por escrito.
La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.
No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, *o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.*

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

ARTÍCULO 7°. *Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.*

ARTÍCULO 11.- *El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.*

ARTÍCULO 23.- *La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.*
La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez.
El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

REFERENTES NORMATIVOS Y PRÁCTICOS A NIVEL INTERNACIONAL: RESOLUCIONES, OPINIONES Y DOCUMENTOS DE TRABAJO RELEVANTES

1. SOPOT MEMORANDUM DEL GRUPO DE BERLÍN.

El documento de trabajo examina, específicamente, el tratamiento de datos personales en entornos del Cloud Computing, haciendo referencia expresa a que las recomendaciones que incluye buscan mantener un alto nivel de protección de datos personales.

2. DICTAMEN 5/2012 DEL GRUPO DE TRABAJO DEL ARTÍCULO 29 DE LA DIRECTIVA 95/46/CE

En su Dictamen, el Grupo de Trabajo destaca los beneficios del Cloud Computing al indicar que ésta "puede aportar beneficios de seguridad; las empresas, especialmente las pequeñas y medianas, pueden adquirir, por un coste marginal, tecnologías de alto nivel, que de lo contrario estarían fuera de su presupuesto".
El dictamen se centra en la situación de una relación entre el responsable y el encargado, considerándose al cliente responsable y al proveedor, encargado. E indica a continuación que en los casos en que el proveedor actúa también como responsable del tratamiento, este debe cumplir requisitos adicionales.
Dentro del dictamen se incluyen algunas garantías:

- Medidas de seguridad a cumplir por el proveedor en atención a los riesgos del tratamiento así como la naturaleza de los datos personales.
- Previsiones sobre la devolución de los datos personales o destrucción segura una vez finalizado el servicio.
- Cláusula de confidencialidad aplicable al proveedor.
- Obligación del proveedor de apoyar al cliente para facilitar el ejercicio de los derechos de acceso, rectificación y cancelación.

• Prohibición de comunicación de los datos de parte del proveedor a un tercero, ni siquiera con fines de conservación, salvo que el contrato prevea la existencia de subcontratistas.
• Responsabilidades del proveedor relativas a la notificación al cliente de violaciones de datos que pudieran afectar a sus datos.
• Listado de lugares donde se tratarán los datos.
• Derecho del cliente a controlar y obligación del proveedor de cooperar.
• Notificación de solicitudes de acceso a datos por autoridades, salvo que esté prohibido.
• Obligación del proveedor de garantizar que cumple con las normas nacionales e internacionales de protección de datos personales.

3. RESOLUCIÓN SOBRE EL CLOUD COMPUTING DE LA CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD.
El presente documento reconoce como aspectos atractivos del Cloud Computing la mayor eficiencia económica, menor impacto medioambiental y operación más fácil. Reconoce, además, la necesidad de que las partes implicadas en los servicios de Cloud Computing cooperen para asegurar un alto nivel de privacidad y protección de datos personales, así como de seguridad tecnológica, dirigiendo sus recomendaciones en este sentido.

4. DICTAMEN DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS
Este documento se centra en la relevancia de la protección de los datos personales principalmente en tres objetivos: la relevancia de la intimidad y protección de datos personales; análisis del futuro reglamento general de protección de datos e identificación de áreas que precisan mayor actuación a nivel europeo desde la perspectiva de la protección de datos e intimidad.

5. DIRECTRICES DEL GSR12 SOBRE PRÁCTICAS IDÓNEAS
Se identifica que el Cloud Computing podría dar lugar a enormes ahorros en costos y potenciar la eficiencia e innovación a nivel de gobiernos, empresas y particulares. Sin embargo identifican la necesidad de que los organismos internacionales, reguladores y encargados de políticas, aúnen esfuerzos por la protección de datos.

CONCLUSIONES

El *Cloud Computing* es un modelo tecnológico que optimiza y facilita el almacenamiento de datos a las personas y especialmente a las empresas, brindando importantes ventajas de carácter económico al reducir costos permitiendo externalizar el soporte tecnológico de las compañías.

Con todo, así como ofrece ventajas, el *Cloud Computing* suscita algunos riesgos a los cuales debe prestarse atención para el correcto desarrollo de esta tecnología. Aspectos como la falta de transparencia respecto de quién controla y dónde son alojados los datos, falta de control de los mismos al ser externalizados, problemas de territorialidad al poder estar alojados incluso en plataformas extranjeras conlleva a considerar que el gran desafío para el correcto funcionamiento del *Cloud Computing* se encuentra en la protección de datos de sus usuarios.

A propósito de esto la normativa chilena regula a nivel genérico la protección de datos conforme a las reglas contenidas en la ley 19.628. La vanguardia regulatoria de estas materias se encuentra en las regulaciones internacionales, hacia las cuales Chile debiera apuntar, que regulan en forma específica las problemáticas que se suscita con el *Cloud Computing.*

DRONES
AERONAVE PILOTADA A DISTANCIA
REMOTELY PILOTED AIRCRAFT (RPA)

¿QUÉ ES UNA RPA?

Conviene señalar que la evolución en la tecnología ha gatillado importantes avances a nivel aeronáutico, que ha permitido pilotar naves a distancia. Este avance es mencionado incluso en el DAN 151, resolución que regula transitoriamente en Chile el uso de Aeronaves Pilotadas a Distancia en espacios públicos señalando lo siguiente:

"La aviación civil se ha basado hasta ahora en la noción de que un piloto dirige la aeronave desde el interior de ella misma y, con mucha frecuencia, con pasajeros a bordo. Retirar al piloto de la aeronave plantea importantes aspectos técnicos y operacionales, cuya magnitud se está estudiando activamente en la comunidad aeronáutica. Los sistemas de aeronaves no tripuladas (RPAS) son un nuevo componente del sistema aeronáutico, que la Organización de Aviación Civil Internacional (OACI), los Estados y la industria aeroespacial se proponen comprender, definir y, en última instancia, integrar" [7].

Comúnmente estos artefactos se conocen como *"drones"*. Pese a que este término no fue recogido por las regulaciones alrededor del mundo, es innegable indicar que la popularidad de esta tecnología ha crecido exponencialmente durante los últimos años y que ha venido para quedarse, razón por lo cual, no puede menos que existir una regulación al respecto.

De acuerdo a lo indicado en el DAN 151 se define como "todo vehículo no tripulado que es pilotado a distancia, apto para el traslado de cosas, y destinado a desplazarse en el espacio aéreo, en el que se sustenta por reacciones del aire con independencia del suelo". En el mismo sentido, se indica que debe ser "capaz de sustentarse en vuelo de acuerdo a sus formas aerodinámicas, pilotada a distancia por medios de control a través de sistemas electrónicos". Finalmente, un sistema RPAS no se conforma únicamente por la aeronave sino también por, la estación de control en tierra además de los medios y links necesarios para el control del vuelo.

ESTADO NORMATIVO EN CHILE

Actualmente la regulación en Chile, y sin perjuicio de los cuerpos normativos que regulan la actividad aeronáutica civil en general: Ley 18.916 y Convenio de Chicago, se remite a dos resoluciones dictadas por la Dirección General de Aeronáutica Civil (DGAC).

En primer lugar, nos encontramos con la DAN 91 que data de junio de 2013, denominada "Reglas del Aire, Anexo D, Sistema de Aeronaves Piloteadas a Distancia"; que se encarga de regular todos los vuelos que están fuera del interés público.

Esta resolución indica que toda nave usada en espacio nacional deberá contar con una autorización previa de la DGAC, notificar a los servicios de tránsito aéreo con una descripción de la operación que incluya los

[7] DAN 151.

requisitos de despegue y aterrizaje, además de las capacidades de comunicación, navegación, vigilancia, detección y procedimientos de emergencia.

A su vez, y complementado la anterior resolución, se publica en abril de 2015 la primera edición de la DAN 151, denominada "Operaciones de Aeronaves Pilotadas a Distancia (RPAS), en asuntos de interés público, que se efectúen sobre áreas pobladas".

La DAN 151 nace como respuesta a la necesidad de regular las "aeronaves sin piloto", inquietud que se venía gestando desde la celebración del Convenio de Chicago en 1944. Ello por cuanto el uso de RPAS en el ámbito civil se configura como una gran oportunidad para ejecutar diversas funciones, tales como captación rápida de noticias, control de fronteras, inspección de líneas de transmisión eléctrica, detección de incendios forestales, control de derrames tóxicos y control de la contaminación, vigilancia de erupciones volcánicas, prospección pesquera, fotografía y filmación desde altura.

Esta resolución tiene carácter transitorio, por cuanto será aplicable hasta que la DGAC emita una nueva normativa, una vez que la Organización de Aviación Civil Internacional (OACI) y/o el Sistema Regional de Cooperación para la vigilancia de la Seguridad Operacional (SRVSOP), publique los requisitos técnicos respecto a la operación de los RPAS, lo que se estima ocurrirá en 2018 y 2015 respectivamente.

No obstante, el objetivo de la DAN 151 consiste en regular las operaciones realizadas por las RPAS en servicios de interés público así como también regular las operaciones de estas aeronaves en el espacio aéreo chileno para que se desarrollen en forma segura junto con las aeronaves tripuladas, a fin de proporcionar un adecuado margen de seguridad operacional.

La norma se aplicará sobre toda persona o entidad que realice operaciones aéreas mediante RPAS de hasta 6 kilos, en asuntos de interés público sobre áreas pobladas o sobre áreas en donde no exista aglomeración de personas. Será la DGAC la encargada de determinar qué se entiende por interés público.

La DAN 151 indica que toda persona y/o entidad que desee realizar operaciones con RPAS, deberá obtener previamente una autorización de la DGAC y una credencial de acuerdo a lo establecido en capítulo D de la misma. Las operaciones de RPAS, deberán efectuarse en condiciones meteorológicas de vuelo visual y permanentemente a la vista y control del operador. Previo a iniciar un vuelo, el operador de un RPAS deberá determinar si la aeronave y su sistema de control se encuentran en condiciones seguras para operar.

A su vez, el tiempo total de vuelo en una operación de una aeronave RPAS, no podrá exceder el 80% de la total autonomía establecida por el fabricante, no pudiendo, en ningún caso, volar más de 60 minutos.

Todo propietario de un RPA, deberá registrarlo en el Sub departamento de Aeronavegabilidad de la DGAC.

¿QUÉ BUSCA PROTEGER LA NORMATIVA CHILENA?

Uno de los principales objetivos del DAN 151, es regular las operaciones efectuadas mediante aeronaves no tripuladas con el fin de garantizar la seguridad de éstas. La DGAC ha indicado que esta resolución se encuentra orientada, principalmente, a asuntos de interés público, cuidando la seguridad de las personas y sus bienes en operaciones que se desarrollen en lugares poblados.

Asimismo, la resolución establece una serie de prohibiciones que resguardan un conjunto importante de bienes jurídicos tales como la vida, la propiedad pública y privada, los derechos ajenos, entre otros.

En este sentido, el Capítulo B establece que durante la operación de un RPAS un operador no podrá:

- poner en riesgo la vida de las personas; poner en riesgo la propiedad pública o privada.
- violar los derechos de otras personas en su privacidad y su intimidad.
- operar en forma descuidada o temeraria que ponga en riesgo a otras aeronaves en tierra o en el aire.

Al respecto, se ha discutido la ausencia de prevenciones en el uso de RPAS tales como paracaídas. Lo anterior, por cuanto se ha estudiado incluso que una caída libre de un RPAS desde una altura de 200 pies, que corresponde a la mitad del máximo permitido, tiene la fuerza suficiente como para quebrar el cráneo de un niño.

En términos de seguridad, la resolución indica que un RPAS no podrá:

- operar a una distancia menor de dos kilómetros de la prolongación del eje de la pista y una distancia menor de un kilómetro paralelo al eje de la pista de un aeródromo.
- operar sobre zonas prohibidas, y peligrosas publicadas por la DGAC, en una AIP[8] Chile y disponible en la página Web institucional, operar sobre zonas restringidas, a menos que cuente con autorización de la Autoridad competente, operar sin tomar conocimiento de los NOTAMS[9] vigentes publicados por la DGAC, operar más de una aeronave en forma simultánea; operar en la noche sin una autorización especial.
- efectuar operaciones a una distancia mayor de 500 metros en una pendiente visual y a una altura mayor de 400 pies (130 m) sobre la superficie en que se opere.
- Ser utilizado para el lanzamiento o descarga de objetos desde el aire.
- operar bajo la influencia de las drogas o el alcohol y operar en las áreas donde se combate un incendio por medio de aeronaves tripuladas.

En términos de responsabilidad por el uso de una RPAS, la DAN 151 establece que será responsabilidad del operador de un RPAS cuidar la separación con otros RPAS operando en el área y coordinarse entre sí. Por otro lado, indica que el operador de un RPAS deberá considerar que debe ceder el paso a cualquier aeronave tripulada en las diferentes fases del vuelo, así como mantener su propia separación con otras aeronaves y que sin perjuicio a lo establecido en esta norma, toda persona o entidad involucrada en la operación de RPAS, deberá dar cumplimiento a todo requisito legal, tributario, municipal, sanitario, medioambiental o de seguros que exijan las entidades públicas en las normas respectivas. Como posible solución a la regulación y prevención del uso de RPAS, consideramos conveniente, la exigencia de un seguro de responsabilidad civil previo a la manipulación de estos artefactos, tal como ocurre en Argentina[10].

Por último, y con el fin de asegurar el resguardo de la propiedad de un RPA, es que dentro de los antecedentes exigidos para su registro, se debe acreditar el dominio mediante una declaración simple, indicando nombre completo del propietario, RUT, dirección, teléfono y correo electrónico.

---

[8] Publicación de Información Aeronáutica.
[9] Acrónimo en inglés de Notice To Airmen (Información para aviadores). Los NOTAM contienen información temporal cuyo previo conocimiento es de vital importancia para la realización del vuelo.
[10] DAN 151.

REFERENTES NORMATIVOS Y PRÁCTICOS A NIVEL INTERNACIONAL: RESOLUCIONES, OPINIONES Y DOCUMENTOS DE TRABAJO RELEVANTES

La OACI prevé que no antes del 2018 podría estar disponible una normativa de operación internacional de los RPAS para consulta a los Estados. Sin perjuicio de ello, varios han sido los Estados que, atendiendo a la urgencia de regulación que exige el tema, han emitido normas de carácter transitorio hasta que se consolide el estándar internacional.

1. ARGENTINA

Mediante la Resolución 527/2015[11] del 10 de julio de 2015, considerando que actualmente la OACI se encuentra elaborando el marco normativo que regulará la operación de dichos vehículos aéreos, aprueba el Reglamento Provisional de Vehículos Aéreos No Tripulados, considerando las previsiones de los artículos 4, 10 y 79 del Código Aeronáutico (Ley N° 17.285).

En el mismo documento se indica que, a medida que cada tema y tecnología alcancen suficiente madurez, se adoptarán Normas y Métodos Recomendados (SARPS, por su sigla en inglés: *Standards and Recommended Practices)* pertinentes, previendo que ello constituirá un proceso evolutivo y gradual.

Las disposiciones del Reglamento serán aplicables a las operaciones aéreas realizadas con vehículos aéreos no tripulados, cualquiera sea su naturaleza constructiva; a toda persona física o jurídica que pretenda obtener una autorización para operar RPA o RPAS o que pretenda ser miembro de la tripulación remota; y a toda persona que lleve a cabo la conservación o reparación de dichos vehículos.

Indica, a su vez, que todo sujeto que pretenda operar un RPAS deberá contar con una autorización expedida por la Administración Nacional de Aviación Civil (ANAC), con excepción de los vehículos pequeños con fines deportivos o recreativos y en las condiciones que se establezcan de conformidad con lo previsto en el Capítulo III de la regulación. Al respecto, la resolución indica que no se considerará como uso recreativo la fotografía o filmación no consentida de terceros o de sus bienes o pertenencias; la observación, intromisión o molestia en la vida y actividades de terceros ni la realización de actividades semejantes al trabajo aéreo.

LA OPERACIÓN DE RPAS SE PROHÍBE EN:

- espacios aéreos controlados, corredores visuales y helicorredores, excepto que, previamente, se haya obtenido una autorización especial de la autoridad aeronáutica con intervención del prestador de servicios de tránsito aéreo;
- áreas sensibles al ruido;
- área de influencia de la senda de aproximación o de despegue de un aeródromo
- zonas prohibidas, restringidas y/o peligrosas que se hayan establecido como tales, excepto que previamente se haya obtenido una autorización especial de la autoridad aeronáutica con intervención del prestador de servicios de tránsito aéreo.

La operación de un RPAS será responsabilidad de quienes la lleven a cabo o faciliten, incluyendo la responsabilidad por daños y perjuicios que puedan provocar a terceros durante sus operaciones. En este

[11] http://thomsonreuterslatam.com/2015/07/15/reglamento-provisional-de-los-vehiculos-aereos-no-tripulados-aprobacion/

sentido, y a diferencia de lo que ocurre en Chile, la legislación argentina exige a los propietarios u operadores de RPAS contratar un seguro de responsabilidad por los daños a terceros que pudiera ocasionar su operación. No se autorizará la circulación aérea de vehículo alguno previsto por este artículo, a menos que acredite tener asegurados tales daños. Las coberturas de riesgos no podrán ser inferiores a las establecidas, para aeronaves, en el artículo 160 del Código Aeronáutico.

Los RPAS no podrán operar sobre zonas densamente pobladas o aglomeración de personas, salvo excepción otorgada en los términos del artículo 8°.

La resolución agrega que:

- sólo se podrán operarán en horario diurno y en condiciones meteorológicas visuales que permitan su operación segura, ello por cuanto se encuentra prohibida su operación nocturna, salvo autorización excepcional
- los RPAS deberán contar con medidas adecuadas para su protección contra actos de interferencia ilícita, conforme a la reglamentación que oportunamente aprobará la autoridad aeronáutica, salvo autorización expresa de la autoridad aeronáutica, los vehículos aéreos pilotados a distancia o sistemas de vehículos aéreos pilotados a distancia tienen prohibido realizar vuelos acrobáticos
- se prohíbe la operación simultánea de más de un vehículo aéreo por la misma estación de piloto remoto a la vez;
- se indica que no podrán transportar personas o carga, excepto —en el caso de la carga— cuando fuera imprescindible para realizar la actividad que se hubiera autorizado.

Asimismo también se regula el uso de RPAS con fines recreativos o deportivos. Al respecto se exige que el piloto sea mayor de 16 años de edad y cumpla con los requisitos establecidos en el Capítulo V del reglamento:

- cuando la tripulación remota estuviera integrada por un miembro menor de 18 años y mayor de 16, deberá encontrarse bajo la supervisión directa de un mayor de edad responsable por sus actos y omisiones
- todo miembro de la tripulación remota de un RPAS deberá adoptar las medidas necesarias para comprobar el correcto funcionamiento del vehículo aéreo o sistema antes de iniciar su uso
- la operación será responsabilidad de quienes la lleven a cabo o faciliten, incluyendo la responsabilidad por los daños y perjuicios que puedan provocar a terceros durante sus operaciones
- que ningún miembro de la tripulación remota participará en su operación bajo los efectos del alcohol o drogas.

Finalmente se establece la existencia de un registro especial que será organizado y administrado por el Registro Nacional de Aeronaves:

- la obligación de los RPAS de llevar una placa de identificación inalterable fijada a su estructura
- fiscalización por parte de la Autoridad Aeronáutica.

2. UNIÓN EUROPEA

La Unión Europea publicó el “Resumen ejecutivo del Dictamen del Supervisor Europeo de Protección de Datos (SEPD) relativo a la Comunicación de la Comisión al Parlamento Europeo y al Consejo “Una nueva era de la aviación: Abrir el mercado de la aviación civil al uso civil de sistemas de aeronaves pilotadas de forma remota de manera segura y sostenible”

El documento describe a los RPA como aeronaves que pueden volar sin necesidad de contar un piloto a bordo y agrega que la mayoría de las veces no se utilizan en un sistema de aeronave simple, sino que incluyen dispositivos como cámaras, micrófonos, sensores y GPS que pueden permitir el tratamiento de datos personales.

Asimismo, el documento parte de la base que, siendo una tecnología emergente con el potencial de interferir gravemente en los derechos de respeto a la vida privada, familiar y a la protección de datos, deben ser considerados de manera cuidadosa, pues estos derechos se encuentran garantizados en el artículo 8 del Convenio Europeo de Derechos Humanos del Consejo de Europa[13] y en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea[14].

Por un lado, el documento destaca que los usos civiles de los RPAS abarcan todos los ámbitos no cubiertos por los usos militares, no limitándose, por tanto, a los usos comerciales, destaca a su vez la protección de datos y la seguridad como elementos clave en el tema, considerando que, al poder combinarse con otras tecnologías como los dispositivos de cámara, sensores de *Wi-Fi,* micrófonos, sensores biométricos, sistemas de GPS, los sistemas de lectura de direcciones IP, los sistemas de seguimiento de RFID[15], ofrecen la posibilidad de tratar datos personales y constituyen herramientas de vigilancia que potencialmente serían igual de poderosas.

El SEPD hace hincapié en que los usos de los RPAS que implican el tratamiento de datos personales constituyen, en la mayoría de los casos, una injerencia en el derecho de respeto de la vida privada y familiar, puesto que cuestionan el derecho a la intimidad y la privacidad garantizado para todas las personas físicas en la UE y, por tanto, únicamente puede permitirse en determinadas condiciones y con garantías específicas. En cualquier caso, cuando los RPAS operados en la UE tratan datos personales resulta aplicable el derecho a la protección de los datos personales consagrados en el artículo 8 de la Carta y debe cumplirse el marco jurídico europeo en materia de protección de datos.

El documento establece que los usos de los RPAS realizados por parte de las personas físicas, para actividades privadas quedarán sujetos a lo dispuesto en la legislación nacional de aplicación de la Directiva 95/46/CE[16] sobre Protección de Datos Personales y en raras ocasiones se beneficiarán de la excepción doméstica. En cualquier caso, como condición previa para las normas en materia de protección de datos, el tratamiento de datos personales deberá ser legítimo en todos los sentidos, lo cual implica que se cumpla con el resto de normas pertinentes en ámbitos como el derecho civil, derecho penal, propiedad intelectual, legislación aeronáutica o medioambiental.

En dichos términos, el SEPD recalca que no es suficiente para quedar amparada por la excepción de fines periodísticos del artículo 9 de la Directiva 95/46/CE la simple publicación de los datos en Internet o en un periódico, sin el objetivo de hacer pública la información, opiniones o ideas.

En términos de uso policial, el documento agrega que los RPAS también deberán respetar el derecho fundamental a la privacidad puesto que dichas actividades deben estar basadas en una legislación clara y accesible, que sirva a un fin legítimo y necesario en una sociedad democrática, y que sea proporcionada con el fin perseguido. Cuando tengan como consecuencia el tratamiento de datos personales, estarán sujetos a las garantías de protección de datos establecidos a nivel de la UE y del Consejo de Europa.

---

[13] http://www.echr.coe.int/Documents/Convention_SPA.pdf
[14] http://www.europarl.europa.eu/charter/pdf/text_es.pdf
[15] Radio Frequency IDentification, en español identificación por radiofrecuencia.
[16] http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:l14012

Por otro lado, para fines de investigación, el uso de los RPAS deberá respetar los principios de necesidad y proporcionalidad.

Por último, el SEPD apoya que la Comisión reconsidere su falta de competencia para regular los RPAS que pesen menos de 150 kilos, teniendo a la vista la necesidad imperiosa de garantizar el respeto de la privacidad, la protección de datos y los requisitos de seguridad relativos a esta nueva tecnología que resulta potencialmente muy intrusiva. A su vez recomienda que la Comisión anime a los fabricantes de RPAS a aplicar la protección de la intimidad mediante el diseño y la privacidad por defecto y que los responsables del tratamiento de los datos elaboren evaluaciones de impacto de la protección de datos cuando las operaciones de tratamiento planteen riesgos específicos para los derechos y libertades de los interesados en virtud de su naturaleza, ámbito de aplicación o fines y que se impulsen medidas que faciliten la identificación del responsable del tratamiento de un RPAS.

3. ESTADOS UNIDOS

En el caso de Estados Unidos, el "Acta de Modernización y Reforma (P.L. 112-095[17])" publicada en 2012 por la Federal Aviation Administration (FAA), estableció el 30 de Septiembre de 2015 como plazo fatal para que la institución emitiera una regulación que permitiera el uso comercial de los RPAS.

En el intertanto, la FAA ha otorgado permisos excepcionales para el uso de RPAS, basándose en la sección 333 de la P.L. 112-095.

El 15 de febrero del presente año, la FAA presentó una propuesta de marco regulatorio para el uso rutinario de RPAS. Esta considera cierta flexibilidad, con el fin de asegurar la cabida a futuras innovaciones tecnológicas.

La normativa propuesta se aplica sobre RPAS que pesen menos de 55 libras (25 kg.) utilizados en operaciones no recreativas. Sólo permite el uso de estos dispositivos durante el día y dentro de la visual de la línea de visión. El documento establece restricciones de altura, exige una certificación del operador, matrícula de la aeronave e indica los límites operacionales.

De acuerdo a la normativa propuesta, el operador de un RPAS no puede ser menor de 17 años, debe aprobar una prueba sobre conocimientos aeronáuticos y obtener un certificado de operador que otorga la FAA. Para mantener dicha certificación, el operador deberá repetir la prueba cada 24 meses.

La propuesta considera las siguientes limitaciones con el fin de minimizar los riesgos sobre otros RPAS, personas y derecho de propiedad:

- un operador de pequeños RPAS siempre debe ver y evitar los aviones tripulados, de existir riesgo de colisión, deberá ser el operador de RPAS quien primero maniobre para evitar dicho incidente
- el operador deberá detener el vuelo cuando su continuación configure un riesgo para otra RPAS, persona o propiedad
- el operador de un RPAS deberá considerar las condiciones climáticas, las restricciones aeroespaciales y la locación de las personas con el fin de disminuir los riesgo en caso de perder el control de la RPAS

[17] https://www.faa.gov/about/plans_reports/modernization/

- las pequeñas RPAS no podrá volar sobre personas, excepto aquellos directamente involucradas en el vuelo
- los vuelos no podrán superar los 500 pies con una velocidad máxima de 100 millas por hora
- los operadores de RPAS no podrán ingresar en los caminos de vuelo de los aeropuertos ni en las áreas espaciales restringidas y deberán obedecer todas las TFR's[18] de la FAA.

La norma propuesta mantiene la prohibición existente de operar una RPAS de manera descuidada o imprudente. También prohíbe al operador lanzar cualquier objeto desde la aeronave.

Los operadores de RPAS deberán cerciorarse de que su aeronave se encuentre en buen estado antes de volar, de lo contrario serán responsables por lo que dichas fallas pudieren ocasionar.

Las reglas indicadas en la propuesta no se aplicarán a los "Model Aircrafts", que de acuerdo a la FAA son aquellas aeronaves pilotadas a distancia utilizadas exclusivamente para propósitos recreacionales y/o deportivos, siempre que se mantengan dentro de la línea visual de visión del operador[19]. Quienes operen un Model Aircraft no requerirán autorización de la FAA, pero sí deberán cumplir con los requisitos establecidos en la sección 336 de la P.L. 112-95 que exigen, entre otros, que la operación se realice en contexto de pasatiempo y/o recreacional.

Por su parte, y en término generales, lo indicado en la propuesta no se aplicará al uso de RPAS por parte del gobierno, pues se espera que estas operaciones se sigan realizando bajo el COA[20], a menos que el operador decida someterse a esta nueva regulación y en tal caso cumplir con sus exigencias.

Por último, y según lo indica la página web de la FAA, lo más reciente en el tema consiste en que la FAA ha firmado un acuerdo pionero con CACI International Inc. para evaluar cómo la tecnología de la empresa puede ayudar a detectar Sistemas Aéreos No Tripulados (UAS) en las proximidades de los aeropuertos.

CONCLUSIONES

Tomando en cuenta el hecho de que las regulaciones expuestas poseen carácter transitorio, resulta necesario el perfeccionamiento de la regulación existente. Lo anterior, con el fin de favorecer el desarrollo comercial de los RPAS y de aprovechar la eficiencia que éstos brindan en múltiples actividades, debiendo siempre resguardarse los derechos y garantías fundamentales de quienes pudieren verse involucrados en operaciones con estos aparatos.

Dicho lo anterior, no es posible desconocer el hecho de que el uso de RPAS incide en aspectos de relevancia jurídica, tales como la protección de datos, propiedad privada, seguridad de la información, integridad física e, incluso, la vida de las personas. Todo esto manifiesta la necesidad de establecer procedimientos que resguarden el íntegro cuidado de estos derechos, tales como mayor ahondamiento dentro de las resoluciones de la DGAC y exigencias de seguros, entre otros que han sido expuestos a lo largo de este informe.

---

[18] Temporary Flight Restrictions: Restricciones Temporales de Vuelo.
[19] https://www.faa.gov/uas/media/model_aircraft_spec_rule.pdf
[20] Certificate of Waiver or Authorization.

INTERNET DE LAS COSAS

La caracterización de Internet de las Cosas ya ha sido desarrollada en el capítulo [XXX] de este informe de economía digital 2015. Sin embargo, a continuación se desarrollan algunos posibles problemas de carácter jurídico o legal a los que habría que prestar atención a la hora de utilizar internet de las cosas.

Dentro de las principales características del Internet de las Cosas se encuentra su fragmentación por industrias, de manera que los softwares, aplicaciones, servicios, plataformas tecnológicas etc., resultan poco interoperables. No hay estándares comunes, siendo este, principalmente, el motivo de la fragmentación.

Otro fenómeno que merece prestarle atención es la creación de alianzas entre compañías de comunicaciones con otras industrias, como por ejemplo la automovilística, en la cual fabricantes de autos y compañías de telecomunicaciones desarrollan autos conectados. Esto podría suscitar algunos problemas de libre competencia o ventas atadas, por ejemplo, por condicionar la elección de un producto en consideración al sistema operativo que este utilice, de manera tal que sea compatible con nuestros dispositivos móviles como *smartphones o tablets.* A partir de ello se estaría dando mayor poder de mercado a los grandes de la industria tecnológica y de telecomunicaciones. Será necesario que los clientes de servicios de Internet de las Cosas puedan cambiar de proveedor sin necesidad de cambiar sus equipos o aparatos y sin que ello acarree la pérdida de información ni condicione la compra de dispositivos que sólo se ajuste a los sistemas operativos.

REGULACIÓN Y EXPERIENCIA COMPARADA: UNIÓN EUROPEA Y ESTADOS UNIDOS

Mirando este fenómeno, ahora desde una perspectiva regulatoria, ocurre que, al igual que Internet en general, no existe regulación específica respecto de Internet de las Cosas ni para comunicaciones entre máquinas. La regulación será, como ha anticipado la Comisión Europea, a nivel de autorregulación. Actualmente no va mucho más allá que la atribución de determinados rangos de numeración específicos para estas comunicaciones que existen en algunos países. Tanto el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (BEREC, por sus siglas en inglés) como la FTC americana se reunieron a final del año pasado, cada uno por su lado y a cada lado del Atlántico, para discutir los problemas o retos jurídicos que plantea el nuevo Internet. La Comisión Europea ya inició hace tiempo discusiones sobre la arquitectura de Internet de las Cosas y su gobierno, para lo que ha lanzado varias consultas. El paquete normativo que la Unión Europea está en proceso de adoptar, conocido como Continente Conectado o Mercado Único de las Comunicaciones Electrónicas, puede que resuelva algunos de los problemas existentes.

Uno de los principales retos, desde una perspectiva legal, para Internet de las Cosas dice relación con aspectos de privacidad y la seguridad. En efecto, estas son las principales objeciones que los consumidores parecen tener a la hora de utilizar objetos conectados y una de las mayores preocupaciones de los reguladores. Los objetos conectados recaban datos, los intercambian, procesan y almacenan automáticamente. Parte de esta información es derechamente personal o bien puede convertirse en información personal luego de procesos de agregación.

En Estados Unidos, la FTC presentó cargos por primera vez contra un prestador de Internet de las Cosas con motivo de una infracción de las normas de privacidad y seguridad. En la Unión Europea, el Proyecto de Reglamento General de Protección de Datos incluye algunos nuevos conceptos de mucha relevancia para

Internet de las Cosas, algunos de los cuales, pese a que el Reglamento todavía está en fase de discusión por el Consejo, han sido incorporados a la reciente Opinión de Grupo de Autoridades Europeas de Protección de Datos de los Estados miembros (GT29) sobre el Internet de las Cosas. El GT29 resalta por ejemplo la importancia de la portabilidad de los datos al cambiar de proveedor, de la privacidad y seguridad por defecto y desde el origen del diseño del equipo o aparato, y de que los aparatos ofrezcan visibilidad sobre si transmiten o no datos personales de su entorno.

La cadena de valor en Internet de las Cosas es compleja y con numerosas capas o agentes que acceden, transmiten y almacenan esos datos. Los puntos susceptibles de ser ciberatacados o accedidos por objetos no identificados son mucho más sensibles y apegados a nuestra intimidad, si pensamos en hogares y coches conectados.

El Internet de las Cosas trae consigo una inseguridad en nuestra información personal altamente preocupante. En un futuro no muy lejano nuestro propio hogar puede convertirse en un objetivo valioso en donde un solo fallo de seguridad podría dejar al descubierto nuestra información personal con sorprendente facilidad.

En la experiencia comparada ya ha habido numerosos ataques documentados contra dispositivos conectados a Internet e incluso a la industria automovilística. Un artículo publicado por "Wired" describió cómo el sistema central informático de un *Jeep Cherokee* permitió a dos hackers hacerse cargo de los controles esenciales del vehículo (incluidos los frenos) de forma remota, un recordatorio de la importancia de una seguridad fiable y sin ningún tipo de brecha posible.

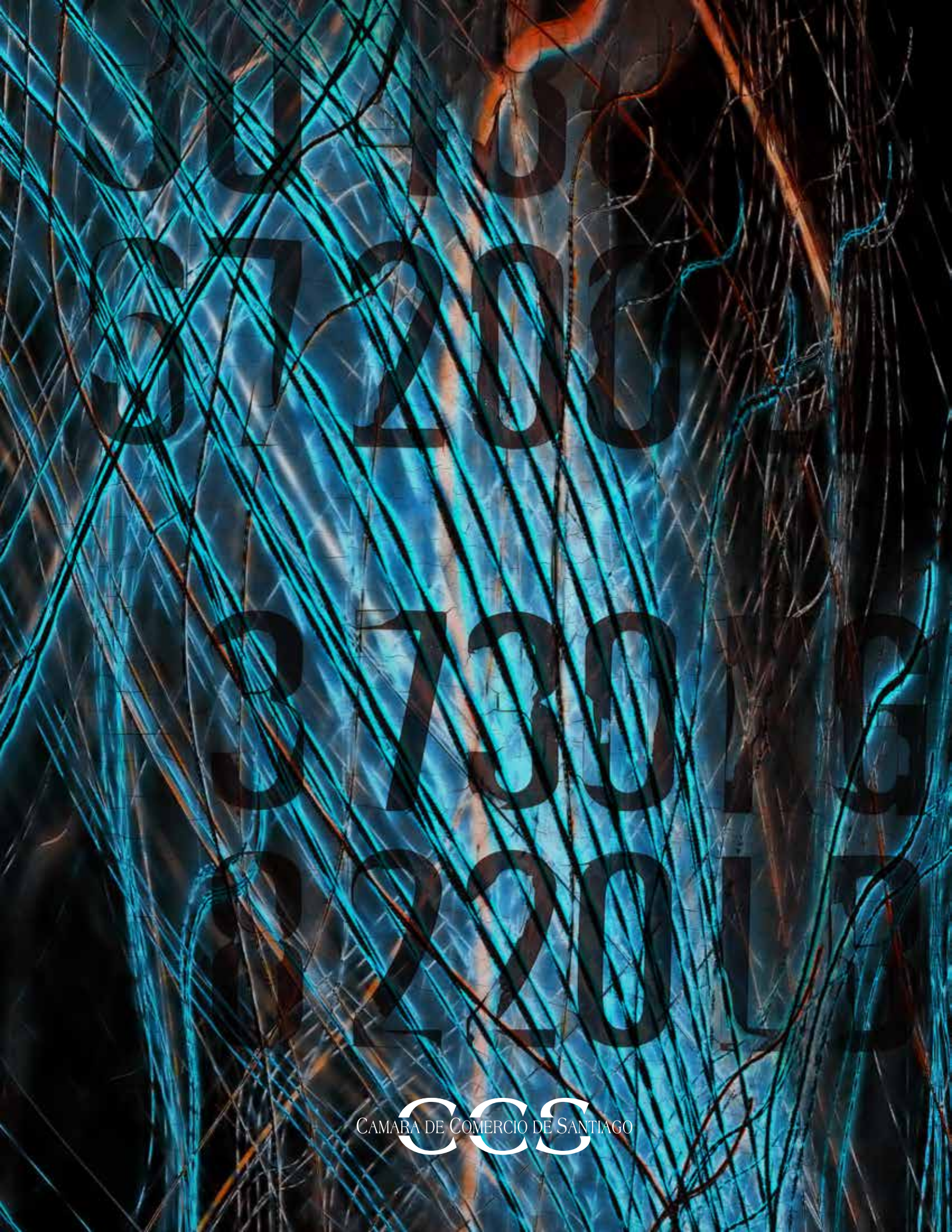
Estos riesgos se extienden también a dispositivos aparentemente infalibles, generando gran cantidad de fallos en la seguridad del usuario y permitiendo a los hackers entrar en la vida cotidiana de los usuarios a través de dispositivos tan aparentemente inofensivos como turbadores como los *monitores para bebés,* disponiendo de total autonomía de los monitores y convirtiéndolos en cámaras espía. En el momento actual en el que incluso el refrigerador no está a salvo de un ataque, se requiere una solución apta para cada dispositivo, con el propósito de facilitar el uso seguro del Internet de Las Cosas y todos sus beneficios.

La gran cantidad de dispositivos que están comenzando a formar parte del Internet de Las Cosas se está convirtiendo en un rompecabezas legal, llegando a ser un problema de tal calibre que el FBI ha alertado sobre la falta de seguridad de los mismos.

La realidad es que el Internet de las Cosas requiere de una nueva infraestructura de seguridad en base a sus criterios técnicos, un factor que es crucial para el éxito de la plataforma. La importancia de estas cuestiones ha sido planteada por la *Comisión Federal de Comercio (Federal Trade Commission)* que están instando a las empresas a construir una seguridad específica para los dispositivos conectados a Internet de Las Cosas desde el principio, así como para garantizar unas normas de calidad internas y externas actualizadas, de manera que sean capaces de garantizar la seguridad de los productos y sus usuarios.

CONCLUSIONES

El novedoso desarrollo de Internet de las Cosas ha llevado a que esté muy por delante de cualquier regulación o normativa tanto a nivel comparado como nacional. Los principales problemas de carácter jurídico se suscitan a propósito de la ciber seguridad de los dispositivos conectados a Internet de las Cosas. Para enfrentar esta problemática hace falta, de una parte una regulación adecuada que se haga cargo de estos problemas. Sin embargo, de otra parte, es necesario crear conciencia en consumidores y usuarios de que seguridad digital ha trascendido a los computadores abarcando un sinnúmero de objetos capaces de conectarse a Internet.


CAMARA DE COMERCIO DE SANTIAGO