UNIVERSIDAD DE CHILE FACULTAD DE DERECHO

PROGRAMA DE MAGISTER EN DERECHO CON MENCION EN DERECHO PÚBLICO

Seguridad Documental y Protección de Datos Personales en la Contratación Electrónica de Créditos de Consumo

Alumno: Raúl Arrieta Cortés

Profesora Guía: Lorena Donoso Abarca

julio 2021

A Vanessa, compañera de vida, sueños e inspiración.

A mis hijos, fuentes de amor infinito y superación.

Resumen

El auge del comercio electrónico ha llevado a extender la contratación electrónica a diferentes tipos de bienes y servicios. El crédito de consumo no se ha encontrado ajeno a dicha situación y, muy por el contrario, día a día proliferan más mecanismos y fórmulas que permiten a las personas contratar esta clase de créditos sin necesidad de desplazarse hacia las instituciones financieras.

El objetivo general de la investigación es analizar el marco en que se desenvuelve la prestación de esta clase de servicios financieros cuando opera a través de los medios y técnicas electrónicas, verificar si en el estado actual permite promover una contratación segura, donde se pueda determinar con certeza la identidad de los clientes, la fijación del contenido contractual y la adecuada protección de los derechos de las personas, tanto en materia de contratos de consumo como de protección de datos personales y proponer aquellas modificaciones que sean necesarias para garantizar estos objetivos.

Sostenemos, que el marco normativo e institucional debe promover un desarrollo seguro que permita garantizar no sólo la autenticidad, fiabilidad e inalterabilidad del contrato, sino también que los derechos de los contratantes no se verán lesionados por el hecho de recurrir a esta forma de contratación, especialmente la protección de los datos personales.

Índice

Abreviaturas y acrónimos

ANSI	Por sus siglas en inglés «American National Standards Institute»
CC	Código Civil
CCom	Código de Comercio
CMF	Comisión para el Mercado Financiero (Chile)
COT	Código Orgánico de Tribunales
FEA	Firma Electrónica Avanzada
FIPS	Por sus siglas en inglés «Federal Information Processing Standard»
NIST	Por su sigla en ingles «National Institute of Standards and Technology» (U.S)
PKI	Por sus siglas en inglés «Public Key Infrastructure»
RSA	Por sus siglas en inglés «Rivest, Shamir y Adleman)
RUN	Rol Único Nacional
SERNAC	Servicio Nacional del Consumidor (Chile)
SHA	Por sus siglas en inglés «Secure Hash Algorithm», Algoritmo de Hash Seguro

Introducción.

Internet, con el transcurso de los años se ha erigido como un medio privilegiado y preferido tanto por los consumidores y usuarios como por los proveedores para llevar a cabo negocios en distintas modalidades. En nuestro caso nos interesa la contratación "B to C" de créditos de consumo a través de plataformas electrónicas.

Este veloz crecimiento y desarrollo de los servicios de la sociedad de la información ha motivado el surgimiento de nuevas tendencias en contratación, impulsadas principalmente por las ventajas que ofrecen las plataformas electrónicas. Aspectos como: amplitud de la oferta, flexibilidad horaria, posibilidad de contrastar con otros oferentes, mayor acceso a información junto a la comodidad de contratar desde donde se esté, ha generado un aumento de la contratación por medios electrónicos, consolidando así el modelo de negocios de comercio electrónico[1].

En el contexto de pandemia, ocasionada por el COVID-19, se ha acelerado aún más el desarrollo del comercio electrónico tanto en Chile como en el mundo, llevándolo a niveles inéditos. Por ejemplo, la última versión del Cyberday desarrollado por la Cámara de Comercio de Santiago generó ventas por más de 640 millones de dólares[2] y la adquisición

[1] CÓRDOVA, D. 2016. Régimen de responsabilidad de compañías de descuento por Internet, ¿Proveedores Intermediarios? En Revista de Derecho, Universidad Católica del Norte, Sección Estudios, Año 23, pp. 23 – 67. p. 25. RDUCN. 2016, vol.23, n.2, pp.23-67. ISSN 0718-9753. [en línea] <http://dx.doi.org/10.4067/S0718-97532016000200002>. [consulta: 19 de julio de 2021].

[2] CÁMARA DE COMERCIO DE SANTIAGO. CyberDay 2021 duplica expectativas y se transforma en el evento más importante en la historia del e-commerce chileno. 2021. [en línea] <https://www.ccs.cl/2021/06/03/cyberday-2021-duplica-expectativas-y-se-transforma-en-el-evento-mas-importante-en-la-historia-del-e-commerce-chileno/> [consulta: 06 de junio de 2021]

de más de 15 millones de unidades de bienes y servicios. Para este 2021 se proyectan ventas de comercio electrónico por más de 10.000 millones de dólares[3].

Entre la variedad de negocios que se pueden desarrollar por Internet se encuentra la contratación de créditos de consumo. De acuerdo a información que publica la Comisión para el Mercado Financiero (CMF), durante el 2020 la contratación de este tipo de créditos superó en Chile alcanzó un monto total superior a los 115 mil millones de pesos[4].

En esta investigación se argumenta que la contratación electrónica del crédito de consumo tiene en nuestro país una regulación suficiente para dotar de certeza jurídica a los diferentes operadores jurídicos que conviven con las nuevas formas de contratación y que además, dota de la seguridad suficiente a los consumidores que se enfrentan a este tipo de contratos tanto en los aspectos contractuales como en materia de protección de datos.

Sin embargo, estimamos que la comunidad jurídica no ha logrado tomar conocimiento y adoptar estas nuevas formas contractuales. Es así como la causa más recurrente en el letargo de adopción de este tipo de sistemas dice relación más bien con una resistencia hacia las nuevas formas, por el temor frente a una eventual judicialización del cobro de los saldos adeudados. Esto se origina en el temor que produce lo desconocido, y la percepción de falta de certeza de los efectos jurídicos prácticos y no por el hecho de que el estatuto jurídico no reconozca de manera categórica estas formas.

Dicho en otros términos, la falta de adopción podría deberse a una escasa alfabetización digital de los operadores jurídicos que les lleva a no correr el riesgo de apoyar la

---

[3] CÁMARA DE COMERCIO DE SANTIAGO. CyberDay 2021 se inicia el lunes 31 de mayo con 670 participantes. 2021 [en línea] <https://www.ccs.cl/2021/05/25/cyberday-2021-se-inicia-el-lunes-31-de-mayo-con-670-participantes/> [consulta: 06 de junio de 2021]

[4] COMISIÓN PARA EL MERCADO FINANCIERO. Resumen de préstamos otorgados anualizados. 2021. [en línea] <https://www.cmfchile.cl/portal/estadisticas/617/w3-propertyvalue-21028.html> [consulta: 06 de junio de 2021].

transformación digital a través de estas nuevas formas contractuales por temor a que, frente a la judicialización de un caso, los tribunales fallen de manera adversa a los intereses de sus clientes.

Sin embargo, esta misma falta de adopción se ha traducido en una escasa validación jurisprudencial que sirva de sustento a los intereses que se busca resguardar.

En este contexto, el objetivo general de esta Actividad Formativa Equivalente a Tesis consiste en sistematizar el régimen regulatorio aplicable a contratación electrónica de los créditos de consumo en Chile, especialmente respecto a la seguridad documental y protección de datos personales, a fin de facilitar la comprensión de esta normativa que permita a los operadores jurídicos adquirir las competencias que les permitan aplicar esta normativa en sus labores de asesoría y consultoría, o en la labor de defensa en eventuales conflictos de intereses de relevancia jurídica asociados a su aplicación en la contratación de créditos de consumo.

Los objetivos específicos que guían esta actividad son:

1. Revisar las consideraciones legales que deben tenerse en cuenta en la implementación de la contratación electrónica de créditos de consumo;

2.- Analizar las principales cuestiones normativas asociadas a la inmaterialidad documental que sustenta esta clase de operaciones a los efectos de construir la evidencia que permita intervenir y defender en sede judicial los términos de la operación de crédito de dinero;

3.- Determinar el estatuto jurídico de la seguridad en esta clase de contratos desde la perspectiva del derecho del consumo y de la protección de datos personales;

4.- Proponer posibles mejoras normativas y de implementación que permitan disminuir los roces que la incorporación de tecnología produce en parte de los operadores jurídicos y con ello aumentar la seguridad y confianza en esta forma de contratación que produce beneficios incalculables para todos los actores que intervienen del proceso.

Estimamos que la investigación es novedosa porque no existen obras en esta materia, y es necesaria, por las incertidumbres que se observa en el medio nacional.

Para ello, en primer lugar, se analizó el régimen jurídico aplicable a la contratación electrónica del crédito de consumo, definiéndose las características, principios y formación del consentimiento en la contratación electrónica en general y en la contratación de créditos de consumo en particular.

En segundo lugar, revisamos los aspectos relacionados con seguridad en una doble dimensión. Por una parte, desde el punto de vista de la seguridad documental, considerando el régimen jurídico desarrollado por la Ley 19.799 para los documentos y la firma electrónica, ambos medios que se plasman como la piedra angular del comercio electrónico seguro. Por otra parte, la seguridad desde la perspectiva del derecho del consumo y la protección de datos personales, de manera de comprender el régimen de responsabilidad y el conjunto de obligaciones de seguridad que pesan sobre las instituciones financieras a la hora de disponibilizar las técnicas y medios electrónicos para el otorgamiento de créditos de consumo, de manera de dar cobertura y asegurar la efectiva protección de datos personales, erigido como derecho fundamental desde su constitucionalización en 2018[5], y de las reglas previstas en el derecho del consumo.

Por último, finalizamos la investigación con unas breves propuestas de mejora, recomendaciones en la implementación de estas herramientas y conclusiones.

Metodológicamente, la investigación ha seguido el método dogmático tradicional, analizando el problema desde los aspectos más generales a los más específicos, consultando tanto fuentes directas como indirectas. Entre las primeras, se ha analizado la

[5] Ley 21.096 por intermedio de la cual se agregó en el numeral 4° del artículo 19 de la Constitución Política de la República, a continuación de la expresión "*y su familia*", lo siguiente: "*, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley*".

escasa doctrina, normativa y jurisprudencia existente en nuestro entorno. En el ámbito de derecho comparado, las principales referencias se hacen al Reglamento Europeo de Protección de Datos y su normativa complementaria.

La principal limitación que tuvimos para esta investigación radica en el hecho de que no hay una nutrida doctrina ni jurisprudencia en nuestro país respecto a la contratación electrónica ni a la seguridad en materia de protección de datos personales. Sin perjuicio de lo anterior, rescatamos y analizamos la escasa jurisprudencia existente hasta la fecha de la entrega de este trabajo.

Asimismo, advertimos que, si bien en una época temprana, esto es, los primeros años después de la dictación de la ley de firma electrónica, la doctrina se hizo cargo de parte de sus normas, desde algunos años a esta fecha no se han producido obras jurídicas que analicen los aspectos más prácticos y contingentes de su aplicación a los diversos ámbitos del quehacer jurídico.

En consecuencia, la falta de doctrina y la escasa jurisprudencia es un factor crítico dentro de la ruta de masificación de este tipo de sistemas. Ello genera incertidumbres respecto a la forma en que razonarán los tribunales y una escasa construcción en la base argumental que permita afirmar la validez, pertinencia y seguridad de los documentos electrónicos en el comercio y la contratación electrónica.

Así, con una mirada esencialmente práctica, el resultado de este trabajo está orientado a proveer un análisis estructurado de las condiciones bajo las cuales la contratación electrónica de los créditos de consumo resulta ser jurídicamente sustentable e incluso en algunos casos mucho más segura y certera para las partes que la tradicional contratación en papel.

CAPÍTULO I.- RÉGIMEN JURÍDICO APLICABLE A LA CONTRATACIÓN ELECTRÓNICA DEL CRÉDITO DE CONSUMO.

1.1 El Crédito de Consumo.

El crédito o préstamo de dinero, conforme prescribe la ley 18.010, es un contrato o convención que se caracteriza porque una de las partes entrega o se obliga a entregar una cantidad de dinero y la otra a pagarla en un momento distinto de aquel en que se celebra (artículo 1). Si concordamos esta norma con el artículo 578 del Código Civil, diremos que de este contrato emanan derechos personales para las partes. Tratándose de dinero, un bien fungible, conforme a lo previsto en el art. 2197 CC, el contratante adquirirá el dominio del dinero que recibe en préstamo, pudiendo destinarlo a las finalidades que estime conveniente, y se obligará a restituirlo en el futuro en la forma y con los intereses que se establecen en el mismo contrato.

Cuando el crédito es de consumo, permite la libre disponibilidad de la cantidad de dinero que se pacte.

Ahora bien en la doctrina, siguiendo a AGUILERA y CERDA, los créditos de consumo pueden ser definidos como aquellos en los que el deudor, persona natural, tiene como finalidad destinar los recursos obtenidos a la adquisición de bienes que satisfacen necesidades de consumo, pudiendo ser durables o no[6].

Continuando nuestro análisis normativo, el Decreto Supremo Nº 43, de 2012, del Ministerio de Economía, Fomento y Turismo (Reglamento de Información al Consumidor de Crédito de Consumo) define en el artículo 3º el crédito de consumo en los siguientes términos:

---

[6] GUTIÉRREZ, P. 2018. Vivir con deudas en Chile. Análisis de la estructura, fallas y regulación en el mercado de créditos al consumo (Memoria para optar al grado de Licenciada en Ciencias Jurídicas y Sociales), Universidad de Chile. [en línea] <http://repositorio.uchile.cl/bitstream/handle/2250/150946/Vivir-con-deudas-en-Chile-an%C3%A1lisis-de-la-estructura-fallas-y-regulaci%C3%B3n-en-el-mercado-de-cr%C3%A9ditos-al-consumo.pdf?sequence=1&isAllowed=y> [consulta 15 junio 2021], p. 30.

"El producto financiero en virtud del cual una parte denominada proveedor, entrega o se obliga a entregar una cantidad cierta de dinero a otra parte denominada consumidor, que se obliga a pagarla en un determinado plazo o número de cuotas, incluyendo la suma de dinero que resulte de la aplicación de una tasa de interés determinada al momento de la contratación".

La Ley 19.496 de protección a los derechos de los consumidores, por modificación introducida por la ley 20.555 (SERNAC Financiero) avanzó en orden a regular el otorgamiento de los créditos, establecer normas y procedimientos destinados a regular la oferta, venta y prestación de productos y servicios financieros, entre los cuales se incluyen los créditos hipotecarios, créditos de consumo, tarjetas de pago, seguros, etc.[7].

Con ello se ha buscado mejorar el acceso al consumidor de créditos en condiciones más transparentes, en base a una intensificación de los deberes de información que debe satisfacer el proveedor de cara a la contratación de un crédito[8].

El artículo 37 de la Ley 19.496 establece la obligación del proveedor de informar lo siguiente:

Artículo 37.- En toda operación de consumo en que se conceda crédito directo al consumidor, el proveedor deberá poner a disposición de éste la siguiente información:

[7] BOZZO, S. 2020. Sobreendeudamiento del consumidor en Chile: Una revisión a la luz del derecho europeo. En Revista de Derecho (Valdivia). Vol. XXXIII – Nº1, junio 2020, ISSN 0716-9132 / 0718-0950, pp 159-183. p. 167. [en línea] <https://www.scielo.cl/pdf/revider/v33n1/0718-0950-revider-33-01-159.pdf> [consulta: 07 de junio 2021].

[8] GOLDBERG, J.L. 2017. El necesario ajuste de la asignación del riesgo de sobreendeudamiento en la regulación de las tarjetas de crédito: desde un sistema basado en los deberes de información a un modelo de corresponsabilidad. En Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, Nº 49, 2º semestre, p. 66.

a) El precio al contado del bien o servicio de que se trate, el que deberá expresarse en tamaño igual o mayor que la información acerca del monto de las cuotas a que se refiere la letra d);

b) La tasa de interés que se aplique sobre los saldos de precio correspondientes, la que deberá quedar registrada en la boleta o en el comprobante de cada transacción;

c) El monto de los siguientes importes, distintos a la tasa de interés:

1. Impuestos correspondientes a la respectiva operación de crédito.

2. Gastos notariales.

3. Gastos inherentes a los bienes recibidos en garantía.

4. Seguros expresamente aceptados por el consumidor.

5. Cualquier otro importe permitido por ley;

d) Las alternativas de monto y número de pagos a efectuar y su periodicidad;

e) El monto total a pagar por el consumidor en cada alternativa de crédito, correspondiendo dicho monto a la suma de cuotas a pagar, y

f) La tasa de interés moratorio en caso de incumplimiento y el sistema de cálculo de los gastos que genere la cobranza extrajudicial de los créditos impagos, incluidos los honorarios que correspondan, y las modalidades y procedimientos de dicha cobranza.

g) Los efectos del incumplimiento del crédito concedido y los efectos procesales del ejercicio de la acción ejecutiva en los casos que corresponda, tales como el embargo, el retiro y remate de bienes, entre otros, de conformidad al reglamento.

Sin perjuicio de lo anterior, cuando se exhiban los bienes en vitrinas, anaqueles o estanterías, se deberán indicar allí las informaciones referidas en las letras a) y b) del inciso anterior.

De acuerdo a ESCALONA, dado que no existe un sujeto calificado en esta norma, la regla permea no solo a bancos e instituciones financieras sino a todo establecimiento comercial que conceda créditos al consumidor como tiendas de departamento, supermercados, cooperativas, cajas de compensación, automotoras, farmacias o cualquier otro agente del mercado que otorgue créditos en forma directa. Excluyéndose, únicamente, aquellos proveedores que, sin conferir crédito, admiten que los productos que comercializan sean adquiridos a través de créditos otorgados por terceros[9].

El mecanismo de obtención de un crédito de consumo es bastante simple. Previo a la suscripción del contrato de crédito de consumo, el futuro deudor debe ingresar una solicitud a la institución financiera que evaluará la situación económica de la persona a fin de determinar el nivel de riesgo que significa realizarle un préstamo de dinero. Según este análisis se determinará el monto máximo al cual podrá acceder el futuro deudor y también permitirá establecer las condiciones del préstamo (cantidad de cuotas, intereses y garantías)[10]. Tomada la decisión de otorgar el crédito vendrá el proceso de suscripción del contrato de crédito de consumo, el que no obstante la libertad contractual que tienen las partes para pactarlo se encuentra sujeto a una especie de dirigismo contractual, pues, el artículo 11 del Reglamento de Información al Consumidor de Crédito de Consumo establece las especificaciones mínimas de los créditos de consumo con el objeto de promover su simplicidad y transparencia.

En atención a los avances tecnológicos y el marco jurídico vigente los oferentes de crédito han buscado generar los mecanismos que permitan otorgar los créditos de consumo incorporando toda la tecnología posible, de manera reducir los costos en su otorgamiento,

---

[9] ESCALONA, E. 2013. Artículo 37, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile. p. 813.

[10] GUTIÉRREZ, P. 2018, cit. nota n. 6, p. 31.

incrementar la colocación de éstos, evitar que los solicitantes deban concurrir a las oficinas de la institución financiera, etc.

En términos muy simples, el desafío ha estado en impulsar el comercio electrónico de créditos de consumo, con la finalidad de facilitar la vida de quien requiera el crédito, sin que se deteriore la seguridad jurídica de quienes intervienen en el proceso.

1.2 La contratación electrónica.

La contratación electrónica es otra manifestación de los cambios que se han producido en la economía de fines del siglo XX y lo que llevamos avanzado del XXI, en que la tendencia a la globalización parece ser la pauta. La tecnologización no es sino un nuevo canal para llevar a cabo distintas actividades, como comunicaciones y contrataciones, sin embargo, no implica una distorsión en cómo se conciben las cosas, las compraventas seguirán siendo compraventas y la prestación de servicios conserva tal carácter. Han surgido y surgirán nuevos modelos de negocios y contratos innominados, formas de pago y garantías. Todo ello influenciado por las nuevas tecnologías de la información[11].

Hoy no se discute que la modalidad negocial electrónica sea otra forma válida para la exteriorización de la voluntad, principio que hoy se encuentra, además, reconocido en términos explícitos bajo la denominación de *principio de validez y eficacia de la forma electrónica, y en los principios de equivalencia de los soportes, y no discriminación*[12].

En tal sentido, el artículo 3º de la Ley 19.799, sobre documento electrónico, firma electrónica y los servicios de certificación de dichas firmas, dispone que:

---

[11] SILVA, P. 2003. Autonomía de la Voluntad, Contratación Electrónica y Protección del Consumidor. Revista Chilena de Derecho Informático (3): 113 – 137. pp. 117 – 118.

[12] PINOCHET, R. 2009. Derecho Civil y Nuevas Tecnologías: la formación del consentimiento electrónico. Santiago, Legal Publishing Chile. 270p. p. 95.

"Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte papel[13]".

De este modo, la equivalencia funcional entre el soporte papel y el electrónico se configura como la piedra angular del comercio electrónico seguro, al reconocer que, salvo exclusión legal expresa, todos los actos jurídicos que se ejecuten o celebren en soporte electrónico valdrán al igual que sus homólogos en papel. Ello, nos conduce a reconocer que es posible concebir con pleno valor jurídico y probatorio todo el proceso de contratación de un crédito de consumo a través de plataformas electrónicas.

Sin perjuicio de que en el ordenamiento jurídico chileno existan normas que aludan a la contratación electrónica, como la Ley 19.799 o la Ley 19.496, a propósito de la celebración de contratos electrónicos en el contexto de consumo, no existe una definición legal de los contratos electrónicos o de contratación electrónica. En tal sentido, ARCOS, señala que, ante la inexistencia de un estatuto autónomo que reglamente la celebración de contratos por medios electrónicos, se hace necesario estudiar leyes separadas para construir su régimen jurídico[14].

No obstante, echando mano tanto a la doctrina como a regulaciones de nuestro entorno de referencia, es posible construir un concepto de contratación o contrato electrónico. Así, por ejemplo, de acuerdo con DAVARA, contrato o contratación electrónica podría definirse de la siguiente manera:

---

[13] PINOCHET, R. 2009, cit. nota n. 12, pp. 95-96.

[14] ARCOS, M. 2012. Contratos de adhesión electrónicos: análisis a los contratos de retail electrónicos y contratos de servicios de suscripción en línea, películas, televisión y otros tipos de entretenimiento audiovisual. Santiago, Fundación Fernando Fueyo, Universidad Diego Portales. 47p. p. 16

"*Aquella que se realiza mediante la utilización de algún elemento electrónico cuando éste tiene, o puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo*[15]."

PINOCHET, por su parte, advierte que diversos autores conciben la noción de contratación electrónica en un sentido similar, concluyendo, al final, que cualquier contrato celebrado a través de medios electrónicos es un contrato electrónico. Siendo la clave, en consecuencia, que la voluntad sea exteriorizada por cualquier clase de medios que puedan calificarse de electrónicos: lo que conllevará como consecuencia natural la posibilidad de archivo y transmisión electrónica del mismo[16].

En normativas de referencia, en el anexo de la ley española de Servicios de la Sociedad de la Información (LSSI), se define al "contrato celebrado por vía electrónica" o "contrato electrónico", en los siguientes términos:

"*Todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones".*

En la Ley General para la Defensa de Consumidores y Usuarios de ese mismo país, por su parte, se indica en su artículo 94, relativo a las Comunicaciones comerciales y contratación electrónica lo siguiente:

"En las comunicaciones comerciales por correo electrónico u otros medios de comunicación electrónica y en la contratación a distancia de bienes o servicios por medios electrónicos, se aplicará además de lo dispuesto en este título, la normativa específica sobre servicios de la sociedad de la información y comercio electrónico".

---

[15] DAVARA, M.A. 1997. Manual de Derecho Informático. Pamplona, Ed. Aranzadi, 1997. 610p. p. 189.

[16] PINOCHET, R. 2009, cit. nota n. 12, p. 119.

Atendido que el elemento común en estas definiciones es el canal a través del cual se desarrolla el contrato, a continuación, conviene precisar, qué ha de entenderse por "medio electrónico".

Al respecto, la Ley 19.799 informa, en su artículo 2 letra a), que por "electrónico" ha de entenderse:

> "*Aquella característica de la tecnología que tiene capacidades eléctricas, digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares".*

A nivel comparado, específicamente en la Unión Europea, la Directiva 2000/31/CE sobre Comercio Electrónico[17], por remisión de su artículo 2 letra a), a la Directiva 98/48/CE modificatoria de la Directiva 98/34/CE del Parlamento Europeo y del Consejo, concibe como "vía electrónica" o "medio electrónico" de la siguiente forma:

> *"Servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético".*

De manera más reciente, en España, la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, define medio electrónico en los siguientes términos:

> "*Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones, incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras"*.

[17] UNIÓN EUROPEA. Parlamento Europeo y del Consejo de la Unión Europea. 2000. Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). 8 de junio del 2000, [en línea] <https://eur-lex.europa.eu/eli/dir/2000/31/oj> [consulta: 21 mayo 2021]

Teniendo en cuenta lo anterior, para efectos de este trabajo, definiremos contratación electrónica como aquel tipo de contratación en el cual la voluntad de las partes se ha manifestado a través de medios electrónicos.

1.2.1 Características de la contratación electrónica.

1.2.1.1 El medio electrónico

La contratación electrónica supone un acto jurídico perfeccionado a través de medios electrónicos, concepto que no se restringe a una tecnología específica, sino que incluirá medios eléctricos, digitales, magnéticos, inalámbricos, ópticos, electromagnéticos u otros similares.

Así, la contratación electrónica tiene como elemento definitorio el uso de la tecnología, además del entorno en que se desarrolla: red informática local o global que permite su materialización y exteriorización en el mundo real. Esto implica que la contratación electrónica es un concepto amplio, que integra las diferentes tecnologías telemáticas que puedan ir empleándose en la contratación[18].

En atención al componente electrónico de la contratación, la identificación de las partes se llevará a cabo en formatos asimismo electrónicos, entre partes que no necesariamente se encuentran en el mismo lugar e incluso puede que no se conozcan. Esto conlleva un primer desafío, consistente en la determinación de la identidad de los contratantes, que ha devenido en la construcción del concepto de identidad digital.

[18] CAMACHO, S. 2019. Características de la contratación electrónica. En CURSO ONLINE Contratación y mercado digital. Aspectos legales y otras cuestiones de interés. Universitat Autònoma de Barcelona. [en línea] https://es.coursera.org/lecture/mercado-digital/la-contratacion-electronica-caracteristicas-XbT8E [consulta: 3 de marzo 2021].

1.2.1.2 La Identidad Digital

Según VANINETTI, la identidad digital se concibe como la expresión de todos aquellos rasgos con los que una persona se individualiza frente a los demás en un entorno digital o electrónico tanto en lo que se "es" en realidad, como en lo que "se quiere" o "pretende" ser[19].

La determinación de la identidad de los contratantes es un elemento central en la construcción de cualquier relación contractual, ya de que de ella dependerá que, luego, sea factible atribuir la manifestación de voluntad a una persona determinada y con ello permitir que se forme el consentimiento con efectos vinculantes.

El Reglamento Europeo (UE) Nº 910/2014 relativo a la identificación electrónica en el mercado interior y por la que se deroga la Directiva 1999/93/CE, en adelante El Reglamento Europeo de Identidad Digital, en su artículo 3 se ocupa largamente de definir los conceptos básicos para la construcción de la identidad digital o electrónica, a saber:

a. **Identificación electrónica**: *el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.*

b. **Medios de identificación electrónica**: *una unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea.*

c. **Sistema de identificación electrónica:** *régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica.*

[19] VANINETTI, H.A. 2016. Identidad, reputación y muerte digital. Revista de Derecho de Familia y de las personas- La ley (9): 237-241. P. 237.

d. **Datos de identificación de la persona**: *un conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica.*

Como podemos aprecia, la identidad digital se construye a partir de elementos internos o inmanentes a la persona y, elementos normativos y tecnológicos, que en conjunto permitirán a terceros poder nombrar de manera unívoca a la persona que se desenvuelve en un entorno digital[20].

Por cierto, la identidad digital, como toda información relativa a una persona natural, identificada o identificable, será dato personal y, por tanto, se le aplicará la normativa relativa a este tipo de datos.

1.2.1.3 El consentimiento electrónico

El consentimiento, de acuerdo con las reglas generales del derecho de los contratos y obligaciones, se formará por la concurrencia de la oferta en conjunto con la aceptación. Ahora bien, tratándose de un contrato electrónico, no basta que la oferta se manifieste a través de medios electrónicos, sino que se considera como esencial que el perfeccionamiento del contrato sea en formato electrónico, cuestión que únicamente ocurre con la aceptación de la oferta[21].

En Cambio, y a contrario sensu, se ha sostenido que cuando la oferta se ha realizado por medios no electrónicos, pero la aceptación sí se realiza a través de estos medios, se estaría en presencia de un contrato electrónico[22].

---

[20] DONOSO, L. 2019. Formalismo Jurídico: Autenticación y otras garantías, En: El Derecho de las TIC en Iberoamérica, Marcelo Bauzá Reilly, Fiadi, la ley Uruguay. pp. 720 - 721

[21]MORENO, J. 1999. Contratos Electrónicos. Madrid, Editorial Marcial Pons. 162p. p. 36.

[22] PINOCHET, R. 2009, cit. nota n. 12, p. 167.

1.2.1.4 Contratación entre ausentes

Adicionalmente, en la contratación electrónica las partes no están presentes, al menos físicamente, al momento de contratar, lo cual es factible gracias al medio electrónico.

Dada esta característica, es que por parte de la doctrina suele calificarse a la contratación electrónica como una contratación a distancia, en el sentido de que las partes, en un sentido espacial, no se encuentran físicamente presentes en forma simultánea. En este sentido, se dice que supone que el contrato ha sido concluido a través de un medio de comunicación a distancia, de cualquier naturaleza, que facilite el contacto entre las partes contratantes[23].

Esta es una característica que sin duda a raíz de la telepresencia se ha ido difuminando, dado que en la actualidad resulta perfectamente posible que las diferentes partes de un acto jurídico concurran virtualmente en un espacio determinado (por ejemplo, un sitio Web, plataforma de videoconferencias) para celebrar un contrato electrónico.

1.2.2 **Principios de la contratación electrónica.**

Desde luego, como se ha indicado, la contratación electrónica, al tratarse de un modo de contratación desarrollada por medios electrónicos, se encuentra permeada por los principios generales del derecho de los contratos: autonomía de la voluntad y buena fe.

Respecto de la autonomía de la voluntad, hay una distinción que conviene tener en cuenta respecto a la naturaleza de las partes del contrato. Evidentemente no será lo mismo un contrato entre comerciantes, que se regiría por las reglas de los contratos mercantiles, que los contratos de consumo, en que un particular contrata con una empresa.

---

[23] PANIZA, A. 2003. Contratación a distancia y defensa de los consumidores: Su regulación tras la reforma de la ley de Ordenación de Comercio Minorista y la ley de Servicio de la Sociedad de la Información y Comercio Electrónico. Granada, Editorial Comares. 410p. p. 101.

En el primer caso, se puede tratar de partes suficientemente sofisticadas, lo que permite pensar que se encuentran en condiciones de sopesar y controlar la plena vigencia del ejercicio del principio de autonomía de voluntad entre las partes, incluyendo, por ejemplo, el modo de resolver conflictos. En cambio, en el caso de una relación contractual de consumo, que es el que encajaría en el supuesto de hecho que motiva este estudio, habría que atender a normas específicas que limitan el accionar contractual de la empresa con miras a construir un entorno regulatorio que supla los desequilibrios entre la empresa y el consumidor[24].

A propósito de lo anterior la regulación del derecho de consumo, contenida en la Ley 19.496 permea de tal forma al comercio electrónico que sirve de límite y orientación para el libre ejercicio de la autonomía de la voluntad.

Ahora bien, atendiendo al componente tecnológico, propio de la contratación electrónica, hay principios especiales a atender en este formato de contratos.

1.2.2.1 Principio de inmaterialidad.

El contrato electrónico es celebrado en un entorno inmaterial, en el sentido tradicional, en el cual confluyen voluntades virtuales, no desconoce, por lo tanto, que los datos y documentos se almacenan en servidores y "ocupan espacio" de almacenamiento, sino que con ello se hace presente que este tipo de contratos se caracteriza porque se materializa a través de un conjunto de datos codificados o algoritmos matemáticos, o impulsos electromagnéticos, que no tienen manifestación en el mundo físico tangible[25]. La forma

---

[24] FELDSTEIN DE CÁRDENAS, S.L., RODRÍGUEZ, M.S., MEDINA, F.A., SCOTTI, L.B y KLEIN VIERA, L. 2012. El rol de la autonomía de la voluntad en los contratos celebrados por medios electrónicos. [en línea] Suplemento de Derecho Internacional Privado y de la Integración (71). <https://www.eldial.com/nuevo/lite-tcd-detalle.asp?id=6587&base=50&id_publicar=&fecha_publicar=26/10/2012&indice=doctrina&suple=Privado> [consulta 3 de marzo 2021].

[25] BIELLI, G. y ORDOÑEZ, C. 2020. Contratos Electrónicos: teoría general y cuestiones procesales. Santiago, Legal Publishing Chile. Tomo I. p.117.

electrónica del negocio jurídico debe entenderse admitida como cualquier otro modo válido de expresión de voluntad en virtud del principio de libertad de forma consagrado en diversas disposiciones del Código Civil y de la incipiente normativa especializada elaborada especialmente para la regulación del contrato electrónico[26].

1.2.2.2 Principio de equivalencia funcional.

Los contratos electrónicos tienen el mismo valor y la misma eficacia legal que aquellos otorgados en papel. Así, supone que este tipo de contratos gozan de los mismos efectos jurídicos, con prescindencia del soporte utilizado para la manifestación de la voluntad. Por tanto, tendrán eficacia legal para su ejecución tanto voluntaria como forzosa.

1.2.2.3 Principio de Neutralidad Tecnológica.

Este principio reconoce la fuerte carga del elemento tecnológico ínsito en el concepto de contrato electrónico y la rapidez con que evoluciona la tecnología y por tanto señala que la normativa no debiera reducirse e incluso debiera intentar no referirse a tecnologías específicas, sino a los efectos jurídicos que se requiere configurar a través de aquellas que se utilicen. Eso a fin de que la normativa no quede obsoleta rápidamente junto con la tecnología existente al tiempo de su entrada en vigor[27]. Así, este principio busca flexibilizar la rigidez propia del texto de las normas, sin que el mismo quede atado a una tecnología específica, evitando el riesgo de desactualización[28].

---

[26] BIELLI, G. y ORDOÑEZ, C. 2020. cit. nota n. 25, p. 118.

[27] PINOCHET, R. 2009, cit. nota n. 12, p. 118.

[28] BIELLI, G. y ORDOÑEZ, C. 2020. cit. nota n. 25, p. 119.

El Servicio Nacional del Consumidor, por su parte, en Circular Interpretativa de marzo de 2019[29], buscó dar a conocer a los proveedores de comercio electrónico los principios orientadores de la contratación en general, haciendo especial mención a principios generales del derecho de los contratos, así como, también a principios especiales de la contratación electrónica.

En este texto, tomando como referente el Código de Buenas Prácticas para el Comercio Electrónico de la Cámara de Comercio de Santiago[30], se han definido los siguientes principios:

1.2.2.4 Principio de protección eficaz e integral.

Los proveedores deben asegurar al consumidor, durante todo el *íter* contractual, una protección eficaz e íntegra, cuyo estándar no puede ser inferior al nivel de protección que se otorga en otras formas de comercialización, cualquiera sea el dispositivo tecnológico por el cual se lleve a cabo. Asimismo, los proveedores deben tener especial consideración en cuando a la protección de niños y consumidores vulnerables, por lo cual deben tener en cuenta los conocimientos de la economía de la información y la economía conductual, evitando los riesgos que a aquel grupo pudiera afectarle.

1.2.2.5 Principio de transparencia en la información.

Todo proveedor deberá otorgar a los consumidores información visible y veraz respecto de la identidad del proveedor y sus datos de contacto nacional, características de los productos y/o servicios que ofrece y comercializa, proceso de transacción electrónica, sus medios,

---

[29] SERVICIO NACIONAL DEL CONSUMIDOR. 2019. Resolución Exenta Nº 0184 del 21 de marzo 2019, Circular Interpretativa sobre buenas prácticas en Comercio Electrónico. [en línea] <https://www.sernac.cl/portal/617/articles-9195_archivo_01.pdf> [consulta 4 de marzo 2021].

[30] CÁMARA DE COMERCIO DE SANTIAGO. Código de Buenas Prácticas para el Comercio Electrónico, [en línea] <https://www.ccs.cl/wp-content/uploads/2020/01/codigo_buenas_practicas.pdf> [consulta 19 de julio 2021].

alcances, seguridad, resguardos, entre otros aspectos que los consumidores requieran tomar conocimiento, evitando el ocultamiento o entrega de información confusa.

1.2.2.6 Principio de legalidad.

El ofrecimiento y contratación de bienes o servicios, así como la atención de post venta deben respetar la normativa legal vigente en la jurisdicción aplicable, cualquiera sea el medio a través del cual se desarrolle.

1.2.2.7 Principio del consentimiento informado.

El consumidor, al dar su consentimiento, debe poder tener un conocimiento adecuado de la naturaleza del contrato celebrado, el bien o servicio sobre el cual recae, sus obligaciones y derechos. Para que ello sea posible, los proveedores electrónicos deberán informar en detalle las condiciones generales y particulares de contratación.

1.2.2.8 Principio de la fuerza obligatoria del contrato.

Los proveedores electrónicos que hubieren aceptado una orden deberán dar fiel y oportuno cumplimiento al contrato celebrado, empleando todos los medios a su alcance para ello, no siendo justificación razonable para incumplir un contrato la falta de stock del producto ofrecido o que la prestación efectiva del servicio se encuentre radicada en una tercera persona, salvo que tales eventualidades hayan sido advertidas al consumidor por el oferente antes de la celebración del contrato.

1.2.2.9 Principio de profesionalidad.

Los proveedores electrónicos deberán observar una conducta profesional en el ejercicio del comercio electrónico, ofreciendo bienes y servicios de calidad y de los que efectivamente dispongan y estén en condiciones de realizar su prestación o intermediarlo de manera oportuna.

1.2.2.10 Principio de buena fe.

Los proveedores deben actuar de un modo recto y transparente para con los consumidores, evitando de esta manera, todas aquellas conductas que tergiversen u oculten maliciosamente o con intención de confundir al consumidor, en cuanto a la información de las características básicas de los bienes y/o servicios que se ofrecen, contener términos y condiciones ambiguos que no respeten y/o restrinjan el marco regulatorio de los cuerpos legales de protección del consumidor propios de la legislación vigente.

1.3 Formación del consentimiento.

La contratación electrónica se le aplican las mismas reglas generales propias del derecho de los contratos. Así, en los términos del artículo 1445 del Código Civil, para que una persona se obligue a otra por un acto o declaración de voluntad será necesario que consienta en dicho acto o declaración y que dicho consentimiento no adolezca de vicio[31].

La Corte Suprema ha sostenido que, para que el acuerdo de voluntades produzca el efecto jurídico de crear una o más obligaciones:

> *"Es necesario que culmine un proceso tendiente a la formación del consentimiento, mediante el concierto de dos actos jurídicos unilaterales e independientes, derivados uno de aquel que toma la iniciativa y le propone un negocio a otro, y este, que es aquel al cual va dirigida la oferta, que acepta la proposición, con su consentimiento*[32]*".*

Consecuentemente, para la formación del consentimiento electrónico, al igual que las reglas de derecho común, deberá darse la concurrencia de la oferta y aceptación.

---

[31] PINOCHET, R. 2009, cit. nota n. 12, p. 146.

[32] CORTE SUPREMA, Causa nº 3362/2006 (Casación). Resolución nº 9336 de 16 de Abril de 2008.

1.3.1 De la Oferta.

La oferta no se encuentra especialmente definida en el Código Civil ni en el Código de Comercio Chileno, sin embargo, la doctrina se ha encargado de conceptualizarla.

Así, se puede definir la oferta como aquella declaración de voluntad cuyo fin es la formación del consentimiento para un negocio jurídico determinado, pretendiendo, para tal propósito, conseguir la aceptación de las condiciones expresadas por parte de los sujetos de derecho a quienes la misma oferta se dirige[33].

Doctrinariamente los requisitos que debe satisfacer una oferta son, al menos, los siguientes:

a. **Debe ser seria**. Supone que efectivamente la intención del oferente sea el desarrollo de un vínculo jurídico a partir de la celebración del negocio jurídico.
b. **Debe ser inequívoca.** Esto implica que no debe dar lugar a interpretaciones distintas de las expresadas.
c. **Debe ser completa o determinada.** Supone que contenga todos los elementos esenciales para la aceptación del negocio.
d. **Debe ser, en principio, libre de forma**. Esto implica que la manifestación de la voluntad pueda ser hecha por cualquier medio.

1.3.2 De la aceptación.

La aceptación, como segundo elemento clave para la formación del consentimiento, puede definirse como aquella declaración de voluntad realizada por el destinatario de la oferta por medio de la cual expresa su conformidad con todos los aspectos de la misma y, consecuentemente, manifiesta su voluntad de llevar a cabo un negocio jurídico[34].

---

[33] PINOCHET, R. 2009, cit. nota n. 12, p. 147.

[34] PINOCHET, R. 2009, cit. nota n. 12, p. 169

En tal sentido, la aceptación, para ser tal, ha de coincidir con los términos en que ha sido planteada la oferta.

La doctrina, por su parte, ha definido como requisitos esenciales de la aceptación los siguientes:

a. **Debe ser pura y simple**, en el sentido de no condicionada y coincidente.
b. **Debe ser seria y definitiva**. Debe ir acompañada de una voluntad de contratar.
c. **Debe exteriorizarse a través de cualquier medio adecuado**. En aplicación del principio de libertad de forma no es necesario que deba manifestarse exclusivamente por el mismo medio utilizado para la formulación de la oferta.
d. **Debe ser tempestiva**. Esto implica que la aceptación debe darse dentro del período en que la oferta se encuentra vigente, es decir, antes de que haya caducado o bien, que por cumplimiento del plazo o condición ya no esté vigente.

De acuerdo con lo anterior, y en aplicación de los principios generales del derecho de los contratos a la contratación electrónica, se advierte que no hay inconvenientes para que la voluntad sea manifestada por medios electrónicos. Es más, tal como señaláramos anteriormente, es la forma que debe tomar para estar en presencia de un contrato electrónico.

La Ley 19.496 contempla una regla especial sobre la aceptación en la formación del consentimiento en el contexto de contratación electrónica en su artículo 12 A:

> *"En los contratos celebrados por medios electrónicos, y aquellos en que se aceptare una oferta realizada a través de catálogos, avisos o cualquiera otra forma de comunicación a distancia, el consentimiento no se entenderá formado si el consumidor no ha tenido previamente un acceso claro, comprensible e inequívoco de las condiciones generales del mismo y la posibilidad de almacenarlos o imprimirlos".*

Consecuentemente, dado que el consentimiento se tendrá por no formado en caso de que el consumidor no haya tenido acceso previo a las condiciones generales de contratación, la sanción será que se entenderá como nulo, de nulidad absoluta, al no configurarse el elemento básico para contar con un contrato legalmente celebrado: el consentimiento.

1.3.3 Momento en que se forma el consentimiento electrónico.

En derecho comparado, el artículo 1258 del Código Civil español indica expresamente que[35]:

> "*Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan"*.

En el caso del Código Civil chileno tal principio no se encuentra formulado en palabras tan claras, pero se desprende inequívocamente de su artículo 1445 Nº 2 al establecer lo siguiente[36]:

> *"Para que una persona se obligue a otra por un acto o declaración de voluntad es necesario: […] 2. que consienta en dicho acto o declaración y su consentimiento no adolezca de vicio".*

Consecuentemente y de acuerdo con este artículo los actos jurídicos formales o solemnes constituyen la excepción, de modo que para estar frente a ellos se requiere de texto legal expreso.

El elemento espiritual como factor crítico en la formación del consentimiento se construyó en base a la hipótesis contractual más simple, esto es, que las partes se encuentran presentes, que la oferta es completa y la aceptación pura y simple, lo que conlleva como lógica consecuencia que el consentimiento se ha de formar en el mismo instante en que se

---

[35] PINOCHET, R. 2009, cit. n.12, p. 219.

[36] PINOCHET, R. 2009, cit. n.12, p. 219.

ha producido la aceptación, así como en el lugar en que ésta se ha efectuado, circunstancias que, además, en tal caso coincidirán con el lugar de emisión de la oferta[37].

Una materia tan estudiada en doctrina como la relativa al momento y lugar del perfeccionamiento del contrato, ha adquirido un nuevo interés, pues se ha constatado que las nuevas tecnologías de la información tienen la capacidad de alterar algunos de los elementos usados tradicionalmente para el análisis del proceso de formación del contrato. Tal es el caso de la nueva dimensión que han adquirido en Internet nociones tan importantes como las de tiempo y espacio, aspectos que necesariamente han llevado a la revisión de las soluciones que hasta antes de la aparición de las nuevas tecnologías se daban por satisfactorias[38].

A propósito de estas circunstancias, repasaremos las distintas teorías que se ocupan del momento en que se forma el consentimiento:

a. **Teoría de la declaración:** Esta teoría surge de la idea mayoritaria en el ordenamiento jurídico chileno acerca de la aplicabilidad de las normas del Código de Comercio en materia civil, de conformidad al artículo 101 del mismo cuerpo legal, el consentimiento ha de entenderse formado cuando se ha producido la aceptación[39].
b. **Teoría del conocimiento:** En contraposición a la teoría de la declaración, en derecho comparado observamos en el ordenamiento jurídico español, que el artículo 1262 de su Código Civil dispone que, *la aceptación hecha por carta no obliga al que hizo la oferta sino desde que llegó a su conocimiento. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta*[40].

---

[37] PINOCHET, R. 2009, cit. n.12, p. 219.

[38] PINOCHET, R. 2009, cit. nota n. 12, p. 219.

[39] PINOCHET, R. 2009, cit. nota n. 12, p. 220-221

[40] PINOCHET, R. 2009, cit. nota n. 12, p. 221

c. **Teoría de la Recepción:** De acuerdo con esta teoría, se exige únicamente que la aceptación haya sido recibida, es decir, que haya llegado al conocimiento del oferente[41].
d. **Teoría de la Emisión:** El consentimiento se entenderá perfeccionado en el mismo momento en que se emite la aceptación ya que éste será el instante en que el oferente conocerá la aceptación, coincidiendo, consecuentemente con las diferentes fases de la aceptación[42].

Así como se discute respecto a si la formación del consentimiento se produce en el momento en que se envía la aceptación o bien cuando la recibe el oferente en el mundo real, en que se presuponen ciertos plazos para que la respuesta que se emite llegue a destino, en el mundo virtual, a pesar de la simultaneidad que puede darse en estas comunicaciones, existe también la falta de certeza de que la respuesta llegue a puerto y, si llega, que el destinatario la abra y lea.

Sin embargo, todos los problemas técnicos que infunden estas dudas son similares a los que ocurrían antiguamente si fallaba el correo o el sistema de telegramas o los mensajeros. En consecuencia, el problema de fondo sigue siendo el mismo: ¿El consentimiento se forma cuando se emite la respuesta -cuestión que el oferente ignora por un tiempo- o cuando ésta se recibe por el destinatario?

Nuestra legislación adhiere a la postura de la aceptación o declaración de la respuesta, lo cual se desprende de la lectura de los artículos 97 y 98 del Código de Comercio, los cuales se refieren a ofertas verbales y a las ofertas escritas, que en la actualidad podrían definirse como ofertas entre personas presentes que deben dar su respuesta inmediata, o ausentes, en cuyo caso, la oferta se realiza por escrito y existe un plazo para su aceptación, ya que

---

[41] PINOCHET, R. 2009, cit. nota n. 12, p. 223

[42] PINOCHET, R. 2009, cit. nota n. 12, p. 227

ésta no puede estar vigente permanentemente. Ahora bien, el medio electrónico permite hacer ofertas entre ausentes, pero con comunicaciones simultáneas, lo que de ninguna manera podría considerarse como una propuesta verbal, ya que éstas se realizan por medios electrónicos que, para todos los efectos, como lo establece la Ley 19.799, se tendrán por escritas[43].

Para la resolución del problema relativo a la determinación del momento de perfeccionamiento del negocio jurídico electrónico podemos considerar, en primer lugar, la existencia de normas especiales sobre la materia especialmente en Derecho Comparado, que contrasta con la ausencia de regulación en el nuestro. Es así como la Directiva 2000/31/CE sobre Comercio Electrónico, en su artículo 2 letra a) entiende por servicios de la sociedad de la información aquellos servicios en el sentido del apartado 2, del artículo 1, de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE, define, a su vez, a los servicios de la sociedad de la información como:

> "*Todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios*".

El criterio general que parece prevalecer en la doctrina respecto a nuevas tecnologías aplicadas al derecho de los contratos es que, no importando la distancia física entre las partes, la contratación electrónica, en principio, en atención a la rapidez con que se perfecciona este tipo de contrato, debiese asimilarse a la modalidad de contratación entre presentes.

En sintonía con lo anterior, LORENZETTI ha sostenido que la definición de las relaciones contractuales presenciales y negocios jurídicos entre ausentes es un asunto de naturaleza técnico-jurídica y no depende de la distancia o ubicación física de las partes, en el sentido

[43] SILVA, P. 2003, cit. nota n. 11, p. 123 y 124.

que lo determinante es la inmediatez entre el envío y la recepción de la propuesta, así como con la aceptación de la misma, lo cual también puede estar sujeto a un plazo fijado por las partes o ser consecuencia de la naturaleza misma de la negociación planteada[44].

Así las cosas, resulta que la determinación del momento de perfeccionamiento del contrato electrónico no presentará problemas, al menos en la mayoría de las hipótesis de contratación electrónica.

Siguiendo las reglas generales formuladas para la contratación entre presentes, el consentimiento se entenderá perfeccionado en el mismo momento en que se emita la aceptación ya que éste será el instante en que conocerá la aceptación el oferente, coincidiendo, en consecuencia, las diferentes fases en que puede encontrarse la aceptación: etapas de declaración, emisión, recepción y conocimiento[45].

Al intentar determinar el momento de perfección del consentimiento electrónico a través del empleo de los principios tradicionales, puede afirmarse que la gran mayoría, por no decir la totalidad de los medios electrónicos de transmisión de la voluntad, pueden ser considerados como una contratación entre presentes, por constituir procesos inmediatos de formación del consentimiento en los que no es posible apreciar espacios de tiempo jurídicamente relevantes que aconsejan aplicar a tales procesos negociales las reglas clásicas de contratación entre personas distantes, ello aun cuando las partes en la contratación electrónica pueden encontrarse a miles de kilómetros de distancia, circunstancia que evidencia la incongruencia de la concepción tradicional de las categorías tiempo y espacio cuando son aplicadas a la realidad conformada por la formación del consentimiento a través de las nuevas tecnologías de la información.

---

[44] LORENZETTI, R.L. (dir). 2015. Código Civil y Comercial de la Nación, Comentado. Santa Fe, Rubinzal-Culzoni, tomo V, p. 627

[45] PINOCHET, R. 2009, cit. nota n. 12, p. 225

En tal sentido, se puede afirmar que hoy es prácticamente insignificante el tiempo que media entre la emisión y la recepción de una comunicación electrónica anulando, en la práctica, el que era el elemento determinante en el pasado para discriminar las diversas consecuencias que podía producir el optar por las teorías de la declaración, de la emisión, recepción o consentimiento a las que se hizo mención. Así, se afirmaba que la teoría de la emisión era aconsejable en el ámbito del comercio, pues su rapidez era compatible con la celeridad que exigen las transacciones comerciales, aspecto que hoy es irrelevante por cuanto, salvo excepciones, la recepción del mensaje electrónico se produce prácticamente en el mismo instante que en el de su emisión.

No obstante, puedan considerarse como anacrónicas las reglas chilenas aplicables a la formación del consentimiento, en definitiva, en el caso de la formación del consentimiento electrónico, la situación no tiene mayor efecto[46]. De acuerdo con MATEU DE ROS, las hipótesis de formación del consentimiento electrónico, más bien, debieran encuadrarse dentro de lo que tradicionalmente se ha conocido como la contratación entre presentes, pues se considera a la contratación electrónica como una especie de contratación entre presentes, de manera virtual, pero una presencia al fin. Toda vez que no hay ausencia ni distancia, sino una forma distinta de presencia, tan auténtica, inmediata e instantánea, y, a menudo, mucho más libre y espontánea[47].

A nivel comparado, concretamente en el ámbito europeo, el artículo 11 de la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior, del 18 de noviembre de 1998, llevaba por título “Momento de celebración del contrato”.

---

[46] PINOCHET, R. 2009, cit. nota n. 12, p. 234 - 236

[47] MATEU DE ROS, R. 2000. El Consentimiento y Proceso de Contratación Electrónica. En: MATEU DE ROS, R y CONDOYA J.M. Derecho de Internet: Contratación Electrónica y Firma Digital. Navarra. Aranzadi. pp. 29 - 84 p.60.

Este artículo 11 inicial se refería a un proceso contractual en el que el destinatario del servicio únicamente pudiera elegir entre pulsar "si" o "no" para aceptar o rechazar una oferta. Así, en concreto, este artículo establecía que, cuando el destinatario de un servicio manifestase su consentimiento utilizando medios tecnológicos, el contrato quedaría celebrado cuando el destinatario del servicio:

> *"Haya recibido por vía electrónica una notificación del prestador de servicios acusando recibo de la aceptación del servicio, y haya sido recibido y que la confirmación esté hecha cuando las partes a las que vayan dirigidos puedan tener acceso a ellos"*.

Tanto el acuse de recibo del prestador de servicios como la confirmación del destinatario debían enviarse lo antes posible. De acuerdo con todo ello, para la conclusión de los contratos electrónicos se establecía un sistema de cuatro pasos: oferta, aceptación, acuse de recibo de la aceptación y confirmación de la recepción del acuse de recibo.

Posteriormente el título de este artículo fue modificado por el de "realización de un pedido", con ello se buscó que la Directiva no se inmiscuyera en cuestiones de conclusión del contrato en atención a los sistemas jurídicos propios de las diversas legislaciones nacionales. Así, la posición común aprobada por el Consejo afirmaba lo siguiente:

> "*Este artículo ya no determina el momento en que el contrato quedará celebrado, sino que sólo aborda el pedido, el acuse de recibo y los medios para corregir los errores de introducción de datos. El título se ha modificado en consecuencia"*.

Entonces, se abandonó la primera redacción en que sí se establecía el momento de perfección del contrato condicionándolo a la notificación del prestador de servicios acusando recibo de la aceptación y se entendía recibido cuando la otra parte a la que iba dirigido podía tener acceso a él, para referirse solamente a la realización de un pedido. La

recepción del acuse de recibo ya no es el elemento decisivo de la perfección del contrato, por lo tanto, no afecta al momento de perfección[48].

1.3.4 Lugar de formación del consentimiento.

Respecto del momento de formación del consentimiento, como se indicó en el apartado anterior, se tiende a asimilar a un contrato entre presentes. Sin embargo, tal asimilación no es del todo pacífica cuando se quiere definir el lugar de formación del consentimiento.

¿Dónde se forma el consentimiento en los contratos electrónicos? La respuesta lógica sería el lugar en que se emite la aceptación, donde se encuentra el dispositivo a través del cual se ha emitido la respuesta, entonces, el domicilio o lugar desde donde se encuentra el aceptante, si se considera que es el consumidor quien acepta.

Si se acepta la teoría tradicional, en cambio, será el domicilio del vendedor, quien acepta la oferta que el comprador hace al adquirir. Esta es la opción que adopta el Código Civil Español en su artículo 1262.2. La ventaja de esta segunda posición es la certeza que tiene el comerciante, y el sistema jurídico, respecto del lugar que fijará la legislación aplicable, a diferencia de la posición más abierta que da al consumidor las ventajas[49].

Sin embargo, no debemos olvidar que la determinación del lugar en que se entiende formado el consentimiento lleva aparejada la determinación de otros elementos clave del negocio jurídico como la fijación del lugar de la ejecución de las obligaciones, la determinación del juez competente para la solución de conflictos, así como la fijación de la ley aplicable en aquellos casos que concurra más de una legislación nacional posiblemente aplicable al contrato[50].

---

[48] PANIZA, A. 2003, cit. nota n. 23, pp. 252 – 254

[49] SILVA, P. 2003, cit. nota n. 11, p. 124.

[50] PINOCHET, R. 2009, cit. nota n. 12, p. 239.

En el caso chileno, a propósito del lugar de la formación del consentimiento, el artículo 104 del Código de Comercio dispone lo siguiente:

> *"Residiendo los interesados en distintos lugares, se entenderá celebrado el contrato, para todos sus efectos legales, en el de la residencia del que hubiere aceptado la propuesta primitiva o la propuesta modificada".*

En este caso, se privilegia los mismos beneficios señalados antes, pero en este caso en favor del aceptante.

Sin perjuicio de lo anterior, PINOCHET[51] estima que la doctrina actual parece uniformarse en torno a la aceptación de la autonomía conflictual en materia contractual. Esto supone que el contrato se regirá por la legislación que las mismas partes hubieren definido.

En caso de no haberse definido por las partes, el contrato se regirá por la ley del lugar en que hubiere sido celebrado.

En materia de consumo, sin embargo, como sería el caso de la contratación electrónica de servicios bancarios y financieros que motiva este trabajo, el lugar de celebración del contrato estará determinado por las reglas propias del derecho del consumidor. Al respecto, y atendido lo dispuesto en el artículo 4 de la Ley 19.496, según el cual *los derechos establecidos por la presente ley son irrenunciables anticipadamente por los consumidores,* necesariamente habrá que estar a lo dispuesto por la misma ley en cuanto al lugar de celebración del contrato.

A propósito de lo anterior, el artículo 50 A de la Ley 19.496 se hace cargo resolver el principal conflicto que acarrea la definición del lugar de celebración del contrato: fijar el tribunal competente en los siguientes términos:

---

[51] PINOCHET, R. 2009, cit. nota n. 12, p. 249.

> *"Los jueces de policía local conocerán de todas las acciones que emanan de esta ley, siendo competente aquel que corresponda a la comuna en que se hubiera celebrado el contrato respectivo, se hubiere cometido la infracción o dado inicio a su ejecución a elección del actor".*

Hasta antes del año 2018 en que se reformó la Ley 19.496, se indicaba especialmente para el caso de contratos celebrados por medios electrónicos que:

> *"En el caso en que no sea posible determinar lo señalado en el inciso anterior, será juez competente aquel de la comuna en que resida el consumidor".*

Frente a la duda respecto de si deberá considerarse la ubicación del dispositivo a través del cual se manifiesta el consentimiento, PINOCHET, estima que no debiera considerarse como lugar de la aceptación electrónica el que corresponda al del punto donde se encuentra ubicado dicho dispositivo, sino que más bien debiera resolverse la determinación del lugar de formación del consentimiento echando mano a las reglas generales de formación del consentimiento, es decir, considerar el lugar desde el cual se ha llevado a cabo la aceptación como aquel en que se ha exteriorizado la voluntad con el propósito serio de obligarse.

Conforme a esta prevención, será aconsejable distinguir en cada caso la función concreta que ha cumplido el computador. Si ha sido el medio utilizado para exteriorizar la voluntad podrá ser utilizado en la determinación del lugar de la oferta o la aceptación, en caso contrario, esto es, que la voluntad haya sido adoptada y exteriorizada por otro medio, no tendrá relevancia para estos efectos.

Teniendo en cuenta que una de las principales funciones de la fijación del lugar de perfeccionamiento del contrato es asignar competencia a los tribunales para conocer de las cuestiones que puedan derivarse del contrato, en materia de contratos de consumo se ha previsto excepcionarlos de las reglas generales, en pos de otorgar competencia a tribunales accesibles para el consumidor.

En la experiencia comparada, de acuerdo con PANIZA, los contratos electrónicos son coincidentes con el caso de los dispositivos automáticos, entendiéndose ambos celebrados, en el caso en que alguna de las partes sea un consumidor, en el lugar en que éste tenga su residencia habitual.

En cambio, cuando se trate de un contrato entre empresarios, será el lugar en que se encuentra establecido el prestador de los servicios[52].

1.4 Regulación de los contratos de crédito de consumo celebrados por medios electrónicos.

Como señalamos antes, el régimen regulatorio de los contratos de crédito de consumo se encuentra contenido en la Ley 19.496 luego de la modificación llevada a cabo por la ley 20.555 de diciembre del 2011, así como también el reglamento especial sobre la materia contenido en el Decreto 43 de julio de 2013 sobre información al consumidor de créditos de consumo. Estas normas no distinguen entre créditos otorgados a través de medios tradicionales o mediante contratación electrónica por lo que son de aplicación al objeto de nuestra investigación.

A continuación, nos referiremos a los aspectos regulados en esta normativa.

1.4.1 La regulación en la Ley 19.496.

En la Ley 19.496, en el contexto de la ley conocida como "SERNAC financiero" conviene prestar atención al artículo 17 B que define el contenido mínimo que debe especificarse en este tipo de contratos, consagrando el principio de transparencia.

De acuerdo con DE LA MAZA, esta ley, en el convencimiento de que la mejor forma de proteger a los consumidores es mejorando la información a la que pueden acceder los

[52] PANIZA, A. 2003, cit. nota n. 23, p. 272

mismos para la toma de sus decisiones de consumo, busca que las empresas que promocionan y dan a conocer sus productos por Internet informen acerca de las características esenciales de los mismos, facilitando el acceso a la información de los consumidores[53]. Veamos lo que dispone esta norma:

> *"Artículo 17 B.- Los contratos de adhesión de servicios crediticios, de seguros y, en general, de cualquier producto financiero, elaborados por bancos e instituciones financieras o por sociedades de apoyo a su giro, establecimientos comerciales, compañías de seguros, cajas de compensación, cooperativas de ahorro y crédito, y toda persona natural o jurídica proveedora de dichos servicios o productos, deberán especificar como mínimo, con el objeto de promover su simplicidad y transparencia, lo siguiente:*
>
> *a) Un desglose pormenorizado de todos los cargos, comisiones, costos y tarifas que expliquen el valor efectivo de los servicios prestados, incluso aquellos cargos, comisiones, costos y tarifas asociados que no forman parte directamente del precio o que corresponden a otros productos contratados simultáneamente y, en su caso, las exenciones de cobro que correspondan a promociones o incentivos por uso de los servicios y productos financieros.*
>
> *b) Las causales que darán lugar al término anticipado del contrato por parte del prestador, el plazo razonable en que se hará efectivo dicho término y el medio por el cual se comunicará al consumidor.*
>
> *c) La duración del contrato o su carácter de indefinido o renovable automáticamente, las causales, si las hubiere, que pudieren dar lugar a su término anticipado por la*

[53] DE LA MAZA, I. 2013. Artículo 17 B (Letras A, B, C, D, E, F). En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile. pp. 376 - 398. p. 385.

sola voluntad del consumidor, con sus respectivos plazos de aviso previo y cualquier costo por término o pago anticipado total o parcial que ello le represente.

d) Sin perjuicio de lo establecido en el inciso primero del artículo 17 H, en el caso de que se contraten varios productos o servicios simultáneamente, o que el producto o servicio principal conlleve la contratación de otros productos o servicios conexos, deberá insertarse un anexo en que se identifiquen cada uno de los productos o servicios, estipulándose claramente cuáles son obligatorios por ley y cuáles voluntarios, debiendo ser aprobados expresa y separadamente cada uno de dichos productos y servicios conexos por el consumidor mediante su firma en el mismo.

e) Si la institución cuenta con un servicio de atención al cliente que atienda las consultas y reclamos de los consumidores y señalar en un anexo los requisitos y procedimientos para acceder a dichos servicios.

f) Si el contrato cuenta o no con sello SERNAC vigente conforme a lo establecido en el artículo 55 de esta ley.

g) La existencia de mandatos otorgados en virtud del contrato o a consecuencia de éste, sus finalidades y los mecanismos mediante los cuales se rendirá cuenta de su gestión al consumidor. Se prohíben los mandatos en blanco y los que no admitan su revocación por el consumidor.

Los contratos que consideren cargos, comisiones, costos o tarifas por uso, mantención u otros fines deberán especificar claramente sus montos, periodicidad y mecanismos de reajuste. Estos últimos deberán basarse siempre en condiciones objetivas que no dependan del solo criterio del proveedor y que sean directamente verificables por el consumidor. De cualquier forma, los valores aplicables deberán ser comunicados al consumidor con treinta días hábiles de anticipación, al menos, respecto de su entrada en vigencia".

1.4.2 Reglamento del “SERNAC Financiero”.

El Reglamento, contenido en el Decreto Supremo 43, de 2013 del Ministerio de Economía, sobre información al consumidor de créditos de consumo, si bien se remite al contenido de la ley, repitiendo algunos preceptos en el mismo sentido, contiene algunas normas que complementan las disposiciones de la Ley 19.496 respecto de la información que debe suministrar el proveedor para la contratación de créditos de consumo a las que conviene prestar atención de cara a definir el régimen regulatorio de este tipo de contratos.

> *“Artículo 9º.- Obligación de Información. El Proveedor deberá otorgar a los Consumidores señalados en los números 2) y 3) del artículo 2°, toda la información que se indica a continuación:*
>
> *1) Información básica comercial, esto es, aquellos datos, instructivos, antecedentes o indicaciones que el Proveedor debe suministrar obligatoriamente al público Consumidor, en cumplimiento de una norma jurídica.*
>
> *Esta información deberá ser suministrada al público por medios que aseguren un acceso claro, expedito y oportuno.*
>
> *2) Información veraz y oportuna sobre los Créditos de Consumo ofrecidos, su tasa de interés, condiciones objetivas de contratación de tales créditos y otras características relevantes de los mismos que considere el Proveedor o que requiera el Consumidor.*
>
> *3) Información del costo total del Crédito de Consumo, lo que comprende conocer la Carga Anual Equivalente y, en su caso, ser informado por escrito de las razones del rechazo a la contratación del Crédito de Consumo, las que deberán fundarse en condiciones objetivas.*
>
> *4) Información sobre las condiciones objetivas que el Proveedor establece previa y públicamente para acceder al Crédito de Consumo.*

5) Información sobre la liquidación total del Crédito de Consumo, a su solo requerimiento.

La liquidación total del crédito deberá contener el Saldo del Crédito, el Costo Total del Pago Anticipado o Prepago que debe pagar el Consumidor para extinguir anticipadamente o prepagar el Crédito de Consumo y la Comisión por Pago Anticipado o Prepago, si la hubiere.

El Proveedor no podrá negar o condicionar la emisión o entrega de la liquidación total del Crédito de Consumo por causa alguna.

El contrato deberá informar al Consumidor que para la extinción del Crédito de Consumo requiere pagar, si se hubiere pactado, los intereses proyectados que se hayan devengado hasta la fecha en que realice el pago del Saldo del Crédito y la Comisión por Pago Anticipado o Prepago, de acuerdo con lo dispuesto en el mismo contrato y en conformidad a la Ley 18.010".

"Artículo 10.- Información Básica Comercial en Créditos de Consumo. Para los efectos de lo establecido en el número 1) del artículo anterior, se entenderá que constituye información básica comercial en los Créditos de Consumo, cada uno de los elementos que el Proveedor debe considerar dentro de la Carga Anual Equivalente; las alternativas de Monto Total del Crédito de Consumo si los hubiere y el número de cuotas a pagar con su periodicidad; la tasa de Intereses Moratorios; el sistema de cálculo y monto de los Gastos de Cobranza extrajudicial en caso de impagos, incluidos los honorarios que correspondan; y las modalidades y procedimientos de cobranza extrajudicial.

Entre las modalidades y procedimientos de cobranza extrajudicial, se indicará si el Proveedor la realizará directamente o por medio de terceros y, en este último caso, se identificarán a las empresas encargadas; los horarios en que se efectuará, y la

eventual información que sobre ella podrá proporcionarse a terceros de acuerdo con la Ley 19.628.

Asimismo, se informará que las modalidades y procedimientos de cobranza extrajudicial pueden variar anualmente, en caso de transacciones cuyo plazo de pago exceda un año, en términos que no resulte más gravoso ni oneroso para los Consumidores ni se discrimine entre ellos, y siempre que tales variaciones se avisen con una anticipación mínima de dos periodos de pago".

Además, cabe advertir, el Decreto 43, en su artículo 11 establece las especificaciones mínimas que ha de contener un Contrato de Crédito de Consumo en los mismos términos del artículo 17 B, sin embargo, y en complemento de dicha norma, añade los siguientes numerales 8 y 9:

"Artículo 11.- Especificaciones Mínimas de los Contratos. Los contratos de Crédito de Consumo deberán especificar como mínimo, con el objeto de promover su simplicidad y transparencia, lo siguiente:

[…]

8) Si el contrato se refiere a un Crédito de Consumo con tasa de interés variable, deberá especificarse en él claramente sus montos, periodicidad y mecanismos de reajuste.

Los mecanismos de reajuste que podrá incluir el Proveedor en el contrato deberán ser objetivos y directamente verificables por el Consumidor, tales como las variaciones que experimenten el índice de precios al consumidor o IPC; la unidad de fomento o UF; el índice valor promedio o IVP; el valor de los tipos de cambio determinados en conformidad a la legislación especial vigente; y el o los índices que reemplacen en el futuro a el o los índices señalados precedentemente, determinados

por una ley especial o por un organismo competente conforme a sus funciones y atribuciones legales.

El Proveedor deberá comunicar al Consumidor los reajustes que corresponda aplicar en la oportunidad prevista en el contrato de Crédito de Consumo con, a lo menos, treinta días hábiles de anticipación a su entrada en vigencia.

Asimismo, el Proveedor deberá comunicar al Consumidor el término de cualquier oferta, promoción o descuento del Crédito de Consumo contratado con, a lo menos, treinta días hábiles de anticipación a la fecha en que se aplicarán los nuevos valores sin la oferta, promoción o descuento.

9) La tasa de Interés Moratorio en caso de incumplimiento y el sistema de cálculo de los gastos que genere la cobranza extrajudicial de los Créditos de Consumo impagos, incluidos los honorarios que correspondan, y las modalidades y procedimientos de dicha cobranza.

Se informará, asimismo, que tales modalidades y procedimientos de cobranza extrajudicial pueden ser cambiados anualmente en el caso de Créditos de Consumo cuyo plazo de pago exceda de un año, en términos de que no resulte más gravoso ni oneroso para los Consumidores ni se discrimine entre ellos, y siempre que de tales cambios se avise con una anticipación mínima de dos períodos de pago.

Las actuaciones de cobranza extrajudicial no podrán considerar el envío al Consumidor de documentos que aparenten ser escritos judiciales; comunicaciones a terceros ajenos a la obligación en las que se dé cuenta de la morosidad; visitas o llamados telefónicos a la morada del deudor durante días y horas que no sean los que declara hábiles el artículo 59 del Código de Procedimiento Civil, y, en general, conductas que afecten la privacidad del hogar, la convivencia normal de sus miembros ni la situación laboral del deudor".

1.4.3 Sanción por el incumplimiento de las normas legales y reglamentarias.

Los deberes de información contenidos en el artículo 17 B de la Ley 19.496 y en los artículos 9, 10 y 11 del Decreto 43, deben analizarse en concordancia con el artículo 17 E de la ley, el cual se hace cargo de definir las consecuencias que acarrea la eventual existencia de cláusulas o estipulaciones que infrinjan los deberes de información antedichos: el consumidor podrá solicitar la nulidad de dichas cláusulas o estipulaciones en los términos indicados.

> *"Artículo 17 E.- El consumidor afectado podrá solicitar la nulidad de una o varias cláusulas o estipulaciones que infrinjan el artículo 17 B. Esta nulidad podrá declararse por el juez en caso de que el contrato pueda subsistir con las restantes cláusulas o, en su defecto, el juez podrá ordenar la adecuación de las cláusulas correspondientes, sin perjuicio de la indemnización que pudiere determinar a favor del consumidor.*
>
> *Esta nulidad sólo podrá invocarse por el consumidor afectado, de manera que el proveedor no podrá invocarla para eximirse o retardar el cumplimiento parcial o total de las obligaciones que le imponen los respectivos contratos a favor del consumidor".*

PIZARRO estima que esta disposición es similar y sigue la misma lógica que la regla contenida en el artículo 16 A, conforme al cual se faculta al consumidor a solicitar la nulidad de las cláusulas abusivas. Así, ambas normas contienen una sanción clara: la nulidad de las cláusulas, de manera que habrá que prestar atención a las reglas generales de nulidad contenidas en el Código Civil.

Para este supuesto, la sanción máxima establecida en el derecho privado, consistente en la nulidad total del contrato resulta muy radical. Adicionalmente, desde el punto de vista de la intención de las partes al contratar y de los principios y normas de interpretación de los contratos (especialmente el efecto útil de los contratos), tampoco se justificaría la ilicitud

total del contrato y su correspondiente declaración de nulidad. Desde esta perspectiva, si el contrato pudiese subsistir, bajo una lógica de nulidad parcial, será el Juez quien determine la nulidad parcial del contrato, en aquellas partes viciadas y, de ser procedente, dará lugar a una indemnización a favor del consumidor[54].

De acuerdo con lo anterior, se constata que la implementación electrónica de la contratación de créditos de consumo debe considerar desde su diseño, estas menciones mínimas para cumplir con la normativa y no arriesgar una posterior declaración de nulidad en los términos señalados.

Para concluir este capítulo advertimos que el régimen regulatorio del crédito de consumo en Chile, a nivel general, se encuentra contenido en la Ley 19.496 de protección a los derechos de los consumidores, la cual, por modificación introducida por la ley 20.555 (SERNAC Financiero) avanzó en orden a regular el otorgamiento de créditos, establecer normas y procedimientos destinados a normar la oferta, venta y prestación de productos y servicios financieros, entre los cuales se incluyen los créditos hipotecarios, créditos de consumo, tarjetas de pago, seguros, etc.[55]

Con ello se ha propendido a mejorar el acceso al consumidor de créditos en condiciones más transparentes, en base a una intensificación de los deberes de información que debe satisfacer el proveedor de cara a la contratación de un crédito.

Sin embargo, considerando que, de la mano de la masificación de Internet como medio privilegiado para el desarrollo de negocios jurídicos, la aparición del comercio electrónico

---

[54] PIZARRO, C. 2013. Artículo 17 E., En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile, pp 440 - 442.

[55] BOZZO, S. 2020. cit. nota n. 7, p. 167.

como nuevo formato de contratación, ha propiciado que un sinnúmero de contratos sea celebrado en línea, siendo uno de ellos el del crédito de consumo.

Sin embargo, en atención al componente electrónico de la contratación, se abren nuevas aristas regulatorias a las cuales prestar atención de cara a definir el régimen regulatorio aplicable a la contratación de los créditos de consumo en Chile, pero en su formato electrónico. Probablemente la cuestión más relevantes guardan relación con el momento en que se entiende formado el consentimiento en los contratos de crédito de consumo que se celebran por medios electrónicos.

CAPÍTULO II.- SEGURIDAD DOCUMENTAL EN LA CONTRATACIÓN ELECTRÓNICA DEL CRÉDITO AL CONSUMO.

2.1.- El Pagaré Electrónico.

La forma más corriente de otorgar un préstamo es contra la firma de un pagaré o la aceptación de una letra de cambio por una determinada suma y a un plazo establecido, aunque también puede pactarse para ser pagado en cuotas. Puede decirse que todos los créditos de consumo quedan documentados mediante alguno de estos instrumentos[56].

El pagaré y la letra de cambio se encuentran regulados por el Título II de la ley 18.092 que dicta nuevas normas sobre letra de cambio y pagaré y deroga disposiciones del Código de Comercio.

Del análisis del referido Título es posible sostener que en la especie no concurre ninguna de las excepciones que el artículo 3º de la Ley 19.799[57] considera para la equivalencia de soportes[58]. Así, resulta perfectamente posible afirmar que es jurídicamente viable contar con un pagaré otorgado utilizando documento y firma electrónica[59].

---

[56] PLOTT, G. 2005. Manual de Operaciones y Servicios Bancarios. Santiago, Editorial Jurídica de Chile. p.92.

[57] Actos o contratos en que la ley: exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico; requiera la concurrencia personal de alguna de las partes; y, aquellos relativos al derecho de familia.

[58] Los actos y contratos celebrados por medios electrónicos estén o no firmados electrónicamente, y, en este último caso, esté la firma electrónica certificada por un certificador acreditado o no, son válidos. De esta manera estos actos y contratos se reputarán como escritos, de la misma manera que si lo fueran en soporte de papel.

[59] De acuerdo con el artículo 2 f) de la Ley 19.799 la firma electrónica es cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor. Por su parte, el artículo 2 g) dispone que "*la firma electrónica avanzada es aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría*".

Ahora bien, resuelto el hecho de que es posible contar con un pagaré electrónico, estimamos que tiene la más alta importancia analizar cuál es la situación del mérito ejecutivo del mismo con miras a asegurar el cobro judicial en un procedimiento compulsivo o de apremio.

Al respecto, es necesario tener presente que el primer requisito para la procedencia de una acción ejecutiva es que la obligación conste en un título ejecutivo.

Los títulos ejecutivos son documentos que dan cuenta de un derecho indubitado, al cual la ley le otorga mérito suficiente para que se pueda exigir el cumplimiento forzado de la obligación que en él se contiene sin necesidad de un juicio declarativo. Sólo la ley puede crear títulos ejecutivos, no así los particulares.

2.1.1.- Pagaré y Juicio Ejecutivo.

En lo que al pagaré electrónico se refiere, hay que tener presente, al efecto, el artículo 434 Nº4 del Código de Procedimiento Civil que dispone:

> "*El juicio ejecutivo tiene lugar en las obligaciones de dar* cuando *para reclamar su cumplimiento se hace valer alguno de los siguientes títulos: Nº 4 Instrumento privado, reconocido judicialmente o mandado a tener por reconocido. Sin embargo, no será necesario este reconocimiento respecto del aceptante de una letra de cambio o suscriptor pagaré que no hayan puesto tacha de falsedad a su firma al tiempo de protestarse el documento por falta de pago, siempre que el protesto haya sido personal, ni respecto de cualquiera de los obligados al pago de una letra de cambio, pagaré o cheque, cuando, puesto el protesto en su conocimiento por notificación judicial, no alegue tampoco en ese mismo acto o dentro de tercero día tacha de falsedad. Tendrá mérito ejecutivo, sin necesidad de reconocimiento previo, la letra de cambio, pagaré o cheque, respecto del obligado cuya firma aparezca autorizada*

por un notario o por el Oficial del Registro Civil en las comunas donde no tenga su asiento un notario".

2.1.2.- Hipótesis legales y Pagaré Electrónico.

El artículo 434 Nº4 del Código de Procedimiento Civil se coloca en tres hipótesis diferentes para señalar que el pagaré permite ser cobrado a través de un juicio ejecutivo. Estas son:

a. Cuando el pagaré ha sido reconocido judicialmente o mandado a tener por reconocido.
b. Cuando el suscriptor del pagaré no haya puesto tacha de falsedad a su firma al tiempo de protestarse el documento por falta de pago, siempre que el protesto haya sido personal, ni respecto de cualquiera de los obligados a su pago cuando, puesto el protesto en su conocimiento por notificación judicial, no se alegó tampoco en ese mismo acto o dentro de tercero día tacha de falsedad.
c. Cuando la firma del suscriptor aparezca autorizada por un notario o por el Oficial del Registro Civil en las comunas donde no tenga su asiento un notario.

Respecto a la hipótesis contenida en la letra a) no hay cuestión alguna que hacer presente para los efectos de este análisis. Sin embargo, respecto a las letras b) y c) si surgen algunos aspectos relevantes que considerar.

Respecto a la hipótesis contenida en la letra b) resulta indispensable determinar la consecuencia jurídica de que el pagaré electrónico se encuentre suscrito mediante la firma electrónica avanzada del suscriptor.

Al respecto, el artículo 5º de la Ley 19.799 dispone que los instrumentos privados suscritos con firma electrónica avanzada tendrán el valor probatorio de los instrumentos públicos. En virtud de lo dispuesto por el artículo 1700 del Código Civil esto quiere decir que hacen plena fe en cuanto al hecho de haberse otorgado y respecto a las declaraciones del pagaré, únicamente contra el suscriptor del mismo. Asimismo, las obligaciones y descargos que el

pagaré contenga harán plena prueba respecto del suscriptor y las personas a quienes se transfieran esas obligaciones y descargos por título universal o singular.

Ahora bien, la cuestión que queda por dilucidar es qué ocurre si el suscriptor del pagaré opone tacha de falsedad a su firma al tiempo de protestarse el documento por falta de pago.

Dado el valor probatorio que le asigna el artículo 5º de la ley 19.799, a los instrumentos privados firmados con firma electrónica avanzada, la tacha de falsedad debería ser resuelta previa realización de la prueba complementaria de autenticidad a que se refiere el inciso tercero del artículo 348 bis del Código de Procedimiento Civil.

Para ello, el perito a través de rutinas tecnológicas deberá limitarse a comprobar que el Hash y la Encriptación de éste son válidas y corresponden al documento y al tenedor del certificado.

De esta forma el procedimiento de validación habitualmente se centrará en:

a. Revisar el certificado de quien aparece suscribiendo el documento, aparte de identificar su nombre, su correo electrónico, su clave pública y su RUN, y otro conjunto de datos, se identifica que algoritmos el usa para firmar. En este caso por ejemplo se usa SHA-2 y RSA;
b. Se busca o se dispone de rutinas estándares y certificadas que implanten estos algoritmos. En este caso se usan rutinas certificadas por el NIST (National Institute of Standards and Technology)[60] que es la organización que pública los estándares

[60] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, [en línea] <https://www.nist.gov/> [consulta: 14 de julio 2021]

FIPS. Para el RSA o el DSA se requiere que la implantación cumpla con el ANSI X9.31, o el FIPS 186-1 o 186-2[61].

De este modo los peritos siguiendo un procedimiento repetible para verificar la firma es capaz de acreditar que el documento suscrito se hizo efectivamente con dichas rutinas, y que el resultado es el que dice.

De este modo con una revisión tecnológica que efectúa el perito será posible resolver de manera certera respecto la titularidad de la firma electrónica que aparece suscribiendo el pagaré y si se mantienen vigentes los atributos de integridad y no repudio del instrumento.

Junto a ello, debe tenerse en consideración lo dispuesto por el artículo 110 de la Ley 18.092 que contiene un claro elemento disuasivo para quien tacha su firma al disponer que:

> *"cualquiera persona que en el acto de protesto o en la gestión preparatoria de la vía ejecutiva tachare de falsa su firma puesta en una letra de cambio o pagaré y resultare en definitiva que la firma es auténtica, será sancionada con las penas indicadas en el artículo 467 del Código Penal[62], salvo que acredite justa causa de error o que el título en el cual se estampó la firma es falso".*

Respecto a la hipótesis contenida en la letra c), estimamos que no se trata de una cuestión de derecho, sino un aspecto fáctico, toda vez que tal como lo señalamos precedentemente

---

[61] COMPUTER SECURITY RESOURSE CENTER, [en línea] <http://csrc.nist.gov/publications/PubsFIPS.html> [consulta: 14 de julio 2021].

[62] 1.º Presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si la defraudación excediera de cuarenta unidades tributarias mensuales.

2.º Presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.

3.º Presidio menor en su grado mínimo y multa de cinco unidades tributarias mensuales, si excediere de una unidad tributaria mensual y no pasare de cuatro unidades tributarias mensuales.

Si el valor de la cosa defraudada excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.

(respecto a la autorización por un notario de la firma en un pagaré), a este no es excluyente contar con la presencia física de la persona cuya rúbrica autentifica.

Por consiguiente, si consideramos que la normativa señala como requisito que la *firma del suscriptor aparezca autorizada por un notario o por el Oficial del Registro Civil en las comunas donde no tenga su asiento un notario,* estimamos que una sana interpretación del artículo 434 N°4 inciso 2° del Código de Procedimiento Civil no permite sostener que sea requisito que el sujeto obligado comparezca ante el notario a firmar en su presencia el instrumento mercantil, sea pagaré, cheque o letra de cambio, sino que sería suficiente la mera actuación de ese ministro de fe.

Sin perjuicio de lo anterior, para autorizar la firma del obligado al notario le debe constar por cualquier medio que la firma estampada en el documento corresponda a dicha persona.

Llegamos a esta conclusión concordando las normas del CPC con los artículos 399 y siguientes del Código Orgánico de Tribunales. En concreto, el artículo 401 N°10, señala que es función de los notarios "*autorizar las firmas que se estampen en documentos privados, sea en su presencia o cuya autenticidad conste".* Tratándose del documento electrónico firmado con firma electrónica avanzada, la autenticidad viene reconocida por la ley 19.799 en los términos que señala la definición de este tipo de firma, a saber:

> *"g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría".*

No obstante, las instrucciones que ha impartido la Corte Suprema a través del Auto Acordado S/N sobre uso de documento y firma electrónica por Notarios, Conservadores y

Archiveros Judiciales, del año 2006[63], va en una dirección contraria a lo señalado, toda vez que en el número octavo ha dispuesto que:

> *"En los casos en que el Notario autorice una firma digital[64] estampada en su presencia, deberá dar fe de habérsele acreditado la identidad del firmante en los términos establecidos en el Código Orgánico de Tribunales*".

Esta referencia es confusa, por cuanto, tratándose de instrumentos privados regiría lo previsto en el artículo 401 del Código Orgánico de Tribunales. Esto sigue siendo válido en el caso de que la Corte Suprema se refiera al artículo 405 de este mismo cuerpo legal, previsto para las escrituras públicas, caso en el cual se prevé que deben ser suscritas ante notario. Sin perjuicio de lo anterior, la referencia seguiría siendo ambigua, puesto que este artículo regula los datos que, relativos a la individualización de las partes, deben hacerse constar en la escritura, como podemos apreciar de su tenor literal:

> *Art. 405. Las escrituras públicas deberán otorgarse ante notario y podrán ser extendidas manuscritas, mecanografiadas o en otra forma que leyes especiales autoricen. Deberán indicar el lugar y fecha de su otorgamiento; la individualización del notario autorizante y el nombre de los comparecientes, con expresión de su nacionalidad, estado civil, profesión, domicilio y cédula de identidad, salvo en el caso de extranjeros y chilenos radicados en el extranjero, quienes podrán acreditar su identidad con el pasaporte o con el documento de identificación con que se les permitió su ingreso al país.*

---

[63] CORTE SUPREMA. 2006. Auto Acordado sobre uso de documento y firma electrónica por notarios, conservadores y archiveros judiciales. 10 de noviembre de 2006. [en línea] <https://www.bcn.cl/leychile/navegar?idNorma=255008> [consulta: 21 mayo 2021].

[64] La firma digital para los efectos del referido Auto Acordado se debe considerar como una equivalente a la firma electrónica en los términos establecidos en la Ley 19.799.

Adicionalmente, esta interpretación es consistente con el texto expreso de la ley. Si repasamos el artículo 401 del Código Orgánico de Tribunales advertiremos que en él se consignan dos hipótesis fácticas de autorización de la firma del instrumento privado por el notario:

a) Que los instrumentos se firmen en su presencia
b) Que la autenticidad le conste al notario

El caso es que, la Corte Suprema, en su Auto Acordado de 2006 ha limitado la actividad notarial a autorizar firmas electrónicas en aquellos casos que se estampan en los documentos electrónicos en su presencia. Con ello, en lo que se refiere al instrumento que estamos analizando, se ha generado artificialmente la limitación de que al momento de otorgarse un pagaré electrónico el suscriptor del mismo debe encontrarse en el oficio del Notario.

Junto a ello, la Corte de Apelaciones de Santiago en resolución de 23 de febrero de 2021 resolvió que la frecuencia y relevancia en la utilización de estos títulos de crédito aconseja que se entreguen instrucciones sobre la materia que se viene considerando.

En concreto, tomando en cuenta la naturaleza jurídica y cualidades de las letras de cambio y pagarés, vale decir, su materialidad, literalidad y autonomía, no resulta legalmente posible, aunque puedan suscribirse de manera electrónica. En efecto, al tratarse de títulos de crédito que, en su caso, permiten ejecutar el cobro sin atender a las relaciones jurídicas que pudieron darles origen, su eventual suscripción de una manera distinta a la materialidad tradicional podría dar espacio o cabida para el ejercicio de más de una acción de cobranza, en forma simultánea. Esto ha quedado en evidencia en el caso de la clonación de tarjetas de crédito. Sin embargo, no se ha prohibido el uso de esos instrumentos por el hecho de que sea factible su uso malicioso o que puedan ser objeto de estos delitos.

A lo señalado anteriormente, la Corte de Apelaciones de Santiago agrega que tanto el endoso como el protesto deben estamparse en el título mismo, ya sea al dorso o en una

hoja de prolongación y que, luego del pago, el obligado tiene la facultad para exigir que le sea entregado el instrumento con la constancia de pago.

Por ende, estima que los efectos que acarrea el rasgo material inherente a esos títulos, hace que no se avengan con la naturaleza electrónica.

Con estas instrucciones, la Corte de Apelaciones de Santiago cerró la posibilidad que los pagarés sean suscritos en forma electrónica, al menos en su jurisdicción.

A nuestro juicio, sería razonable que el legislador resuelva esta problemática, modificando la ley de letras de cambio, pagares y cheques y previendo los resguardos que permitan avanzar a la normativa al actual estado de la técnica, de la misma manera que en su momento se hizo con la factura electrónica. A eso nos referiremos a continuación.

2.13.- Mandato electrónico.

Como consecuencia de la imposibilidad de contar con una letra de cambio o un pagaré electrónico con mérito ejecutivo es que el comercio y la industria del crédito han recurrido a la figura del mandato electrónico.

A través de éste el mandatario (cliente) autoriza al proveedor (comercio o institución crediticia) para que actuando por su cuenta y riesgo acepte letras de cambio o suscriba pagarés con o sin obligación de protesto, autorice la firma del o los representantes del proveedor ante Notario Público y reconozca deudas en su beneficio por los montos, capital, intereses, costas, impuestos y demás gastos que se originen con motivo del o los créditos otorgados.

Así, lo que se busca es que las operaciones de crédito de dinero queden respaldadas a través de la posibilidad de los proveedores de emitir las letras de cambio o pagarés necesarios de acuerdo a las reglas generales, pero a partir de un mandato que ha sido otorgado electrónicamente y con ello beneficiarse de las oportunidades que la gestión documental electrónica trae consigo.

Ahora bien, al respecto resulta importante tener presente que el contrato de mandato se encuentra definido en el artículo 2116 del Código Civil como:

> *"un contrato en que una persona confía la gestión de uno o más negocios a otra, que se hace cargo de ellos por cuenta y riesgo de la primera".*

Por su parte, el artículo 233 del Código de Comercio define al mandato comercial como:

> *"aquél por el cual una persona encarga la ejecución de uno o más negocios lícitos de comercio a otra que se obliga a administrarlos gratuitamente o mediante una retribución y a dar cuenta de su desempeño."*

De acuerdo con el artículo 2123, el mandato es, además, un contrato consensual, es decir, que puede celebrarse por escrito, por escritura pública, privada e incluso verbalmente.

> *"El encargo que es objeto del mandato puede hacerse por escritura pública o privada, por cartas, verbalmente o de cualquier otro modo inteligible, y aun por la aquiescencia tácita de una persona a la gestión de sus negocios por otra; pero no se admitirá en juicio la prueba testimonial sino en conformidad a las reglas generales, ni la escritura privada cuando las leyes requieran un instrumento auténtico."*

Así, en virtud del principio de equivalencia de soportes a que se refiere el artículo 3 de la Ley 19.799, por medio del cual los actos y contratos suscritos por medio de firma electrónica serán válidos de la misma manera y producirán los mismos efectos que si se hubiera suscrito por escrito y soportado en papel, es que el mandato que se otorgue a través de documento y firma electrónica tendrá la misma validez ya sea que se firme por manuscritos o medios electrónicos, como firma electrónica simple o avanzada.

2.14.- Proyecto de ley que busca crear el pagaré electrónico.

Finalmente, resulta pertinente hacer presente que está en tramitación el Proyecto de ley Boletín 8466-07 que modifica la Ley 19.799 y otros textos legales conteniendo una doctrina

más acorde con las necesidades del tráfico jurídico y comercial. El proyecto modifica la ley 18.092 disponiendo expresamente lo siguiente:

> *"Tendrá mérito ejecutivo, sin necesidad de reconocimiento previo, la letra de cambio o pagaré extendido en documento electrónico y suscrito por el obligado con firma electrónica avanzada y sellado de tiempo, siempre que el impuesto de timbres y estampillas respectivo sea pagado en los plazos que corresponda, según el artículo 15 del decreto ley N° 3.475, que modifica la Ley de Timbres y Estampillas, contenida en el decreto ley N° 619, de 1974"*.

De aprobarse el texto propuesto, no se hará necesario realizar gestión preparatoria alguna para que el pagaré electrónico tenga mérito ejecutivo, toda vez que el título se encontrará completo por el sólo ministerio de la ley. Con todo, estimamos que sería conveniente hacer ciertas adecuaciones al Proyecto de Ley que permitan:

1. Trasladar el momento del pago del Impuesto de timbres y estampilla al momento del protesto y no a aquel en que se extiende.
2. Precisar que todas las operaciones que tienen lugar durante el ciclo de vida del pagaré se pueden efectuar mediante documento electrónico, en cuyo caso la persona que efectúa la diligencia deberá estampar su firma electrónica en el pagaré electrónico o en otro documento electrónico que se mantenga indisolublemente vinculado con la letra de cambio o el pagaré respectivo.
3. Crear un Registro Nacional de letras de cambio y pagaré electrónica donde sean anotadas por la persona a que debe hacerse el pago. El registro deberá procesar y registrar electrónicamente las letras de cambio y pagarés electrónicos que sean librados, debiendo coordinar y suministrar la información necesaria que permita el endoso, protesto y pago del impuesto de timbres y estampillas.

A modo de conclusión de este capítulo, podemos apreciar que la normativa no solo no prohíbe la contratación electrónica de créditos de consumo, sino que, a nuestro juicio, establece las bases que permiten su implementación. Los problemas normativos que detectamos se refieren a situaciones de borde, pero relevantes a los efectos de otorgar certezas a los operadores jurídicos. La mención expresa a que en estos casos el lugar del contrato podrá ser pactado y, en defecto de pacto sea el domicilio del consumidor si bien es útil no es necesaria, sin embargo, las normas claras respecto de los instrumentos mercantiles electrónicos si aparece como urgente.

La seguridad en la gestión de los documentos es un elemento fundamental para dotar de certeza jurídica a todo el tráfico documental electrónico. Para ello, resulta necesario velar por la debida implementación de mecanismos que permitan asegurar el trinomio autoría, integridad y no repudio en el ciclo de vida de los documentos electrónicos.

Para ello la Ley 19.799, normativa que se cierne como la piedra angular del comercio electrónico seguro, se aboca a regular fundamentalmente la existencia del documento y la firma electrónica, ambos elementos a través de los cuales se concretiza la posibilidad de manifestar la voluntad en un acto jurídico y con ello dar vida al contrato de crédito de consumo a través de técnicas y medios electrónicos.

Dado lo anterior, resulta indispensable detenerse en el análisis de la regulación que la legislación hace del documento y la firma electrónica.

2.2.- El documento electrónico.

Mucho se ha dicho en doctrina que la expresión “documento” obedece a un concepto más amplio que el de “instrumento”, pues aquél comprende todo medio externo representativo de una idea. En nuestro derecho positivo ambas expresiones son sinónimas y se refieren a la prueba documental o escrita, cuya característica esencial es constituirse en el testimonio

del pensamiento o de la manifestación de voluntad de una persona. Según KISCH documentos:

> *"Son todas las cosas donde se expresa, por medio de signos, una manifestación del pensamiento. Es indiferente el material sobre el que los signos están escritos. También lo es la clase de escritura (pueden ser letras, números, signos taquigráficos, grabados en madera, etc.*[65]*"*.

Sobre la base de la definición precedente y siguiendo en el análisis a BLANQUER[66] son dos las notas características del documento: la primera, que es una cosa y la segunda que enseña algo. De ello se desprende, por una parte, la corporalidad del mismo y, por la otra, el atributo "docencia".

A su vez, la corporalidad del documento se compone, según dicho autor, del soporte del documento y la grafía que a él se incorpora, que es la escritura.

En consecuencia, tratándose de documentos electrónicos[67], el soporte en que se almacene el documento deberá tener propiedades electrónicas, excluyendo, en consecuencia, aquellos que se almacenen en medios ópticos o auditivos, salvo que se encuentren en tal formato, y la escritura que se incorpora al documento utilizará el lenguaje binario, que consiste en una combinación de unos y ceros que representan los diferentes caracteres del lenguaje humano[68].

---

[65] ALESSANDRI, A. y SOMARRIVA, M. 1991. Derecho Civil. Parte Preliminar y Parte General. Santiago, Editorial Conosur. Tomo II. p. 417.

[66] DE PRADA. V. 2001. Nuevos Campos que abre la informática a la función notarial. En Colegios Notariales de España. Notariado y Contratación Electrónica. Madrid. p. 317.

[67] De acuerdo con el artículo 2 d) de la Ley 19.799 el documento electrónico es "*toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior*".

[68] TEMBOURY, M. 2000. La Prueba de los Documentos Electrónicos en los Distintos Órdenes Jurisdiccionales, En: Derecho de Internet. Contratación Electrónica y Firma Digital. Navarra, Aranzadi, p. 413.

Los documentos surgen como consecuencia de la necesidad de dejar testimonio de las actuaciones que realizan las personas y, en tal sentido, es que el papel ha sido durante largos años el dominador como soporte absoluto al que se incorpora el pensamiento.

Sin embargo, el papel comienza poco a poco a ceder el protagonismo absoluto con la llegada de la transformación digital, entendida ésta como el cambio asociado a la aplicación de tecnologías digitales en todos los aspectos de la sociedad humana.

El artículo 2 letra d) de la Ley 19.799 define el documento electrónico como:

> *"Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior"*.

En consecuencia, se puede advertir con toda claridad que sigue manteniéndose el doble carácter, al que se refería BLANQUER, y únicamente se altera el soporte en que es contenido y que forma parte de la corporalidad del documento. Es por ello por lo que todo lo que tradicionalmente se dice para el documento debe ser entendido igualmente para el documento electrónico, sin perjuicio de las particularidades que le aporta el soporte en que se almacena.

Atendida la norma referida, se hace necesaria la concurrencia copulativa de tres requisitos para la existencia legal de un documento electrónico. Estos son:

a. Que se trate de la representación de un hecho, una imagen o idea.
b. Que sea creado, enviado, comunicado o recibido por medios electrónicos.
c. Que se almacene en un medio idóneo para permitir su uso posterior.

Técnicamente se puede afirmar que el documento electrónico depende de su contenido, de los mecanismos de representación y almacenamiento junto a los elementos y procedimientos que permitan su administración y uso posterior.

2.2.1.- Igualdad entre el papel y el soporte electrónico.

Desde mucho antes de la entrada en vigor de la Ley 19.799, el documento electrónico ya se utilizaba, tanto para el desarrollo de actividades del mundo privado, como en las primeras manifestaciones de gobierno electrónico que se habían ido incorporando en nuestro país.

Sin embargo, llegado el momento en que se hacía necesario hacer uso del documento electrónico en un conflicto de relevancia jurídica surgía, entre otras cosas, la necesidad de determinar el valor jurídico y probatorio del mismo. Ello llevó a las instituciones gubernamentales pioneras en el tema a dictar diferentes actos administrativos que dieran valor jurídico a los actos que se ejecutaban por medios electrónicos.

Con la finalidad de poner término a estas interrogantes y encontrar una solución, la Ley 19.799 se pronuncia, justamente, sobre ese tipo de cuestiones y, en tal sentido, en el artículo 1º consagra, este principio entre sus principios rectores al indicar que:

> "*Las actividades reguladas por esta ley se someterán a los principios de […] equivalencia del soporte electrónico al soporte de papel*"[69].

A continuación, el artículo 3° materializa tal principio, disponiendo lo siguiente:

> *"Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos o no por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel"*.

---

[69] Como ya se dijo, todos los actos y contratos celebrados por medios electrónicos, estén o no firmados electrónicamente, y, en este último caso, esté la firma electrónica certificada por un certificador acreditado o no, son válidos. De esta manera estos actos y contratos se reputarán como escritos, de la misma manera que si lo fueran en soporte de papel.

La equivalencia también está presente al momento de definir la admisibilidad como prueba en juicio y el valor probatorio de los documentos electrónicos. Historia de la ley. Compilación de textos oficiales del debate parlamentario. Volumen 1. Sesión 30º, en martes 29 de agosto de 200, página 6.

Agrega que, tratándose de actos o contratos en que es necesaria la escrituración o que la ley prevea consecuencias jurídicas por constar de ese modo, se les reputarán como escritos[70].

De este modo, la Ley 19.799 reconoce la existencia legal de los documentos electrónicos asignándoles tres importantes efectos jurídicos:

a. Igual validez que los documentos en papel.
b. Producen los mismos efectos que los celebrados por escrito y en soporte papel
c. Se les reputa como escritos para todos aquellos casos en que la ley asigne efectos jurídicos por constar de ese modo el acto o contrato.

Esta equivalencia de soportes resulta especialmente relevante a la luz de los artículos 1708 y 1709 del Código Civil donde se declara la inadmisibilidad de la prueba de testigos para acreditar aquellos actos o contratos que deben constar por escrito, debiendo hacerlo aquellos que contienen la entrega o la promesa de entregar una cosa que valga más de 2 unidades tributarias mensuales.

El punto es que en virtud de la Ley 19.799, los actos y contratos otorgados por medios electrónicos se reputarán como escritos, en los casos en que la ley exige que consten de ese modo y en todos aquellos casos en que la ley prevea consecuencias jurídicas por constar de ese modo.

De esta manera, el documento electrónico será mirado como documento escrito para todos los efectos legales, incluyendo su calidad de escrito como requisito de validez o como medio

[70] A modo de ejemplo se puede señalar el artículo 1709 del Código Civil que dispone “No se admitirá prueba de testigos respecto de una obligación que haya debido consignarse por escrito.

de prueba de un acto o contrato, y para todos los efectos referidos a los artículos 1708 y 1709 del Código Civil[71].

Sin embargo, la equivalencia de soportes antes referida no es absoluta y el artículo 3º inciso 2 de la Ley 19.799 señala que no opera la equivalencia de soporte para los actos o contratos:

a. En que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico.
b. En que la ley requiera la concurrencia personal de alguna de las partes.
c. Los relativos al derecho de familia.

Con relación a aquellos actos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico, es necesario tener presente que las solemnidades:

> "*Son los requisitos externos prescritos por la ley como indispensables para la existencia misma del acto; son las formas en que, en ciertos actos, debe expresarse el consentimiento para que se considere dado. Su omisión produce la inexistencia o nulidad absoluta del acto*"[72].

Por lo tanto, un acto o contrato quedará excluido de la Ley 19.799 en la medida en que no se pueda cumplir electrónicamente la solemnidad que, legalmente, se le exige a dicho acto. Por consiguiente, se tratará de una situación de hecho, que deberá analizarse caso a caso. *Prima facie* es posible afirmar que esta exclusión es la más fácil de resolver, toda vez que únicamente implica adecuar el ordenamiento jurídico a las nuevas tecnologías, para que se puedan cumplir, por medio del documento electrónico, las solemnidades requeridas por la ley para la existencia y/o validez del acto o contrato que se ejecuta o celebra. En definitiva,

---

[71] CANELO, C. 2003. La Eficacia Probatoria y la ley de Firma Electrónica. Revista Chilena de Derecho Informático, Núm 2, p. 65.

[72] ALESSANDRI, A. y SOMARRIVA, M. 1991, cit. nota n. 65, p. 295.

requiere asumir que la incorporación de las nuevas tecnologías a nuestra legalidad es un proceso gradual, que recién se inició con la Ley 19.799.

Sin embargo, con relación a las demás exclusiones que considera la Ley 19.799, el asunto es más delicado y se hará necesaria una discusión más profunda toda vez que obedecen a una convicción del tratamiento del tema hecho por los legisladores, más que a los ajustes de las normativas específicas.

La Ley 19.799 continúa el desarrollo normativo señalando que existen instrumentos públicos y privados electrónicos. Atendido el análisis que nos convoca, es decir la contratación electrónica de créditos de consumo, el análisis normativo se limitará a la regulación que la ley hace de los instrumentos privados electrónicos.

En una acepción amplia, son instrumentos privados los otorgados por los particulares sin intervención de funcionario público en su calidad de tal[73].

Por ello, podemos afirmar que el documento privado se caracteriza, sustancialmente, por no estar protegido por la fe pública que se debe a los instrumentos públicos y que proviene de la participación de un funcionario público en su formación y/o cumplimiento de formalidades especiales[74].

Sobre la base de lo anteriormente expuesto, se hace necesario dejar asentado que el instrumento privado podrá ser tal por haberse suscrito entre particulares o bien porque tuvo la intervención de un funcionario público que se encontraba actuando fuera del ámbito de sus competencias.

---

[73] ALESSANDRI, A. y SOMARRIVA, M. 1991, cit. nota n. 65, p. 443.

[74] RIOSECO. E. 2017. La prueba ante la jurisprudencia: Derecho Civil y Procesal Civil. Santiago, Editorial Jurídica de Chile. p. 385.

Un análisis especial, merecen los instrumentos privados que son firmados ante notario o que son protocolizados. Con relación a ellos, es necesario tener presente que, de conformidad con lo dispuesto en el artículo 425 inciso 1° del Código Orgánico de Tribunales:

> *"Los notarios podrán autorizar las firmas que se estampen en documentos privados, siempre que den fe del conocimiento o de la identidad de los firmantes y dejen constancia de la fecha en que se firman*".

Sin embargo, la autorización de la firma por el notario no convierte al instrumento privado en instrumento público. Lo que hace es únicamente dejar constancia de que el documento fue firmado ante un testigo calificado.

Para los efectos del análisis que nos convoca, resulta fundamental la distinción hecha precedentemente, toda vez que, en nuestra opinión, no hay obstáculo legal para que un notario autorice una firma electrónica. Será una cuestión de hecho la forma en que esto se haga. Hay jurisprudencia de nuestros tribunales que fortalecen esta consideración, según la cual:

> "*La autorización del notario de la firma de un pagaré no supone necesariamente la presencia de este ante el ministro de fe. El vocablo autorizar no supone la presencia de la persona cuya rúbrica autentifica. Por consiguiente, la correcta interpretación del artículo 434 N°4 inciso 2° del Código de Procedimiento Civil no lleva a exigir siquiera la comparecencia, ante el notario, del obligado que firma un instrumento mercantil, sea pagaré, cheque o letra de cambio; basta, al efecto, la sola actuación de ese ministro de fe. Para autorizar la firma del obligado es suficiente que al notario le conste por cualquier medio que ella corresponda a dicha persona*"[75].

[75] ALESSANDRI, A. y SOMARRIVA, M. 1991, cit. nota n. 65, Pág. 445.

Con todo, como señalamos antes, el Auto Acordado de la Corte Suprema sobre Uso de Documento y Firma Electrónica por Notarios, Conservadores y Archiveros Judiciales, en el número octavo, dispone que el Notario sólo podrá autorizar una firma digital en la medida que haya sido estampada en su presencia, debiendo dar fe de haberse acreditado la identidad del firmante en los términos establecidos en el Código Orgánico de Tribunales. De este modo, para que un Notario autorice una firma digital (firma electrónica o firma electrónica avanzada) deberá, de conformidad con el artículo 425 del Código Orgánico de Tribunales, dar fe del conocimiento o de la identidad de los firmantes, dejar constancia de la fecha en que se firma el documento y, por aplicación del artículo 409, el Notario podrá exigir, adicionalmente, que se registre la impresión del pulgar de la mano derecha o, en su defecto, el de la izquierda de los firmantes.

Con fecha 23 de febrero de 2021 la Corte de Apelaciones de Santiago procedió a regular el uso de herramientas informáticas en las diferentes notarías de la jurisdicción de Santiago, dictando instrucciones a todos los notarios con el fin de propiciar el uso de sistemas telemáticos en las diversas actividades que realizan los notarios y compatibilizar la optimización de sus servicios entregando la mayor facilidad posible a los usuarios asegurando la fe pública.

Las principales definiciones giran en torno a lo siguiente:

I.- En cuanto a la utilización de firma electrónica avanzada por parte de los notarios:

Los notarios podrán utilizar el dispositivo de su firma electrónica avanzada siempre que sea en forma personal e intransferible, en los días y horarios de funcionamiento de su oficio notarial y con relación a actuaciones verificadas dentro de su territorio jurisdiccional, con estricto apego a la ley y autos acordados de la Corte Suprema expedidos en la materia.

II.- En cuanto a la autorización de escrituras públicas:

Tratándose de esta clase de instrumentos el notario sólo podrá autorizar las firmas materiales o manuscritas estampadas en su presencia. Es decir, no se permite la firma electrónica avanzada para la suscripción de escrituras públicas.

III.- En cuanto al uso de medios telemáticos para la autorización de firmas estampadas en instrumentos privados y de plataformas tecnológicas para la verificación de identidad:

a. Autorización de firmas estampadas en forma remota o semipresencial.

   Podrán autorizarse las firmas que los otorgantes estampen en instrumentos privados cuando ello se haga en forma semipresencial o por medios telemáticos siempre que la verificación de la identidad en forma remota, lo sea de una manera que garantice que el notario pueda dar fe del conocimiento o de la identidad de los firmantes.

   Así, los notarios pueden implementar sistemas de verificación electrónica de identidad de los suscriptores de los instrumentos privados para que en forma electrónica el notario pueda realizar la autorización de las firmas.

b. Autorización de firmas estampadas en instrumentos privados, en forma no presencial, cuya autenticidad consta al notario.
   - Queda permitida la utilización de bases de datos o de plataformas tecnológicas para verificar la identidad de los firmantes o la autenticidad de sus firmas, siempre que las mismas tengan un carácter oficial o que sean propias de la notaría y de su exclusiva responsabilidad; y
   - Queda proscrito el redireccionamiento o derivación de esta clase de trámites a plataformas o bases de datos privadas y externas.

IV.- Situación de las letras de cambio y pagarés:

No está permitida la autorización de firmas electrónicas estampadas en letras de cambio ni pagarés, ni en endosos o protestos.

V.- En cuanto a la territorialidad de la función notarial:

En cualquier caso, el ejercicio de las funciones notariales sea de manera presencial o por vía telemática, sólo puede realizarse dentro del territorio para el que hubiere sido nombrado el notario.

2.2.2.- Valor probatorio del documento electrónico.

La importancia de la firma electrónica está dada por la posibilidad de vincular el contenido o declaración de un documento con una determinada persona y, en tal sentido, por el deseo de obligarse con lo que dicho instrumento consigna.

Lo anterior asociado a la posibilidad de determinar con mayor o menor grado de certeza a la persona suscriptora y la posibilidad de repudiar el documento, ha llevado al legislador a reconocer un diferente valor probatorio atendiendo a la naturaleza de la firma que fue utilizada para suscribir el documento o contrato. Es en tal sentido que el artículo 5º establece lo siguiente, para luego referirse a las reglas que regirán en cada caso:

> *"Los documentos electrónicos podrán ser presentados en juicio, y en el caso de que se busque hacerlos valer como medios de prueba".*

Con ello el legislador robusteció la equivalencia entre el soporte de papel y el electrónico y, adicionalmente, dio una pauta al juez para que valore esta clase de documentos que se incorporaron con plena eficacia en nuestro sistema jurídico.

Para consagrar el valor probatorio de los instrumentos privados electrónicos el legislador optó por seguir la asignación tradicional de valor probatorio de la ley común, sin perjuicio

de asignar un valor probatorio privilegiado cuando el documento se encuentra suscrito con firma electrónica avanzada y sellado de tiempo.

Tratándose de los instrumentos privados, la Ley 19.799 introduce un distingo atendiendo a si el documento electrónico fue suscrito con firma electrónica avanzada o no y si tiene o no sellado de tiempo. Así, podemos distinguir:

a. **Instrumento privado con firma electrónica avanzada y sellado de tiempo**. Tendrá el mismo valor probatorio que un instrumento público. Es decir, de conformidad con el artículo 1700 del Código Civil, hace plena prueba en cuanto al hecho de haberse otorgado y su fecha, pero no en cuanto a la verdad de las declaraciones que en él hayan hecho los interesados.

   Que haga plena prueba quiere decir que por sí sólo basta para acreditar el hecho al que se refiere, sin que sea necesario el auxilio de otros medios probatorios para que produzca convicción[76].
b. **Instrumento privado sólo con firma electrónica avanzada**. Esta clase de instrumentos tendrá el mismo valor probatorio que un instrumento público, excepto respecto a la fecha en que fue otorgado. De este modo, hará plena prueba únicamente respecto al hecho de haberse otorgado.
c. **Instrumento privado con firma electrónica**. Respecto a estos documentos surge el problema de que éste, por sí mismo, no tendrá la aptitud de probar su origen, a diferencia de lo que ocurre con los instrumentos públicos o con los privados suscritos mediante una firma electrónica avanzada, ya que hay ausencia de garantías que aseguren que quien aparece como signatario lo haya suscrito realmente.

Así, se hace necesario distinguir si el documento se encuentra reconocido o mandado tener por tal y, en este sentido, el principio general que aplica es que este tipo de documento no

[76] ALESSANDRI, A. y SOMARRIVA, M. 1991, cit. nota n. 65, p. 428.

tiene valor probatorio alguno con respecto a los otorgantes, sin perjuicio de que pueda ser considerado un principio de prueba por escrito.

En caso de que sea reconocido o mandado tener por reconocido, adquiere valor de escritura pública respecto de las partes que aparecen o se reputan haberlo suscrito y de las personas a quienes se han traspasado las obligaciones y derechos de éstos, todo ello de conformidad con el artículo 1702 del Código Civil. Con relación a las declaraciones que en él se hacen y, de conformidad con el artículo 1706 del Código Civil y 5° de la Ley 19.799, el documento privado electrónico reconocido, al igual que el instrumento público electrónico y el instrumento privado firmado con firma electrónica avanzada, hace plena prueba entre las partes aun en lo meramente enunciativo, con tal que tenga relación directa con lo dispositivo del acto o contrato.

El mérito de la firma electrónica avanzada es que otorga un valor probatorio privilegiado a los instrumentos privados. Esto si bien puede parecer innovador, tiene toda lógica, toda vez que la firma electrónica avanzada tiene la particularidad de permitir identificar fehacientemente al autor, haciendo no repudiable el documento al garantizar la autoría y la integridad del mismo. Consecuentemente, carecería de sentido dotar al suscriptor del documento de la posibilidad de desconocer el documento, ya que las características técnicas de la firma electrónica avanzada dan certeza respecto de la titularidad e integridad del documento signado, haciéndolo en consecuencia irrepudiable.

Así, para terminar de analizar el que los instrumentos privados con firma electrónica avanzada y sellado de tiempo hagan plena prueba, se hace necesario definir el valor que este tipo de documento tiene para las partes y los terceros. Adicionalmente, hay que estar a lo que dice relación con el otorgamiento mismo del documento, su fecha y la verdad de las declaraciones que contiene.

a. **Valor probatorio entre las partes:** En cuanto al otorgamiento hace plena prueba del hecho de haberse otorgado por las personas y de la manera que en el instrumento

se expresa (artículos 17 y 1700 del Código Civil). En lo que dice relación con las declaraciones de las partes y las que emite el funcionario, hay que tener presente que, si bien las primeras se presumen sinceras, no hacen fe pública, ya que se conceden en atención al funcionario y no a las partes. A su vez, no todas las declaraciones del funcionario hacen plena prueba, habrá que distinguir:

Hacen plena prueba:

- Las que se refieren a hechos propios suyos.
- Las que aseveran hechos que el funcionario percibe por sus sentidos.
- Las que se refieran a hechos que haya comprobado por medios que la propia ley le suministra.

No hacen plena prueba:

- Las declaraciones que hace confiando en el dicho de otra persona.
- Las declaraciones que importan meras apreciaciones, sea porque los hechos a que se refieren no puede percibirlos por sus propios sentidos, sea porque no puede legalmente comprobarlos.

Respecto a las declaraciones de las partes, el artículo 1700 del Código Civil dispone que, en cuanto a la verdad de las declaraciones que en el documento han hecho los interesados, no hacen plena fe sino en contra de los declarantes. Dichas declaraciones pueden ser dispositivas o enunciativas. Las primeras son las que las partes tienen en consideración al momento de contratar y representan el objeto del acto o contrato, expresan la voluntad y especifican el objeto sobre el cual recae. Las enunciativas son aquellas en que las partes simplemente relatan enunciativamente hechos o actos jurídicos anteriores.

Respecto a las declaraciones enunciativas, de acuerdo con el artículo 1700 del Código Civil, el documento que las contiene no hace plena prueba de la verdad de

los hechos a que la declaración se refiere. Sin embargo, deben presumirse verdaderas en atención al principio del *onus probandi* en virtud del cual lo normal se presume y lo excepcional se debe probar, y lo normal es que el contenido de las declaraciones dispositivas sea veraz y no falso, por lo que deberá ser probada la falsedad de las declaraciones de este tipo.

En lo tocante a las disposiciones enunciativas, la sinceridad de las declaraciones no se presume, ya que las partes no prestan a ellas la misma atención que a las dispositivas. Sin embargo, el mérito probatorio de estas disposiciones está en función de la confesión extrajudicial o de testimonio, según sea el caso.

No obstante, hay ciertas declaraciones enunciativas que el legislador las equipara a las dispositivas y son las que tienen relación directa con éstas. Para tal efecto, el artículo 1706 del Código Civil dispone que el instrumento público hace fe entre las partes aun en lo meramente enunciativo, con tal que tenga relación directa con lo dispositivo del acto o contrato.

b. Valor probatorio respecto de terceros: esta clase de instrumentos producen plena prueba que respecto de los contratantes. En artículo 1700 del Código Civil no ofrece dudas al respecto. En cuanto a las declaraciones, es necesario distinguir entre las declaraciones dispositivas y enunciativas. Respecto de las primeras, se presumen verdaderas por el principio básico del *onus probandi*, descrito con anterioridad[77]. Las declaraciones enunciativas no tienen mérito alguno contra terceros, pero el tercero sí podrá invocarlas contra el que las ha hecho y la declaración tendrá en contra de

[77] Esta doctrina ha sido recogida por nuestra Corte Suprema, la que ha sostenido "*que es propio del instrumento público o auténtico, como su nombre lo indica, hacer fe contra todo el mundo y no sólo respecto de los declarantes, en cuanto lo que en él han dicho los interesados; y tal presunción de verdad debe subsistir mientras no se pruebe lo contrario*" (sentencia de 16 de agosto de 1940). ALESSANDRI, A. y SOMARRIVA, M. 1991, cit. nota n. 65, p. 435.

éste el mérito de la confesión extrajudicial. De esta manera servirá de base a una presunción judicial que acredite los hechos confesados, de conformidad con el artículo 398 del Código de Procedimiento Civil.

2.2.3.- Aspectos procesales del documento electrónico.

Una de las cuestiones que no quedó resuelta en la Ley 19.799 y que generó grandes incertidumbres era lo referido con la forma en que se debía incorporar este medio a las actuaciones judiciales.

Según ha quedado claro en las páginas precedentes, no hay duda de que el documento electrónico tiene tanto valor y eficacia jurídica como medio de prueba. Sin embargo, no fue inicialmente señalado por el legislador los aspectos relativos a la producción de la prueba de documentos electrónicos en el proceso, y así cumplir su finalidad principal: dar constancia de un determinado hecho, acto o contrato.

En la doctrina surgieron diferentes reacciones con relación al tema. Algunos sostuvieron que debe ser acompañado como prueba documental, otros que a través de la inspección personal del tribunal o mediante informe de peritos.

En definitiva, sea cual sea la posición que se tenga respecto de la forma en que el documento electrónico debe allegarse al proceso, es unánime el considerar que no se trata de una prueba autónoma y, en consecuencia, que era necesario subsumirla en los supuestos contemplados en la legislación procesal.

Estimamos que el documento electrónico debe ser acompañado como prueba documental, de manera de respetar su naturaleza y fisonomía. El aceptar que pueda acompañarse de una manera diferente implica tolerar que el documento electrónico se convierta en un medio de prueba distinto al que es por sus rasgos.

Por lo tanto, será necesario efectuar el análisis a la luz de lo dispuesto en el Título XI del Libro II del Código de Procedimiento Civil. Para ello, distinguiremos entre los instrumentos públicos y los privados.

Respecto de los instrumentos públicos, el artículo 342 del Código de Procedimiento Civil señala que:

> *"Serán considerados como instrumentos públicos en juicio siempre que en su otorgamiento se hayan cumplido las disposiciones legales que dan este carácter:*
>
> *1º. Los documentos originales.*
>
> *2º. Las copias dadas con los requisitos que las leyes prescriban para que hagan fe respecto de toda persona o, a lo menos, respecto de aquella contra quien se hacen valer.*
>
> *3º. Las copias que, obtenidas sin estos requisitos no sean objetadas como inexactas por la parte contraria dentro de los tres días siguientes a aquel en que se dio conocimiento de ellas.*
>
> *4º. Las copias que, objetadas en el caso del número anterior, sean cotejadas y halladas conforme con sus originales o con otras copias que hagan fe respecto de la parte contraria.*
>
> *5º. Los testimonios que el tribunal mande agregar durante el juicio, autorizados por su secretario u otro funcionario competente y sacados de los originales o de copias que reúnan las condiciones indicadas en la letra anterior.*
>
> *6º. Los documentos electrónicos suscritos mediante firma electrónica avanzada".*

Al respecto, merece un detenimiento especial por el tema en estudio lo que se refiere a los documentos originales. En materia electrónica se presentan dificultades a la hora de determinar cuál es el documento original y cuál es la copia, lo que reviste una gran importancia al momento de valorar la prueba. Así, lo que resulta verdaderamente relevante

en los documentos electrónicas es que se pueda garantizar en ellos la autoría, integridad y no repudio, elementos que se garantizan por medio de la incorporación en ellos de firma electrónica soportada, en la actualidad, en tecnología de infraestructura de clave pública.

Con relación a los instrumentos privados en soporte papel, a diferencia del instrumento público, no interviene un funcionario que dé fe de su autenticidad, sino que lleva firmas cuya verdad nadie garantiza. Asimismo, carece de valor probatorio por sí mismo mientras no sea reconocido por la persona contra quien se hace valer o se mande tenerlo por reconocido en virtud de una resolución judicial[78].

En consecuencia, se hace necesario que en el proceso se produzca este reconocimiento, para lo cual el artículo 346 del Código de Procedimiento Civil prevé un reconocimiento expreso del documento y uno tácito. El primero está dado por el hecho de que la persona a cuyo nombre aparece otorgado o la parte contra la cual se hace valer haya declarado en el juicio reconociéndolo; o haya hecho igual declaración en un instrumento público o en otro juicio diverso. En forma tácita se produce el reconocimiento cuando, puesto en conocimiento de la parte contraria, no se alega su falsedad o falta de integridad dentro de los seis días siguientes a su presentación. Para ello el tribunal deberá apercibir a aquella parte con el reconocimiento tácito del documento si nada expone dentro de dicho plazo.

En consecuencia, la forma de acompañar los documentos privados en los procesos judiciales es bajo el apercibimiento del artículo 346 N°3 del Código de Procedimiento Civil. Esto es, solicitando que se tenga por reconocido si la parte contra la cual se hace valer no alega la falsedad o falta de integridad dentro del plazo de seis días.

[78] PAILLAS, E. 1979. Estudios de Derecho Probatorio. Santiago, Editorial Jurídica de Chile. 158p, p. 67.

En este punto surge una cuestión que es necesario analizar, toda vez que el artículo 5° N°2 de la Ley 19.799 dispone que los documentos que posean la calidad de instrumento privado harán plena prueba en cuanto hayan sido suscritos mediante firma electrónica avanzada.

Por lo tanto, tratándose de instrumentos privados suscritos por medio de una firma electrónica avanzada no sería necesario requerir el reconocimiento que se exige a los instrumentos privados para que se tengan por reconocidos en un proceso judicial.

Sin duda, se trata de una cuestión que es novedosa e innovadora en nuestro sistema jurídico, toda vez que se respetan las cualidades técnicas de la firma electrónica avanzada al extremo de permitir que, sin la intervención de un datario de fe pública, haya garantía de la autoría e integridad del documento y que, consecuentemente, este se tenga por si solo por reconocido.

Adicionalmente, surge la necesidad de determinar si el hecho de que un documento privado suscrito por medio de una firma electrónica avanzada no requiere del reconocimiento de la parte contra la cual se hace valer para que haga plena prueba. Sin embargo, surge la duda razonable de si su presentación trae aparejado el que el documento se acompañe en el proceso con citación o bajo el apercibimiento del artículo 346 N°3 del Código de Procedimiento Civil.

Al respecto, si bien podríamos señalar que el documento debiera ser acompañado con citación para ser consecuente con el texto y espíritu de la ley, cuando los asimila en sus efectos probatorios a los instrumentos públicos. Sin embargo, el año 2007, mediante la ley 20.217, se efectuó una modificación al Código de Procedimiento Civil introduciéndose un nuevo artículo 348 bis, que dispone:

> *"Presentado un documento electrónico, el Tribunal citará para el 6° día a todas las partes a una audiencia de percepción documental. En caso de no contar con los medios técnicos electrónicos necesarios para su adecuada percepción, apercibirá a*

la parte que presentó el documento con tenerlo por no presentado de no concurrir a la audiencia con dichos medios.

Tratándose de documentos que no puedan ser transportados al tribunal, la audiencia tendrá lugar donde éstos se encuentren, a costa de la parte que los presente.

En caso de que el documento sea objetado, en conformidad con las reglas generales, el Tribunal podrá ordenar una prueba complementaria de autenticidad, a costa de la parte que formula la impugnación, sin perjuicio de lo que se resuelva sobre pago de costas. El resultado de la prueba complementaria de autenticidad será suficiente para tener por reconocido o por objetado el instrumento, según corresponda.

Para los efectos de proceder a la realización de la prueba complementaria de autenticidad, los peritos procederán con sujeción a lo dispuesto por los artículos 417 a 423.

En el caso de documentos electrónicos privados, para los efectos del artículo 346, N°3, se entenderá que han sido puestos en conocimiento de la parte contraria en la audiencia de percepción.

En el caso que los documentos electrónicos acompañados puedan ser percibidos directamente en la carpeta electrónica, el tribunal podrá omitir la citación a audiencia de percepción, debiéndose entender que han sido puestos en conocimiento de la parte contraria desde que se notifica la resolución que los tiene por acompañados bajo el apercibimiento correspondiente".

De este modo, la reforma creo las condiciones para asegurar que los documentos electrónicos se presenten en forma electrónica y se asegure la posibilidad de ser percibido por todos los interesados, estableciéndose que desde el momento de la percepción que se tiene de éstos es que comienza a correr el plazo para hacer las alegaciones que en derecho correspondan en contra de ellos. Adicionalmente, establece una novedad en lo que guarda

relación con el peritaje, ya que si bien establece que se rige por las reglas que norman dicha actuación judicial establece expresamente que el resultado del peritaje es vinculante para el juez.

Ahora bien, las normas aquí revisadas deben ser analizadas en concordancia con la Ley 20.886 sobre tramitación digital de los procedimientos judiciales, que dispone en su artículo 6º:

> *"Los documentos electrónicos se presentarán a través del sistema de tramitación electrónica del Poder Judicial o, en caso de requerirlo así las circunstancias, se acompañarán en el tribunal a través de la entrega de algún dispositivo de almacenamiento de datos electrónicos.*
>
> *Los documentos cuyo formato original no sea electrónico podrán presentarse materialmente en el tribunal y quedarán bajo la custodia del funcionario o ministro de fe correspondiente. No obstante, los títulos ejecutivos cuyo formato original no sea electrónico deberán presentarse materialmente en el tribunal y quedarán bajo la custodia del funcionario o ministro de fe correspondiente, bajo apercibimiento de tener por no iniciada la ejecución.*
>
> *Sin perjuicio de lo dispuesto en el inciso anterior, los documentos y títulos ejecutivos presentados materialmente deberán acompañarse con una copia en formato digital a través del sistema de tramitación electrónica del Poder Judicial o, en caso de requerirlo así las circunstancias, en el tribunal, a través de la entrega de algún dispositivo de almacenamiento de datos electrónicos.*
>
> *Si no se presentaren las copias digitales de los documentos o títulos ejecutivos, o si existiere una disconformidad substancial entre aquellas y el documento o título ejecutivo original, el tribunal ordenará, de oficio o a petición de parte, que se acompañen las copias digitales correspondientes dentro de tercero día, bajo*

apercibimiento de tener por no presentado el documento o título ejecutivo respectivo.

En casos excepcionales, cuando se haya autorizado a una persona para presentar escritos materialmente por carecer de los medios tecnológicos, no será necesario acompañar copias digitales. En este caso, los documentos y títulos ejecutivos presentados en formato que no sea electrónico serán digitalizados e ingresados inmediatamente por el tribunal a la carpeta electrónica".

Finalmente, se debe tener en consideración que la referida ley de tramitación digital de los procedimientos judiciales incorporó una modificación al artículo 348 bis agregando un inciso final en los siguientes términos:

"En el caso que los documentos electrónicos acompañados puedan ser percibidos directamente en la carpeta electrónica, el tribunal podrá omitir la citación a audiencia de percepción, debiéndose entender que han sido puestos en conocimiento de la parte contraria desde que se notifica la resolución que los tiene por acompañados bajo el apercibimiento correspondiente".

2.3.- La Firma electrónica[79].

En el comercio electrónico el documento en papel como soporte que habilita para dejar constancia de los actos y contratos se sustituye por el documento electrónico. De la misma forma las firmas ológrafas son sustituidas por las firmas electrónicas, convirtiéndose en el mecanismo técnico que permite manifestar la voluntad frente a una determinada

[79] Esta sección fue elaborada a partir de un trabajo anterior realizado por mí y que fuera publicado en la Revista Chilena de Derecho Informático. Arrieta, R. 2003. Los prestadores de servicios de certificación de firma electrónica en el derecho chileno. En: Revista chilena de derecho informático. No2 año 2003. [en línea] <http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492,SCID%253D14662%2526ISID%253D292,00.html> [Consulta: 19 de julio 2021].

declaración en un documento electrónico y que, en consecuencia, permite a su autor hacerla suya y obligarse por lo que ella contiene.

La firma electrónica es definida en la Ley 19.799 en el artículo 2 letra f), como

> "*Cualquier sonido, símbolo o proceso electrónico, que permita al receptor de un documento electrónico identificar al menos formalmente a su autor*".

Sobre la base de la definición precedente, es posible advertir que se trata de un mecanismo tecnológicamente indefinido y, por lo tanto, cualquier técnica que permita plasmar el nombre o identificador formal de una persona, en un documento electrónico, deberá ser considerado como firma electrónica y dotar a dicho documento del valor probatorio que corresponda conforme a la ley.

Esta posibilidad dada por la ley ha sido objeto de latas discusiones y críticas ya que, por propender a la neutralidad tecnológica, se ha dado paso a que se utilicen algunas técnicas y medios electrónicos que hacen muy dificultoso, sino imposible en algunas oportunidades, los peritajes que permitan determinar la autoría de un determinado documento electrónico. Ello traerá aparejada la pérdida o detrimento del valor probatorio de esta clase de documentos, pudiendo llegar a cuestionarse el verdadero valor de firma de los mecanismos que no permitan dejar rastro del actuar del suscriptor del documento.

Por ello es por lo que, sin perjuicio de la neutralidad tecnológica establecida en la ley, las aplicaciones que se desarrollen e incorporen el uso de firma electrónica, deberán optar por tecnologías capaces de dejar un profundo rasgo de autoría, de manera de poder otorgar un mayor grado de seguridad y certeza respecto de la actuación en que se participa.

Actualmente, la infraestructura de clave pública es la tecnología que masivamente se encuentra disponible y que satisface de mejor forma estos requerimientos.

No obstante, el legislador contempló la firma electrónica avanzada, a la cual se le exigen atributos que restringen los mecanismos a ser utilizados y al mismo tiempo garantiza el que

quede un rastro susceptible de ser periciado. Así, el artículo 2 letra g) de la Ley 19.799 dispone que la firma electrónica avanzada es:

> "A*quella certificada por un prestador acreditado, y que ha sido creado usando medios que el titula mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría*".

Dicha norma ha sido objeto de una discusión acalorada, toda vez que se le acusa de romper el principio de neutralidad tecnológica al estar redactada en términos que hacen alusión a tecnología de infraestructura de clave pública. La discusión nos parece inoficiosa, toda vez que hoy aparece como vinculada a tal tipo de tecnología, porque es la que masivamente se encuentra disponible y, consecuentemente, es la que sirvió de inspiración al legislador. No obstante, tuvo la precaución de eliminar todo indicio que la limitara a tal tipo de tecnología. Así, estimamos que lo importante de destacar es el hecho de que la tecnología que se puede utilizar para la firma electrónica avanzada está dada por la forma de operar y por los objetivos que debe cumplir. Es decir, por el hecho de que los datos de creación de firma son generados y custodiados en todo momento por el mismo titular y, al mismo tiempo, por estar garantizado por su intermedio la autoría, integridad y no repudio del documento suscrito.

2.3.2.- La firma en los documentos privados electrónicos.

Hay variada doctrina y jurisprudencia en torno a la idea de que el instrumento privado, para ser tal, requiere estar a lo menos firmado por el o los otorgantes. Ello pareciera tener toda lógica si miramos a la firma como un medio idóneo que lleva asociada la voluntad de su titular, la que vinculada a un documento permite producir la convicción de que ella es afirmación de voluntad y, por ello, se acepta y se hace propio lo que allí se manifiesta.

Sin embargo, dicho criterio no fue el que siguió el legislador en el debate parlamentario ya que, tal como consta en la Historia de la ley, el documento electrónico ha de tener valor probatorio, independientemente de la naturaleza de la firma que se ha utilizado para suscribirlo, como del hecho de que el documento no aparezca firmado.

En tal sentido, cobra plena validez el análisis jurisprudencial que realiza Rioseco respecto del instrumento privado ante la jurisprudencia al señalar lo siguiente:

> "*Nos parece que la situación es diferente según se trate de constatar hechos a través del instrumento o de reconocer que una persona asume cierta obligación en el acto o contrato de que el documento da cuenta. Para esto último la firma es esencial, puesto que comporta la expresión voluntaria, personal y gráfica, en orden a obligarse, de modo que si falta no hay tal expresión. Pero si sólo se trata de constatar hechos de que el documento da cuenta o consigna, bastaría que emanara del otorgante por haberlo escrito sin necesidad de que estuviese firmado*[80]."

Por lo anterior, tratándose de un documento privado electrónico que carece de firma electrónica, será un problema de prueba el determinar si se le puede atribuir autoría como para definir si ha sido escrito por la persona contra la cual se hace valer y, de esta manera, cumplir con lo dispuesto por la ley común. En consecuencia, no se deberá desechar, *a priori,* el mérito de esta clase de documentos por el hecho de no encontrarse firmados.

[80] RIOSECO. E. 2017, cit. Nota n. 74 p. 387.

2.3.2.- Aspectos técnicos de la firma electrónica.

Antes de entrar en el análisis técnico de la firma electrónica, nos parece relevante precisar que no toda firma electrónica soportada en infraestructura de clave pública[81] es una firma electrónica avanzada, pero sí a la inversa.

Para entender con claridad en que consiste una infraestructura de clave pública nos parece relevante hacer un poco de historia y abordar algunos aspectos técnicos. Así, se hace necesario distinguir entre criptosistemas de cifrado simétricos[82] o de llave secreta y asimétricos[83] o de llave pública.

Un criptosistema, puede describirse como un conjunto normativo constituido por un emisor, quien es quien genera un mensaje denominado “mensaje en claro”; un dispositivo cifrador (que eventualmente incluirá un generador de llaves), que con el concurso de una

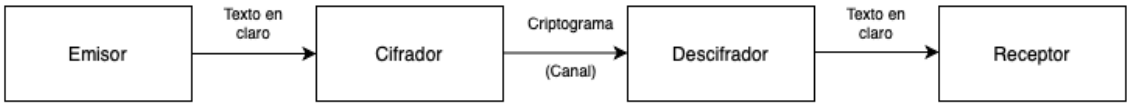
---

[81] Una infraestructura de claves públicas (PKI) es un sistema de recursos, políticas y servicios que da soporte al uso del cifrado de claves públicas para autenticar a las partes que participan en una transacción.

[82] En atención a que resulta clara y simple, recurriremos a la descripción que se realiza en Wikipedia, citando a G. J. Simmons, "A survey of Information Authentication". Contemporary Cryptology, The science of information integrity, ed. GJ Simmons, IEEE Press, New York, (1992), que señala lo siguiente: la criptografía de clave simétrica (en inglés symmetric key cryptography), también llamada criptografía de clave secreta (en inglés secret key cryptography) o criptografía de una clave (en inglés single-key cryptography), es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y este lo descifra con la misma clave. [en línea] < https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica> [consulta: 15 de julio 2021]

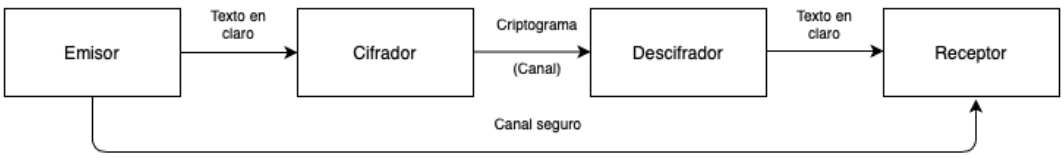
[83] En atención a que resulta clara y simple recurriremos a la descripción que se realiza en Wikipedia, citando a G. J. Simmons, "A survey of Information Authentication". Contemporary Cryptology, The science of information integrity, ed. GJ Simmons, IEEE Press, New York, (1992), que señala lo siguiente: la criptografía asimétrica (en inglés asymmetric key cryptography), también llamada criptografía de clave pública (en inglés public key cryptography) o criptografía de dos claves (en inglés two-key cryptography), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que recibirá el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves solo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves. [en línea] <https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica> [consulta: 15 de julio 2021]

clave criptográfica o simplemente llave de cifrado, transforma el “mensaje claro”, en un mensaje ininteligible, denominado “texto cifrado”; un canal (de almacenamiento o transmisión); un dispositivo descifrado, cuya misión es la inversa del cifrador; y un receptor de la información. Así mismo, debe incluir un protocolo de intercambio de llaves[84].



Esquema de un criptosistema de cifrado.

Históricamente apareció primero el criptosistema simétrico, caracterizado por el hecho de que la llave de cifrado es la misma que se emplea para descifrar. La vulnerabilidad del sistema depende del mantenimiento en secreto de la llave empleada. Ello obliga a que el canal que se utilice para poner la llave en poder del receptor del mensaje sea extremadamente seguro, ya que de ser obtenida por un posible interceptador el mensaje queda al descubierto.



Esquema de un criptosistema simétrico.

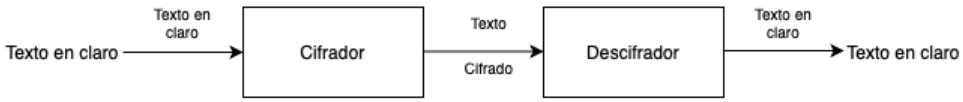
La vulnerabilidad del sistema planteado llevó a Whithfield Diffie y Marty Hellman, en 1976, a demostrar la posibilidad de construir un criptosistema que no precisaba la transferencia

[84] RIBAGORDA. A. 2002. Sistema de certificación: la firma y el certificado digital. En: FERNANDEZ, M., CREMADES, J. e ILLESCAS, R. Régimen Jurídico de Internet. Madrid, Wolters Kluwer, pp. 1313 - 1138. p. 1313.

de una clave secreta entre el emisor y el receptor del mensaje, con anterioridad a una transmisión cifrada. Nacían, así, los criptosistemas asimétricos.

Estos criptosistemas asimétricos funcionan sobre la base de dos llaves: una pública que se hace de general conocimiento y una privada que se debe mantener bajo el control exclusivo del titular.

Obviamente ambas llaves no son independientes, pero del conocimiento de la pública no es posible inferir la privada, a no ser que se tenga algún dato adicional, que también debe mantenerse en secreto o bien debe ser destruido una vez que ha sido generado el par de llaves. No se trata de claves independientes, sino que lo que hace una lo deshace la otra, o lo que es lo mismo, lo que una cifra la otra lo descifra.



Esquema de un criptosistema asimétrico.

Como puede advertirse, este sistema criptográfico asimétrico, también denominado de llave pública, en alusión a que la clave que sirve para descifrar es de conocimiento universal, y por esta vía resuelve el problema del canal seguro para la distribución de las llaves. De esta manera, el titular de la clave privada firma los mensajes y cualquier persona puede descifrarlos y acceder a su contenido, con la certeza de que el mensaje emana y por tanto puede ser atribuido al firmante. Asimismo, esta llave cumple una función de confidencialidad, puesto que permite enviar información cifrada al titular del par de llaves, con la confianza de que sólo esa persona podrá descifrarlo y abrir el mensaje, con su clave privada.

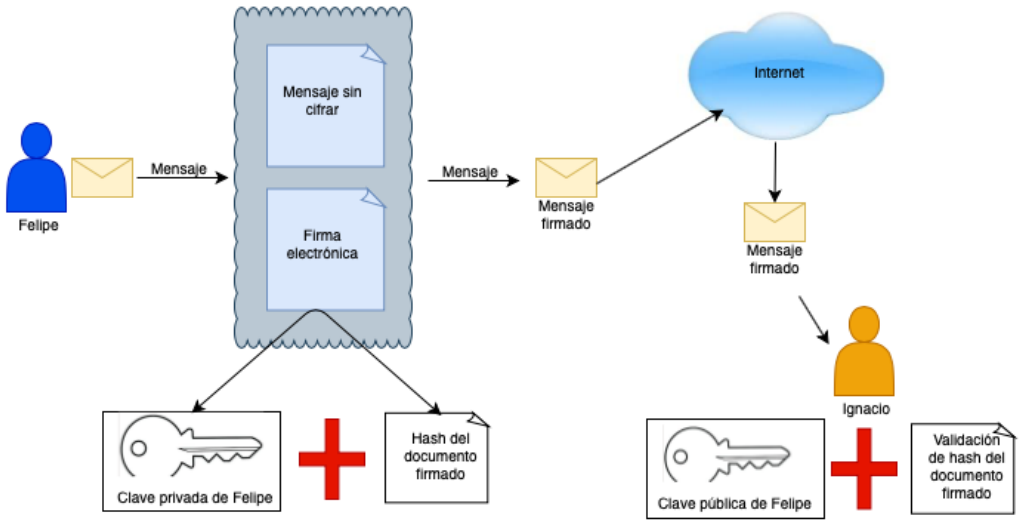
No obstante, la solución técnica dada por esta clase de criptosistemas se ha advertido que presentan dos inconvenientes principales: En primer lugar, en lo que respecta a la necesidad de garantizar la autenticidad de las llaves públicas, es decir, que la llave realmente

pertenece a quien dice. En segundo lugar, los cifrados asimétricos son mucho más lentos en sus operaciones de cifrado y descifrado que los sistemas de clave secreta.

El problema de la autenticidad de las llaves públicas ha sido resuelto por la aparición de los Prestadores de Servicios de Certificación de Firma Electrónica, cuya principal misión es constituirse en terceras partes que dan confianza de que la llave pública realmente pertenece a quien dice ser.

En cuanto a la lentitud de los sistemas asimétricos para cifrar y descifrar, el avance tecnológico será el que permita resolverlo. Con todo en la actualidad las buenas prácticas recomiendan usar el cifrado asimétrico para informaciones exiguas.

La firma electrónica soportada en infraestructura de clave pública opera sobre la base de un criptosistema asimétrico, donde el titular del certificado posee un par de llaves que le han sido proporcionadas por un prestador de servicios de certificación de firma electrónica que da testimonio de que el par de llaves se encuentran asociadas a la persona que aparece suscribiendo el documento.



Esquema de firma electrónica basada en infraestructura de llave pública.

2.4.- Los prestadores de servicios de certificación de firma electrónica[85].

Como consecuencia de la Sociedad de la Información, ha surgido una variada gama de figuras que interactúan con la finalidad de permitir la generación, procesamiento y distribución del conocimiento y de la información.

Es en ese escenario que surgen los prestadores de servicios de certificación, cuya función principalmente es la de expedir certificados de firma electrónica.

Es importante hacer presente que los prestadores de servicios de certificación en el derecho comparado han recibido diferentes denominaciones, tales como terceras partes confiables o autoridades de certificación. No obstante, sin importar el nombre que reciban, siempre realizan esencialmente la misma función: emitir certificados de firma electrónica para dar confianza a las transacciones electrónicas en que se concurre con su suscripción.

La ley define al certificador o prestador de servicios de certificación, en el artículo 2 letra c), disponiendo que es "*la entidad prestadora de servicios de certificación de firmas electrónicas*".

Dicha definición no ayuda a esclarecer lo que es un prestador de servicios de certificación; sin embargo, se encuentra complementada por lo preceptuado en el artículo 11 de la ley, la que, siguiendo la directiva europea sobre firma electrónica[86], distingue entre certificadores acreditados y los que no lo están.

---

[85] Esta sección fue elaborada a partir de un trabajo anterior realizado por mí y que fuera publicado en la Revista Chilena de Derecho Informático. Arrieta, R. 2003. Los prestadores de servicios de certificación de firma electrónica en el derecho chileno. En: Revista chilena de derecho informático. No2 año 2003. [en línea] <http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492,SCID%253D14662%2526ISID%253D292,00.html> [Consulta: 19 de julio 2021].

[86] UNIÓN EUROPEA, Parlamento Europeo y del Consejo de la Unión Europea. 1999. Directiva 1999/93/CE "Por la que se establece un marco comunitario para la firma electrónica", de 13 de diciembre de 1999.

Los prestadores de servicios de certificación son las personas jurídicas nacionales o extranjeras, públicas o privadas, que otorgan certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar. Estas personas jurídicas, en caso de que deseen acreditarse, deberán estar domiciliadas en Chile y seguir el procedimiento de acreditación que señala el Título V de la ley y que desarrolla el Reglamento de la ley[87].

De la definición señalada se puede sostener que:

a. **Se trata de personas jurídicas**. El desarrollo de la actividad se encuentra reservado a este tipo de personas y consecuentemente la actividad les es privativa. Luego, conforme a la ley, una persona natural no podrá actuar como certificador de firmas electrónicas.
b. **Nacionales o extranjeras.** No es necesario que la persona jurídica se encuentre domiciliada en Chile para prestar los servicios de certificación de firma electrónica. Sin perjuicio de ello, sí es requisito contar con un domicilio chileno, para acreditarse y poder prestar el servicio como corresponde a esa clase de prestadores de servicios de certificación.
c. **Públicas o privadas.** Las personas jurídicas pueden serlo de derecho público o de derecho privado y, consecuentemente, nada obsta a que el certificador adopte cualquiera de las formas sociales previstas en el ordenamiento jurídico o, como así también, que el Estado cree una empresa para que desarrolle tal actividad.

[87] Ministerio de Economía Fomento y Reconstrucción. 2002 Decreto Supremo 181, de 2002.

2.4.1.- Obligaciones de los certificadores de firma electrónica.

La obligación es el vínculo jurídico entre dos o más personas determinadas (titular del certificado y prestador de servicios de certificación), mediante el cual una de ellas tiene la facultad de exigir algo de la otra.

La ley ha creado dos categorías de prestadores de servicios de certificación, aquellos que están acreditados y los que no lo están. Los primeros son los que voluntariamente han seguido un procedimiento ante la entidad acreditadora, radicada en la Subsecretaría de Economía y empresas de menor tamaño[88], a través del cual esa entidad ha efectuado la revisión del cumplimiento de los requisitos y obligaciones impuestos por el ordenamiento jurídico, y las guías técnicas de acreditación que esa entidad genera, las que recogen estándares y buenas prácticas de prestación del servicio.

Si esta revisión es satisfactoria, obtendrán el reconocimiento e inscripción de la Entidad Acreditadora en el registro público que para tales fines mantiene[89].

Como consecuencia, se hace necesario analizar las obligaciones que deben cumplir las certificadoras de, distinguiendo entre aquellas que son comunes y las que son exclusivas de los prestadores acreditados de servicios de certificación.

---

[88] ENTIDAD ACREDITADORA, [en línea] <https://www.entidadacreditadora.gob.cl/> [Consulta: 11 de julio 2021]

[89] ENTIDAD ACREDITADORA, [en línea] <https://www.entidadacreditadora.gob.cl/entidades/> [Consulta: 11 de julio 2021]

2.4.2.- Obligaciones comunes a ambos tipos de certificadores de firma electrónica.

a. Contar con reglas sobre prácticas de certificación[90] que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano (artículo 12 a) de la ley).

   Esta primera obligación que se impone a los prestadores de servicios de certificación conlleva un doble carácter:

   I. Tener prácticas de certificación que sean objetivas y no discriminatorias.

   Las prácticas de certificación son una descripción detallada de las políticas, procedimientos y mecanismos que el certificador se obliga a cumplir, en la prestación de servicios de certificación u homologación (artículo 6 Reglamento).

   Podemos afirmar que se trata de una declaración unilateral que hace el prestador de servicios de certificación por medio de la cual, se obliga a desarrollar su actividad, en la forma descrita en la Práctica. En tal sentido, se trata de una fuente de obligaciones para el certificador, que pasan a ser parte integrante del contrato que suscribe el titular del certificado de firma electrónica con la entidad que se lo provee. Ello lleva a que el titular del certificado tenga derecho a exigir no sólo lo que el contrato suscrito dispone, sino que también el contenido de la Práctica.

   Que sean objetivas y no discriminatoria será una cuestión de hecho que deberá ser resuelta, caso a caso, por los Tribunales de Justicia en caso de controversia. Con todo, tratándose de prestadores acreditados de servicios de certificación, el hecho mismo de la acreditación da un indicio de que dichas prácticas están acordes con este requisito, toda vez que ha existido un proceso de auditoría

[90] Esto es lo que técnicamente se conoce con el nombre de CPS por su sigla en inglés que abrevia "*certification practice statement*".

que ha verificado el cumplimiento de las normas técnicas fijadas en el Reglamento, que justamente buscan iluminar el mejor criterio para la elaboración de dichas prácticas.

II. **Comunicarlas a los usuarios de manera sencilla y en idioma castellano**. En atención a que las prácticas extremadamente técnicas, y el rol que juegan en la conformación de los derechos y obligaciones entre certificador y el titular de la firma electrónica, el legislador estimó necesario que para proteger a la parte más débil de la relación (titular del certificado) era necesario imponer al certificador la obligación de entregar al usuario una información simple y comprensible. Sólo de esa manera, el usuario podrá elegir con libertad y responsabilidad, al momento de tomar la decisión de adquirir una firma electrónica.

En cuanto al idioma, pese a que se trata de una actividad que se desarrolla en el marco de Internet, caracterizado por la aterritorialidad, el legislador exigió que la información se proporcione en la lengua oficial de Chile, de forma de permitir de una mejor manera a los habitantes conocer las condiciones en que se realiza la actividad.

b. **Mantener un registro de acceso público de certificados, en el que quedará constancia de aquellos emitidos y los que queden sin efecto, en los términos señalados por el Reglamento**. A dicho registro podrá accederse por medios electrónicos de manera continua y regular. Esta obligación tiene por finalidad que cualquier persona pueda comprobar que el certificado que se le presenta en un documento es auténtico y estaba vigente al momento de la firma. Para mantener este registro, el certificador podrá tratar los datos proporcionados por el titular del certificado que sean necesarios para este efecto, los que no se podrán utilizar para otros fines. Dichos datos deberán ser conservados a lo menos durante seis años

desde la emisión inicial de los certificados. En lo restante se aplicarán las disposiciones de la ley Nº19.628, sobre protección de la vida privada.

Esta obligación también conlleva un doble carácter:

I. **Registro de acceso público de certificados.** Se traduce en la necesidad del certificador de contar con un sitio de acceso electrónico, en el que se contenga un listado de los certificados de firma electrónica que ha emitido, indicando si el certificado se encuentra vigente o revocado.

   Con ello, la ley ha modificado la estructura tradicional en que se conservan estas listas, en la experiencia nacional e internacional, toda vez que por regla general ellas son únicamente listas de revocación, que no muestran los certificados que se encuentran vigentes, sino los que han sido revocados o suspendidos. Por ello es que la vigencia de un certificado de firma electrónica se determina por exclusión, ya que al no encontrarse el certificado de firma electrónica en dicha lista hace presuponer que está vigente. Sin embargo, el legislador quiso dar mayor certeza a las personas destinatarias o receptoras de los documentos electrónicos.

   Dicho registro debe permitir el acceso en forma regular y continua, lo que deberá ser descrito en las prácticas de certificación y calificadas por los Tribunales de Justicia, en caso de conflicto.

II. **Conservación de datos.** Los antecedentes que proporcione el solicitante del certificado, para la contratación del mismo, deben ser conservados, por el prestador de servicios de certificación, por al menos seis años.

   Es interesante advertir que, frente a esta obligación, el legislador no eximió de esta obligación al prestador de servicios de certificación que cese en su función. Al respecto, estimamos que si el legislador guardó silencio no corresponde al intérprete atribuirle la intención de liberarlo y, en consecuencia, la obligación se mantiene para el certificador aun cuando deje de desarrollar la actividad. El

mismo criterio siguió el Reglamento, cuyo artículo 11 inciso 2º, dispone que, "*en caso que el prestador de servicios de certificación cese en su actividad, deberá transferir dichos datos a un prestador acreditado de servicios de certificación o a una empresa especializada en la custodia de datos electrónicos, por el tiempo faltante para completar los seis años desde la emisión de cada certificado*".

El objetivo de lo anterior es garantizar la disponibilidad de los antecedentes que sirvieron de fundamento a la emisión de un certificado por todo el tiempo que el legislador estimó que era necesario, a los efectos de poder contar con ella en el evento que se produzca algún conflicto que requiera recurrir a dicha información.

c. **Transparencia activa.** En el caso de cesar voluntariamente en su actividad, los prestadores de servicios de certificación deberán comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establece el reglamento y deberán, de no existir oposición de estos últimos, transferir los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca. En caso de existir oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad.

   Uno de los principios inspiradores de la ley, que se encuentra consagrado en el artículo 1°, es el de la libre prestación de servicios. Ello trae aparejado que cualquier persona jurídica que cumpla con los requisitos legales y reglamentarios puede desarrollar la actividad, e igualmente dejar de hacerlo. Ello no obsta a que se exija adoptar medidas que protejan la titular del certificado de una interrupción de servicios.

Esta obligación contiene varios aspectos importantes que es necesario tener presente al momento de producirse el cese de la actividad por decisión del prestador de servicios de certificación:

I. **Comunicar a los titulares de los certificados que el prestador cesará en la actividad.**

   Esta comunicación deberá señalar que el certificador cesará en su actividad y, adicionalmente, manifestar al titular del certificado que tiene derecho a oponerse al traspaso de los datos de éste a otro prestador de servicios de certificación, situación en la cual su certificado será revocado (artículo 8 a) del Reglamento).

II. **Dar el aviso con una antelación de al menos dos meses.**

   El plazo fijado por esta norma es absolutamente concordante con lo dispuesto en el artículo 12 g) de la ley, que impone al prestador acreditado de servicios de certificación, la obligación de solicitar a la Entidad Acreditadora la cancelación de su inscripción en el registro público de certificadores acreditados que mantiene con al menos un mes de anticipación a la fecha en que se desea se produzca el cese de la actividad, indicando el destino que dará a los datos de los certificados (artículo 8 a) del Reglamento).

   Indudablemente para que el certificador que va a cesar en su actividad, voluntariamente, pueda señalar el destino que dará a los certificados de firma electrónica emitidos por ella, es necesario que el titular del certificado, haya manifestado su intención respecto al traspaso de los datos a otro prestador de servicios de certificación.

III. **Traspasar los datos de los certificados a otro prestador de servicios de certificación, en caso de no existir oposición del titular.**

   Este requisito, es consecuencia de la necesidad de asegurar la continuidad en la prestación de los servicios de certificación, no obstante, la libertad del

certificador para dejar de prestar el servicio para el cual fue contratado. Adicionalmente, puede ser considerado como la fórmula que se da al certificador que cesa anticipadamente de prestar un servicio, para no ser compelido al cumplimiento forzado del contrato de certificación de firma electrónica.

Esta norma conlleva un límite intrínseco, cual es que, en caso de que el certificador que cesa en la actividad se encuentre acreditado, los datos de los certificados de firma electrónica avanzada que haya emitido necesariamente se los deberá traspasar a un prestador acreditado de servicios de certificación (artículo 8 a) del Reglamento), toda vez que sólo de esa forma el certificado podrá mantener su carácter.

d. **Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, y las leyes Nº19.496, sobre Protección de los Derechos de los Consumidores, y Nº19.628, sobre Protección de la Vida Privada.**

   Se trata de una norma de clausura, que tiene por finalidad no hacer taxativa la numeración de las obligaciones previstas en el artículo 12 de la ley, sino que asentar que todo el ordenamiento jurídico aplica plenamente al desarrollo de la actividad.

   Las obligaciones que emanan de la ley de protección al consumidor son las comunes a un proveedor de bienes y servicios, y fueron tratadas en el capítulo I.

   Las relativas a la protección de datos serán analizadas en el capítulo III.

2.4.3.- Obligaciones exclusivas de los certificadores acreditados.

Se trata de obligaciones que los prestadores de servicios de certificación deben cumplir para obtener y mantener la acreditación:

a. **Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten.**

Se trata de una obligación que tiene por objeto lograr una efectiva simetría de la información, entre el certificador y el usuario o titular del certificado de firma electrónica.

Por medio de ella, se busca proteger el interés público y fortalecer la elección del consumidor, ya que, al contratar sobre la base de una buena información, oportuna y completa, le será posible elegir responsablemente el servicio de certificación con el que estime contratar. Se trata, por lo tanto, de una manifestación del principio de transparencia de la ley de protección a los consumidores.

b. **En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante, o de su representante legal, si se tratare de persona jurídica.**

Esta obligación, es la que impone al prestador acreditado de servicios de certificación, la realización de actividad registral sobre quien solicita un certificado de firma electrónica avanzada, de forma que se garantice, fehacientemente, la identidad del titular. Conforme al diccionario de la Real Academia Española de la Lengua, que sea fehaciente significa que “hace fe, que es “fidedigno”.

Esto tiene fundamento en el hecho de que la firma electrónica avanzada permite identificar al titular del certificado de manera fidedigna, haciendo fe de que es la persona que dice ser, y que como consecuencia el vínculo que existe entre el firmante y los datos de creación de firma se mantiene incólume. Dado este carácter, se exige un alto grado de precisión y certeza del proceso por medio del cual se genera ese vínculo, para que permitirá dar seguridad y garantía de que la persona que dice ser realmente lo sea. Solo así realmente dará confianza de la identidad de los intervinientes en una comunicación electrónica.

En el derecho comparado, para el desarrollo de esta actividad registral, se contempla la figura de la Autoridad o Entidad de Registro.

En el caso de Chile, se prevé que sea el mismo prestador de servicios de certificación quien lleve a cabo el procedimiento de comprobación fehaciente de la identidad del solicitante del certificado de firma electrónica avanzada. Los proveedores podrán delegar en un Notario o en un oficial del Registro Civil estas actividades de registro, sin embargo el mandato no libera a la PSC de la responsabilidad legal por esta actividad.

La normativa prevé que dentro del proceso el solicitante deberá comparecer personal y directamente ante quien realice la comprobación. Si se trata de una persona jurídica, deberá hacerlo su representante legal.

De esta forma, aunque el prestador de servicios de certificación en la práctica utilice autoridades de registro, siempre se entenderá que la actividad la realiza el mismo, con todas las implicancias de responsabilidad que ello conlleva.

El Reglamento ordena que la comprobación fehaciente de la identidad del solicitante se realice en conformidad con las normas técnicas fijadas en la primera disposición transitoria[91].

En el contexto de la crisis ocasionada por la pandemia del Covid-19, algunos prestadores de servicios de certificación han facilitado la obtención de certificados de firma electrónica por medios de canales electrónicos, exigiendo para su creación la utilización de la Clave Única del Registro Civil.

---

[91] ETSI. 2002. TS 102 042 “Policy requirements for certification authorities issuing public key certificates”. [en línea] <https://www.etsi.org/deliver/etsi_ts/102000_102099/102042/01.01.01_60/ts_102042v010101p.pdf> [consulta 5 de abril 2021].

c. **El Servicio de Registro Civil e Identificación, por su parte, ha habilitado canales para la comprobación de identidad que implique menor contacto o riesgos de contacto,** sin que se pierda la identificación del titular, como por ejemplo, la comparecencia por medio de videollamadas concertadas con funcionarios del servicio o bien, la habilitación de tótems en algunos puntos como municipalidades u oficinas de ChileAtiende, con miras a facilitar la comprobación fehaciente de la identidad a través de otros medios no presenciales, al menos físicamente, que propicien igualmente el cumplimiento del requisito. Pagar el arancel de acreditación al momento de solicitar la misma. El artículo 24 inciso 2° del Reglamento dispone que los costos de la acreditación serán pagados por el prestador de servicios de certificación que solicite acreditarse, los que no serán restituidos en el evento en que la acreditación no se conceda por incumplimiento de los requisitos y obligaciones legales y reglamentarias exigidos para el desarrollo de la actividad como acreditado. El arancel es fijado en el primer trimestre de cada año por la Subsecretaría de Economía, mediante resolución.

d. **Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores**.

   Esta obligación tiene por objeto que la Entidad Acreditadora financie la actividad de inspección que debe desarrollar, por mandato del artículo 20 de la ley, la que tiene por principal objeto garantizar a los usuarios de la firma electrónica avanzada la seguridad técnica del sistema.

   Comprende, por lo tanto, el peritaje que se realice con la finalidad de constatar el cumplimiento de los requisitos y obligaciones legales y reglamentarias, como la sujeción de la actividad a las normas técnicas que se fijan para el desarrollo de la actividad. Adicionalmente, los gastos de carácter administrativo, que genera el sistema para su adecuado funcionamiento.

De conformidad con el artículo 24 del Reglamento, el pago del arancel lo deberá realizar el certificador dentro del plazo de 90 días contados desde la fecha de la resolución que los fija.

e. **Solicitar la cancelación de su inscripción en el registro de prestadores acreditados, el que es llevado por la Entidad Acreditadora, con una antelación no inferior a un mes antes del cese en su actividad, y comunicar el destino que dará a los datos de los certificados, especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto.**

El principio que está subyacente en esta obligación es que las cosas se deshacen de la misma forma que se hacen. Si el certificador se acreditó para desarrollar la actividad de una determinada forma, debe desacreditarse para dejar de prestar el servicio correspondiente y ello sólo lo puede hacer la Entidad Acreditadora, la que para ello deberá velar por la protección de los derechos de los titulares de certificados de firma electrónica.

Atendida la importancia del servicio que se presta, nada más y nada menos que la de permitir a sus usuarios comunicarse en forma segura por medios electrónicos, es que debe informar si el servicio que está prestando garantiza la continuidad por medio de otro prestador de servicios de certificación y, en caso de ser así, con cuál, o bien, en caso contrario, si los va a revocar.

La norma en comento habla de los “datos de los certificados”, aunque en realidad está refiriendo al certificado propiamente tal. La confusión se produce con ocasión de que, al transferir el certificado a otro certificador, necesariamente éste deberá emitir un nuevo certificado de firma electrónica con sus datos. Esto se desprende del hecho que la norma concluye señalando que, en caso de que los datos de los certificados no se transfieran a otro certificador, estos deberán quedar sin efecto.

f. **En caso de cancelación de la inscripción en el registro de prestadores acreditados, los certificadores comunicarán inmediatamente esta circunstancia a cada uno de los usuarios y deberán, de la misma manera que respecto al cese voluntario de actividad, traspasar los datos de sus certificados a otro prestador, si el usuario no se opusiere**.

Ésta conlleva una doble obligación:

I. **Comunicar a sus usuarios de la cancelación**. Esta carga se impone al certificador, en aras de la seguridad del titular del certificado, teniendo concordancia con la forma en que el certificador realiza la actividad y con el hecho cierto de que al tener dicha calificación se encuentra legalmente habilitado para emitir certificados de firma electrónica avanzada. Al ser cancelada la inscripción es revocada la acreditación y, en consecuencia, el certificador pierde la habilitación para desarrollar la actividad como acreditado.

II. **Traspasar los datos de sus certificados a otro prestador**, si el usuario no se opusiere. Se obliga así al prestador de servicios de certificación, a traspasar los datos de sus certificados a otro prestador, y ello lleva como consecuencia que han cambiado las circunstancias bajo las cuales contrató el titular del certificado. Este aspecto parte de la base que el certificador al ser desacreditado cesa en el desarrollo de su actividad, lo que no es predeterminable, ya que éste podrá tomar la determinación de seguir desarrollando la actividad sin estar acreditado. En este caso este aspecto de la obligación debe mantenerse restringido al traspaso de los datos de los certificados de firma electrónica avanzada por ellos emitidos, debiendo en consecuencia ser transferidos, necesariamente, a otro prestador acreditado de servicios de certificación.

g. **Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto**

tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pago.

Se trata de una obligación que tiene por objeto permitir que la Entidad Acreditadora se encuentre en permanente conocimiento de las circunstancias bajo las cuales el certificador acreditado se encuentra desarrollando la actividad, ello con la finalidad de poder decidir si hay motivo para revocar la acreditación, por haberse modificado las condiciones que sirvieron de base a ella, y atendido el potencial peligro a que se puede ver afectada la comunidad, como consecuencia de las nuevas circunstancias.

2.4.4.- Actividades que realizan los prestadores de servicios de certificación de firma electrónica.

La Ley 19.799 no regula de manera específica o categórica las actividades que realizan los certificadores. Sin embargo, de lo dispuesto en el artículo 11 de la Ley 19.799, que define a los prestadores de servicios de certificación, podemos señalar que imperativamente se les ordena prestar el servicio de certificación. Ello conlleva la necesidad de determinar que se entiende por certificación bajo el prisma de esta actividad.

La norma en comento agrega que el certificador puede prestar servicios adicionales, al disponer "*sin perjuicio de los demás servicios que puedan realizar*". Esto llevó a un interesante debate parlamentario en torno a la necesidad de que los certificadores fueran personas jurídicas con giro exclusivo, buscando interpretar que dicha expresión, recogida del derecho comparado, trae consigo que el prestador de servicios de certificación puede realizar actividades que no se encuentran dentro del giro del negocio. Sin embargo, ello no hubiera sido acorde con la tendencia mundial, toda vez que dicha expresión apunta a la prestación de servicios complementarios que no sólo se encuentran dentro del giro del negocio sino, lo que es más, permiten que este se desarrolle de una manera más plena, satisfaciendo de esta manera los diferentes requerimientos que pueden tener los diferentes

actores que comercializan o se relacionan por medios electrónicos y que persiguen que cada vez sea más seguro.

2.4.4.1.- Actividad de certificación.

La certificación de las firmas electrónica busca generar seguridad a las personas que se comunican por medios electrónicos. Para ello actúan terceras partes, prestadores de servicios de certificación, dando certeza respecto a la identidad de las personas. Con tal fin al generar un documento electrónico, firmado por medio de una firma electrónica avanzada se garantiza que, quien hizo uso de los datos de creación de firma, realmente es la persona que se está identificando.

Resultado de las diferentes necesidades de los usuarios, en cuanto al grado de seguridad que requieren en la identificación de las personas en la red y los costos que la misma lleva asociada, es que el legislador ha previsto la posibilidad de que se certifiquen las firmas electrónicas o firmas electrónicas avanzadas. La diferencia entre ambas radica, desde un punto de vista técnico, básicamente en el grado de certidumbre con que el titular del certificado se puede identificar en la red. La primera identifica de manera formal, en cambio la avanzada de forma fehaciente.

Por ello es que, tratándose de certificados de firmas electrónicas avanzadas, se han impuesto mayores exigencias para la prestación del servicio, tal como se analizó con ocasión de las obligaciones de los certificadores.

Consensuadamente se pueden reconocer como parte del proceso de certificación las siguientes actividades:

a. **Solicitud del certificado**. La adquisición de un certificado de firma electrónica es un acto voluntario, sin perjuicio de que ciertas circunstancias pueden llevar a que una persona se vea forzada a contar con uno para los efectos de poder insertarse en las

diferentes formas de comunicación que se impongan al interior de una determinada comunidad a la cual pertenezca o le interese pasar a formar parte.

Sin embargo, sea cual sea el grado de libertad que tiene la persona para solicitar la firma electrónica, debe realizar un acto voluntario, cual es solicitar al prestador de servicios de certificación que se le emita un certificado de firma electrónica. Para ello, junto con la solicitud deberá proporcionar una serie de antecedentes de carácter personal que dotarán, en parte importante, de contenido al certificado, permitiendo cumplir con posterioridad la función de instrumento identificador en la Red.

Los antecedentes que el solicitante deba declarar dependerán de la naturaleza del certificado que esté solicitando y de lo que señalen las prácticas de certificación del prestador con quien se esté contratando. Sin embargo, al tenor de lo dispuesto en el artículo 15 letra c) de la ley, al menos, deberá indicar el nombre, dirección de correo electrónico y rol único tributario.

En cuanto a los medios o vías por las cuales puede realizarse la solicitud, se deberá estar con lo señalado en las prácticas de certificación. Estimamos, que la solicitud se podrá realizar por cualquier medio.

b. Registro del solicitante. Una vez que el prestador de servicios de certificación recibe la solicitud, procederá a la aprobación de la misma para lo cual deberá comprobar los antecedentes que le han sido declarados.

Los procedimientos de comprobación son fundamentales para que el sistema de las firmas electrónicas funcione en capacidad de brindar confianza a los usuarios. Por medio de estos procedimientos, el prestador de servicios de certificación verifica la exactitud de las declaraciones del solicitante, que de acuerdo con las prácticas y políticas de certificación del prestador de servicios de certificación. La rigurosidad en esta etapa será la que permita que los receptores de mensajes electrónicos confíen en la identidad del emisor.

Existen diferentes aspectos a ser verificados, pero siempre será necesario comprobar:

I. **Identidad del sujeto.** La comprobación de la identidad del solicitante es indispensable que se realice en buena forma, ya que es justamente en esta etapa de la emisión del certificado que se da seguridad y certeza de que la persona que se identifica en la Red con dicho certificado es realmente quien dice ser.

   Mientras más precisa sea la forma en que se realiza la comprobación de la identidad de la persona, mayor confianza existirá en el certificado y, consecuentemente, habrá menos posibilidades de rechazo del mismo por los receptores de las comunicaciones electrónicas.

   Existen diferentes técnicas para verificar la identidad del solicitante, dependiendo del grado de certeza con que se quiera dotar a la firma electrónica:

   - **Presencia personal.** Es la forma más segura de verificar la identidad de una persona, toda vez que evita, o al menos se dificulta, la suplantación de la misma.

     Consiste en la comparecencia personal del solicitante ante el prestador de servicios de certificación para que realice, en conformidad con las normas técnicas y sus prácticas de certificación, la verificación de la identidad del solicitante.

     El hecho que el certificador realice la verificación de la identidad del solicitante en la forma debida, no obsta a eventuales conductas delictuales por parte del solicitante y que al no ser fácilmente perceptibles pueden hacer incurrir en un error. Consecuentemente, lo que se persigue es que se utilice la debida diligencia para obtener un resultado certero.

- **Documentos acreditativos.** Consiste en pedir al solicitante de una firma electrónica que proporcione antecedentes escritos que den fe de su identidad.

  Habitualmente, se recurre a documentos que han sido emitidos por datarios de fe pública. Por ejemplo, cédula nacional de identidad, pasaporte, declaración jurada de identidad ante Notario.

  Esta clase de documentación permite obtener información de quien solicita un certificado, sin embargo, no es posible por medio de ella realizar la comprobación fehaciente de la identidad del solicitante, toda vez que, al no cotejar dicha documentación con la presencia física de la persona, puede presumirse que cualquiera pudo obtener dichos documentos y suplantar a quien efectivamente lo es.
- **Confirmación de datos personales por una tercera parte.** Se trata de mecanismos en los cuales la información que es proporcionada por el solicitante, es cotejada por una tercera parte contra una base de datos que se mantiene para dichos fines. Ejemplo, de estas terceras partes, puede ser Equifax con su sistema de información de personas naturales y jurídicas.

  La utilización de esos sistemas deberá estar en armonía con lo preceptuado en la Ley 19.628 sobre protección de la vida privada.
- **Sistemas mixtos.** Se trata de sistemas que combinan las diferentes técnicas señaladas, de manera de satisfacer de mejor forma las exigencias legales y de mercado.

En Chile, los prestadores acreditados de servicios de certificación, para comprobar fehacientemente la identidad del solicitante deberán recurrir necesariamente a sistemas mixtos, donde se exija la comparecencia personal, por mandato del artículo 12 e) de la ley.

c. **Posesión legítima de los datos de creación de firma.** Se trata de verificar que los datos de creación de firma son entregados realmente a la persona que solicitó el certificado de firma electrónica.

Los datos de creación de firma son el medio que permite al titular de la firma suscribir un documento en forma electrónica.

En consecuencia, la persona que se haga de los datos de creación de firma será quien pueda identificarse en la Red con la debida seguridad que otorga el prestador de servicios de certificación.

Por lo anterior, reviste gran importancia que los datos de creación de firma sean efectivamente entregados a su titular, para lo cual se puede recurrir a diferentes mecanismos, los que deberán estar declarados por el certificador en su Práctica de Certificación.

La forma de verificar la posesión legítima de los datos de creación de firma dependerá del sistema de generación de éstos.

Actualmente existen básicamente dos sistemas:

I. **Generación de los datos de creación de firma en el entorno del titular de los mismos**. En este sistema los datos firmantes son generados en el "hardware" o "software" en que serán utilizados y almacenados.

La gran ventaja que representa este sistema es que elimina todo problema que pueda traer aparejada la transferencia segura de los mismos. Es así como se produce una mayor confianza en el sistema, ya que ha sido el propio titular el que los ha generado y nunca ha dejado de tener el exclusivo control sobre ellos.

Sin embargo, representa el problema de no saber si el sistema en que han sido generados realmente cuenta con las suficientes garantías.

Este último aspecto no ha sido abordado por la ley nacional, a diferencia de lo que ocurre con la Directiva Europea sobre Firma Electrónica[92] que exige para la firma electrónica avanzada calificada que se utilicen dispositivos seguros de creación de firma, lo que necesariamente conlleva que tanto el "hardware" como el "software" que se utilice esté debidamente acreditado. Es recomendable que esta exigencia sea incorporada a nuestro sistema.

II. **Generación de los datos de creación de firma en un sistema central. Se** trata de un sistema en que los datos de creación de firma son generados por el prestador de servicios de certificación, por lo que dichos datos deberán necesariamente ser transportados desde el certificador hasta el titular del certificado.

Consecuentemente, en lo que dice relación con la posesión legítima de los datos de creación de firma por el solicitante, el certificador deberá utilizar mecanismos que permitan dar certeza de ello.

Persiguiendo dicho fin, el Reglamento de la ley de firma electrónica dispone, en el artículo 31, que en el caso que los datos de creación de firma *sean generados por el prestador de servicios de certificación, éstos deben ser entregados al usuario o titular del certificado, de manera de garantizar la recepción de los mimos en forma personal*. Para dotar de confianza al sistema y evitar manipulaciones abusivas por parte del certificador, es que la misma norma prohíbe al certificador mantener copias de los datos de creación de firma electrónica una vez que estos hayan sido entregados a su titular.

III. **Otra información verificable.** Como consecuencia de la estructura de los certificados de firma electrónica y de los requerimientos especiales que puede

[92] UNIÓN EUROPEA. 1999. cit. nota n. 86.

tener cada titular de firma electrónica, es que se prevé la posibilidad de la inclusión de menciones o atributos adicionales, situación en la cual se hará necesario que el prestador de servicios de certificación constate la veracidad de las declaraciones que al respecto haya hecho el solicitante.

IV. **Toda información que se incorpore a un certificado de firma electrónica debe ser constatada**, de manera que, en caso de haber menciones extraordinarias, éstas no alteren la cualidad de instrumento identificador.

d. Firma y emisión del certificado. Una vez que se ha efectuado el registro del solicitante y se ha verificado la exactitud de los datos proporcionados, el prestador de servicios de certificación procede a emitir el certificado de firma electrónica, firmándolo por medio de la firma electrónica de la cual es titular.

El certificado de firma electrónica es un documento electrónico que se encuentra firmado por el propio prestador de servicios de certificación.

Ahondaremos en estos aspectos al analizar los certificados de firma electrónica.

e. Publicación y archivo. Emitido y firmado el certificado por el prestador de servicios de certificación, la ley manda en el artículo 12 que conste en un registro de acceso público al que se acceda por medios electrónicos.

Para tales efectos la ley ha autorizado al prestador de servicios de certificación a tratar los datos del titular del certificado (artículo 12 b)). Asimismo, la obligación de archivo consiste en la mantención de los datos que sirven de base a la emisión del certificado, por un período de a lo menos 6 años, contados desde la fecha de la emisión del mismo.

La finalidad de la publicación y archivo es hacer que los certificados estén disponibles para la verificación del estado de las firmas electrónicas.

f. Revocación y suspensión. Los certificados de firma electrónica no pueden tener una validez indefinida, muy por el contrario, la legislación nacional ha previsto, en el

artículo 16 Nº 1, que los certificados tengan un plazo de vigencia que, en ningún caso, excedan los 3 años.

Sin embargo, puede ocurrir que circunstancias como las previstas en la ley o en el Reglamento hagan necesario el término anticipado de la vigencia de un certificado de firma electrónica, temporal o definitivamente.

La revocación del certificado, de acuerdo con el artículo 34 del Reglamento produce "*el cese permanente de los efectos jurídicos de este conforme a los usos que le son propios, impidiendo el uso legítimo del mismo"*. Si el cese es temporal, hay suspensión del certificado conforme al artículo 33 del Reglamento. Produce los mismos efectos que la revocación, pero en un período de tiempo acotado. Una vez que cesa el motivo que la originó el certificado recobra su valor jurídico, y, en caso de que la causa de suspensión se transforme en permanente, el certificado será revocado.

2.5.- Certificados de firma electrónica[93].

De acuerdo con el artículo 2 letra b) de la Ley 19.799, El certificado de firma electrónica es:

> *"Una certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica".*

Se trata de un documento electrónico que da fe de la relación que hay entre el titular de dicho documento y los datos que permiten generarlo.

Del análisis de la ley se puede advertir que, si bien el legislador no adhirió a ninguna tecnología en particular, de manera tal de respetar el principio de neutralidad tecnológica propugnado en el artículo 1º, debió tener a la vista la tecnología que mayoritariamente se

---

[93] Esta sección fue elaborada a partir de un trabajo anterior realizado por mí y que fuera publicado en la Revista Chilena de Derecho Informático. Arrieta, R. 2003. Los prestadores de servicios de certificación de firma electrónica en el derecho chileno. En: Revista chilena de derecho informático. No2 año 2003. [en línea] <http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492,SCID%253D14662%2526ISID%253D292,00.html> [Consulta: 19 de julio 2021].

encuentra disponible en la actualidad, con algunas salvedades conceptuales, a los efectos de redactar la misma.

Es por ello que es habitual oír hablar en los medios especializados que la ley de firma electrónica se basa en un sistema de PKI[94] asimétrica. Si bien ello es cierto, por lo expresado, no es del todo exacto, ya que se tomaron las precauciones necesarias para no reducir la ley a esa tecnología. La razón fundamental de ello es el hecho de que la tecnología avanza de manera más rápida de lo que es posible la adecuación normativa.

Para analizar una firma electrónica avanzada que opera sobre tecnología PKI[95], haremos algunas precisiones, de manera de instruir al lector no lego en la materia y así hacer más sencilla su comprensión.

2.5.1.- Menciones básicas del certificado de firma electrónica.

El artículo 15 de la ley dispone que los certificados de firma electrónica deberán contener, al menos, las siguientes menciones:

a) *Un código de identificación único del certificado.*

b) *Identificación del prestador de servicios de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada.*

c) *Los datos de la identidad del titular, entre los cuales deberán necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y*

d) *Su plazo de vigencia.*

---

[94] Sigla del Inglés "*Public Key Infraestructure*".

[95] También llamada firma digital.

Al respecto, es imprescindible que dichas menciones se encuentren contenidas en los certificados de firma electrónica, sin distinguir la naturaleza de la firma. Este requisito se exige en atención a que la firma electrónica se encuentre respaldada por un certificado. Como consecuencia de lo anterior, lo que permitirá distinguir si el certificado pertenece a una firma electrónica avanzada o no, está dado por la inclusión de los datos de la acreditación del prestador de servicios de certificación y porque el mismo certificado lo señale.

Una cuestión que se presentó como sustantivamente compleja a la hora de estructurar los certificados, sobre la base del estándar internacional X-509 v3, fue la inclusión del RUT, toda vez que se trata de un identificador único que sólo es utilizado en Chile. Adicionalmente, el legislador incurrió en una imprecisión al exigir el RUT (rol único tributario) y no el RUN (rol único nacional), toda vez que ello haría suponer que una persona que no ha iniciado su actividad tributaria no puede adquirir un certificado de firma electrónica, lo que es absolutamente alejado de la voluntad del legislador y de las buenas prácticas que aplican a la materia.

2.5.2.- Límites funcionales del certificado de firma electrónica.

El certificado de firma electrónica podrá establecer límites en cuanto a sus posibles usos, conforme a lo preceptuado en el artículo 14 inciso 3º de la ley. Sin embargo, dichos límites deber ser reconocibles por terceros, como condición de validez de los mismos y la responsabilidad del certificador queda circunscrita al uso que ha sido permitido.

Este aspecto fue desarrollado por el Decreto 181, que contiene el reglamento de la ley de firma electrónica, cuyo artículo 29 inciso 2º, señaló que:

> *"Los atributos adicionales que los prestadores de servicios de certificación introduzcan con la finalidad de incorporar límites al uso del certificado no deberán*

dificultar o impedir la lectura de las menciones señaladas en el artículo 15 de la ley, ni su reconocimiento por terceros".

Con lo anterior, se ha perseguido que no se incorporen menciones a los certificados que limiten el uso de los mismos a comunidades cerradas ya que, si bien se deja abierta la posibilidad de ello, la obligatoriedad de lectura de las menciones básicas permitirá siempre identificarse en la Red con ese certificado de firma electrónica. La limitación funcional estará dada por el uso que se ha permitido, de conformidad con las prácticas de certificación del prestador con quien se ha contratado (artículo 32 del Reglamento) y las condiciones particulares del contrato.

En resumen, la incorporación de límites funcionales a los certificados de firma electrónica debe obedecer a una cuestión contractual entre el certificador y el titular, y no a una cuestión tecnológica que genere barreras de entrada, que puedan estimular el desarrollo de conductas monopólicas que afecten la libre competencia.

2.5.3.- Tipos de certificados en la Ley 19.799.

Del tratamiento que ha hecho la ley del certificado de firma electrónica podemos afirmar que se ha regulado de una manera directa lo que dice relación con los certificados de firma electrónica de identidad.

El certificado de identidad es un documento electrónico, firmado electrónicamente por un prestador de servicios de certificación, que avala la vinculación de los datos de creación de firma con el titular del certificado[96].

Con respecto a quien puede ser titular de un certificado de firma electrónica, se presenta una cuestión de interés, toda vez que la ley no señala de un modo si las personas jurídicas

[96] RIBAGORDA. A. 2002. cit. nota n. 84. p. 1314.

pueden ser titulares de certificados de firma electrónica. Al no estar resuelto de una manera expresa en la ley y partiendo de la base de que en nuestra tradición las personas jurídicas no firman, sino que lo hacen sus representantes legales, deberíamos concluir que éstas no pueden ser titulares de un certificado.

No obstante lo anterior, la duda se robustece con ocasión de los certificados de firma electrónica avanzada, debido a que en el artículo 12 e) de la ley, se impone como obligación al prestador acreditado de servicios de certificación en el otorgamiento de esta clase de certificados, la comprobación fehaciente de la identidad del solicitante, para lo cual deberá requerir previamente, ante sí o ante notario u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal, si se tratare de persona jurídica. En consecuencia, tangencialmente, la ley prevé la posibilidad de que un prestador de servicios de certificación genere un certificado de firma electrónica avanzada para una persona jurídica.

Frente a ello, resulta interesante determinar cuál es la utilidad práctica que puede tener que una persona jurídica cuente con firma electrónica avanzada, toda vez que en el sistema jurídico nacional éstas no pueden actuar sino por medio de su representante legal, lo que traerá consigo la necesidad de que éste también cuente con un certificado de firma electrónica avanzada para actuar en nombre de la persona jurídica. Ello conducirá a que la persona jurídica firme y que posteriormente concurra con su firma el representante legal de la ésta de manera de validar y dar fuerza obligatoria a la manifestación de voluntad.

Otra posibilidad, que es la que parece más razonable, es que en una extensión del certificado de firma electrónica de identidad se incorpore una mención en la que se señale que se está actuando en representación de una persona jurídica, que se especifiquen los poderes, si se requiere de la firma de más de una persona para obligar, etc. Sin embargo, podría llevar a que un mismo certificado tenga numerosas extensiones, ello sin pensar en que una misma persona puede ser representante de más de una persona jurídica.

Adicionalmente, es necesario preguntarse qué ocurre si el titular del certificado deja de ser representante legal de la persona jurídica, o sus poderes son modificados, etc. Ello nos conduciría necesariamente a la revocación del certificado de firma electrónica, generándose en consecuencia la necesidad de adquirir un nuevo certificado.

Con la finalidad de resolver los problemas señalados precedentemente es que se han desarrollado los certificados de firma electrónica de atributos los que, si bien no están contemplados en la ley expresamente, se encuentran completamente ajustados a la misma y podrían, eventualmente, ser considerados como uno de los servicios adicionales que los prestadores de certificación pueden realizar en virtud de lo dispuesto en el artículo 11.

Los certificados de atributos[97] son documentos electrónicos firmados electrónicamente por un prestador de servicios de certificación, que avala la capacidad de actuar en nombre de una persona jurídica, con determinados poderes, etc. Su contenido dependerá de la necesidad de proporcionar información del titular, y siempre requieren del acompañamiento de un certificado de firma electrónica de identidad, sin el cual no tienen virtud alguna. En consecuencia, la persona se identifica por medio de su certificado de firma electrónica, el que puede acompañarse de uno de atributo, que indica, por ejemplo, que se está identificando para actuar en nombre de tal o cual empresa y con tales o cuales poderes.

2.6.- Sellado de tiempo.

Hay innumerables ejemplos que nos muestran la importancia que tiene en nuestra legislación la certeza de la fecha y en algunos casos de la hora. La ley otorga o niega

[97] RFC 3281.

determinados efectos jurídicos a situaciones dependiendo la fecha u hora en que fueron creados, firmados o enviados[98].

El sellado de tiempo aparece como un mecanismo que permite certificar la fecha y hora en que se ha llevado a cabo una transacción electrónica, es decir, a un determinado documento se le asigna, mediante un certificado, una fecha y hora determinada de tal forma que en cualquier momento posterior es posible comprobar[99]:

a. Quién ha firmado el documento, siempre que haya utilizado firma electrónica.
b. Qué día firmó y envió el documento electrónico.
c. A qué hora firmó o envió el documento electrónico.
d. Si al momento de firmar y fechar el documento, el certificado del suscriptor del documento se encontraba vigente (en la medida que se valide con el certificador de la firma electrónica).

El legislador reconociendo la relevancia de tener certeza respecto del momento en que un documento electrónico fue suscrito, sobre todo para que los instrumentos públicos puedan hacer plena prueba respecto de la fecha, fue que en el año 2007 modificó la Ley 19.799 agregando una letra i) al artículo 2º, disponiendo que la fecha electrónica es:

> *"Un conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados".*

De este modo, la fecha electrónica en términos prácticos es un atestado que da un tercero adicionando un certificado de tiempo a un documento electrónico. Así, el objeto del sellado de tiempo es publicitar respecto de cualquier persona el momento en que un documento

[98] DIVIN. F. 2005. El sellado de tiempo en nuestro derecho. Revista Chilena de Derecho Informático. Santiago. Universidad de Chile. p. 78.

[99] DIVIN. F. 2005., cit. nota n. 98, p. 81.

electrónico fue creado o suscrito de manera de darle fecha cierta en el ordenamiento jurídico.

La misma modificación de la ley del 2007 estableció en el artículo 5º Nº2 que si la fecha electrónica es otorgada por un certificado de firma electrónica acreditado el instrumento privado en que ésta se estampe hará plena prueba respecto de su fecha.

A partir de dicha consecuencia jurídica el Ministerio de Economía construyó una interpretación, en nuestra opinión supra legal, de que las certificadoras de firma electrónica debían acreditar el sellado de tiempo, fijando al efecto un conjunto de normas técnicas cuyo cumplimiento debe ser verificado por la Entidad Acreditadora para poder prestar el servicio.

De este modo las certificadoras de firma electrónica acreditadas que deseen proveer el servicio de sellado de tiempo deben acreditar el referido servicio de acuerdo con un conjunto de normas ETSI, ISO, RFC y NIST.

La forma en que se debe demostrar a la Entidad Acreditadora el cumplimiento de las normas se regula en Guía de Evaluación Procedimiento de Acreditación Prestador de Servicios de Certificación Sellado de Tiempo versión 1.0 de 2013, donde la revisión gira en torno a la verificación de requisitos técnicos básicos, seguridad, tecnología, seguridad física, las políticas del certificador para el sellado de tiempo y la forma en que el certificador administra el sellado de tiempo.

A modo de conclusión podemos sostener que el andamiaje jurídico construido por la Ley 19.799 resulta suficiente para dotar de seguridad al comercio electrónico de créditos de consumo, encontrándose las principales dificultades prácticas de su uso en la falta de conocimiento de los operadores jurídicos de esta regulación y a que se encuentra pendiente dotar de mérito ejecutivo a los pagarés electrónicos para mantener la ejecución de las obligaciones incumplidas en una pretensión fundada en un título procesalmente privilegiado.

CAPÍTULO III.- SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES EN LA CONTRATACIÓN ELECTRÓNICA DEL CRÉDITO AL CONSUMO.

Asociado a los créditos de consumo se realiza una profusa actividad de tratamiento de datos personales. En primer lugar, en la solicitud de crédito se realizan operaciones de evaluación de riesgo comercial, luego, en la suscripción se almacenan datos relativos a los documentos que se suscriben por la persona, además de las transferencias y las anotaciones en cuenta de los montos correspondientes. En caso de que existan garantías, se tratarán los datos personales que permitan su establecimiento, y luego en la ejecución posterior, las anotaciones en relación con el pago o no pago de las cuotas correspondientes, morosidades, acciones de cobro forzado, repactaciones, todo ello hasta la conclusión total de la obligación de devolución y cierre del crédito. A estas operaciones de tratamiento de datos directas, se suman otras indirectas, asociadas a los seguros suscritos por la persona o en su nombre, para cubrir los riesgos de muerte, enfermedad o cesantía, en relación con el pago de los saldos pendientes del crédito.

En todas estas operaciones de tratamiento de datos, la seguridad es una de las herramientas o instrumentos de que disponemos para asegurar el respeto a los derechos de la persona frente al tratamiento de sus datos personales. La seguridad abarca varios ámbitos: disponibilidad, autenticación, integridad y confidencialidad[100].

Se trata de un deber que recae sobre los responsables del tratamiento de datos personales consistente en implantar dentro de la empresa una serie de medidas de índole técnicas y organizativas que garanticen la seguridad y protección de los datos personales, evitando así posibles incidencias que puedan provocar su pérdida, alteración o acceso no autorizado a los mismos.

[100] FERNÁNDEZ, C. 2012. En: Revisa de Derecho UNED, núm. 10. Algunos retos de la protección de datos en la sociedad del conocimiento. En especial detenimiento en la computación en nube (Cloud computing). p. 142.

Para definir el régimen jurídico de la seguridad en el tratamiento de datos personales en materia del crédito al consumo es necesario tener en consideración tanto la Ley 19.496, la Ley 19.628 y la Ley 20.575, de cuyo análisis concordado podremos construir la estructura normativa que deberá tenerse en consideración para determinar la forma y medidas que el responsable del tratamiento de datos deberá implantar para tratar de manera leal los datos personales de los titulares que han solicitado un crédito de este tipo.

3.1.- Seguridad y consumidores.

De acuerdo con la Ley 19.496, el derecho a la seguridad es uno de los derechos básicos que le asiste al consumidor en una relación de consumo. De hecho, así es expresamente señalado en el artículo 3 letra d) de la ley que indica lo siguiente:

> "*Son* derechos *y deberes básicos del consumidor: La seguridad en el consumo de bienes o servicios, la protección de la salud y el medio ambiente y el deber de evitar los riesgos que puedan afectarles".*

De la lectura de artículo se desprende que, así como al consumidor le asiste un derecho a la seguridad en el consumo, como contrapartida supone un deber que este mismo ha de satisfacer: evitar los riesgos que puedan afectarles.

Así las cosas, en cumplimiento de este deber, el consumidor debe ser prudente en el uso del servicio, traduciéndose en la responsabilidad de conocer y seguir las instrucciones y advertencias comunicadas por el proveedor[101].

[101] CORRAL, H. 2013. Artículo 3 D). En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile. pp. 109 – 116. pp. 114 - 115.

En el ámbito judicial, a propósito de los deberes de seguridad del consumidor, la Corte de Apelaciones de Santiago[102], confirmando sentencia del Primer Juzgado de Policía Local de Pudahuel, en un caso suscitado a propósito de la apropiación de clave secreta de la cliente y obtención de la clave *digipass* y la posterior realización de la transferencia electrónica por parte de terceros ajenos sostuvo lo siguiente:

> *"Que fue la misma demandante y cliente del Banco la que, descuidadamente, proporcionó los datos necesarios para que terceros ajenos a la institución bancaria pudieran utilizar su cuenta corriente, soslayándose así las condiciones o requisitos de seguridad que el propio Banco dispuso para efectuar transacciones desde dicha cuenta".*
>
> *Lo alegado por el SERNAC implica desconocer el descuido cometido por la misma cliente del Banco quien, a pesar de causarle extrañeza la solicitud de datos personales y secretos mediante un simple correo no personalizado, igualmente proporciona dichos datos permitiendo con ello que desconocidos -tanto para ella como para el Banco- pudieran manipular su cuenta corriente y realizar transferencias electrónicas con sus fondos.*
>
> *Que la conducta antes descrita, en la cual el referido Banco no tuvo participación, deriva de un engaño cuya víctima resultó ser la propia cuentacorrentista, hecho que reviste caracteres delictuales, tal como se ha indicado, que no puede ser enmarcado dentro del ámbito de la ley Nº 19.496.*

[102] PRIMER JUZGADO DE POLICÍA LOCAL DE PUDAHUEL, Sentencia rol Nº 5697-9-2017, de agosto de 2018; En el mismo sentido, CORTE DE APELACIONES DE COYHAIQUE, resolución nº 20, 06-12-2019; Causa nº 77/2019 (P. Local). CORTE DE APELACIONES DE CHILLAN, Resolución nº 15, 17 de enero 2020; JUZGADO DE LETRAS DE LOS ANDES, Sentencia Nº C-372-2012 del 18 de junio de 2013; TERCER JUZGADO DE POLICÍA LOCAL DE TEMUCO, sentencia Rol Nº 20703, 10 de noviembre de 2014; PRIMER JUZGADO DE POLICÍA LOCAL DE ANTOFAGASTA, sentencia Rol Nº 5101-17-7, 19 de julio de 2017.

De acuerdo con CORRAL, el derecho a la seguridad en el consumo, en atención a la historia de la ley, su contexto y, además, la terminología empleada en el Derecho de Consumo a nivel comparado supone la exigencia a los proveedores de que sus productos o servicios no causen daños.

La seguridad impone al producto o servicio el no causar daños o perjuicios, más allá de los derivados de su propia idoneidad para cumplir con el fin al que estaba destinado. Estos daños, de acuerdo con CORRAL, pueden ser en la persona: lesiones corporales, muerte o incluso la aflicción psíquica, o bien en su patrimonio, en caso de resultar menoscabados bienes distintos del producto o servicio[103].

Así, las brechas de seguridad en el *íter* contractual de los créditos de consumo, atendiendo a las características de los servicios implicados, desde luego, no afectará a la persona en los términos expresados por CORRAL. Sin embargo, podría implicar importantes menoscabos en el patrimonio, así como, también, en ámbitos no patrimoniales como, por ejemplo, en materia de privacidad, honra y protección de datos personales, todos derechos constitucionalmente reconocidos en el artículo 19 de la Constitución.

De este derecho a la seguridad para el consumidor se deduce, además y como contrapartida, un deber para el proveedor: brindar seguridad al consumidor. Al respecto, la Corte de Apelaciones de la Serena[104] lúcidamente ha señalado lo siguiente:

> *"Tales derechos, que deben ser entendidos en un sentido amplio, son el correlato de las fundamentales obligaciones del proveedor, como la de velar por la seguridad del consumidor*".

---

[103] CORRAL, H. 2013. cit. nota n. 101. p. 109

[104] CORTE DE APELACIONES DE LA SERENA, Causa Nº 181-2008, Resolución Nº 21.265, de 11 de diciembre de 2008.

La Corte de Apelaciones de Concepción[105], en sintonía con lo anterior, a propósito de una denuncia infraccional por anormalidades en el abono de créditos por internet y transferencias electrónicas, en que incluso se produjo un cambio en el registro de la dirección electrónica del cliente, sostuvo lo siguiente:

> *"Que no puede trasladarse el deber de seguridad en los procedimientos financieros informáticos al cliente, como al parecer se pretende por la querellada, ya que en cuanto a la prevención de fraudes, son los bancos los que deben contar con sistemas o procedimientos que permitan identificar, evaluar, monitorear y detectar en el menor tiempo posible aquellas operaciones con patrones de fraude, de modo de marcar o abortar actividades u operaciones potencialmente fraudulentas, para lo cual deben establecer y mantener, de acuerdo a la dinámica de los fraudes patrones conocidos de éstos y comportamientos que no estén asociados al cliente".*

Luego, otra regla que conviene considerar para la definición del régimen jurídico de la seguridad en el consumo se encuentra en el artículo 23 inciso 1º de la Ley 19.496 que establece el sistema de responsabilidad infraccional de la ley. De acuerdo con este artículo se calificará como infracción a la ley la negligencia en la prestación de servicios que implique, justamente, un menoscabo en la seguridad.

> *"Comete infracción a las disposiciones de la presente ley el proveedor que, en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o a deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio".*

---

[105] CORTE DE APELACIONES DE CONCEPCIÓN, Causa Nº 497/2015. Resolución Nº 123869, de 31 de agosto de 2015.

De acuerdo con este artículo, las deficiencias en seguridad hacen que la aplicación del artículo sea extensiva no solo a productos, sino también a servicios, de manera que las brechas de seguridad en el contexto de la contratación en línea de créditos de consumo, encajaría en el supuesto de hecho del artículo 23 como para ser considerada, además, como una infracción a la Ley 19.496.

Al respecto, CONTARDO, indica que el artículo 23 de la Ley 19.496 se hace extensible, a la seguridad y calidad de los servicios, convirtiendo así a este artículo en la principal fuente de responsabilidad infraccional en la Ley 19.496[106].

En materia de servicios, cabe distinguir entre tres posibles sujetos intervinientes en la cadena de consumo: proveedor, prestador e intermediario.

a. Proveedor es quien ofrece la prestación de servicios a cambio de un precio o tarifa. Lo normal es que coincida con el prestador de servicio.
b. Prestador de servicio es quien materialmente ejecuta el servicio a favor del consumidor.
c. Proveedor intermediario es la figura que se aplica cuando no converge el proveedor con el prestador. Es decir, el proveedor intermediario cobra una tarifa respecto de un servicio que prestará un tercero.

De acuerdo con CONTARDO, a diferencia de lo que ocurre en materia de productos, en el caso de los servicios no se produce el problema de responsabilidad del fabricante, por razones de técnica legal. Esto principalmente porque el proveedor intermediario es contraparte del consumidor en el contrato de consumo, de manera que se aplica la responsabilidad del artículo 43 de la Ley 19.496, o bien, porque prestador y proveedor

[106] CONTARDO, J.I. 2013. Artículo 23 inciso 1º, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile. pp. 556 – 582. pp 563-564.

coinciden de manera que se genera una relación directa de consumo. De acuerdo con estos argumentos, se dice que la responsabilidad por la seguridad recae siempre en el proveedor, sin que sea extensiva a otros sujetos que no sean considerados como tal[107].

A nivel jurisprudencial, a propósito de la aplicación de la responsabilidad infraccional del artículo 23, la cantidad de sentencias es vasta, destacando la sentencia de la Corte de Apelaciones de Santiago de julio del 2010[108] en que, conociendo de una denuncia y demanda por el cobro de un seguro no contratado, en que se demostró que fueron cobrados intereses, impuestos y prima. La Corte indicó lo siguiente:

> *"Que el artículo 23 la Ley 19.496, sobre Protección de los Derechos de los Consumidores, dispone que: "Comete infracción a las disposiciones de la presente ley el proveedor que, en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio", situación que en el caso analizado tiene plena aplicación, considerando que la misma entidad bancaria denunciada reconoció que el problema que afectó al consumidor se produjo por un error y falla operativa".*

La Corte de Apelaciones de Temuco[109], por su parte, en fallo de junio del 2013, a propósito de la clonación de tarjetas, por medio de las cuales se retiró dinero tanto en Chile como en el extranjero, indicó lo siguiente:

> *"Que en el caso sub judice, los giros fraudulentamente efectuados desde la cuenta corriente con chequera electrónica, mediante el retiro de dinero, a través de cajeros automáticos instalados en el país y en el extranjero, constituyen desde el punto de*

---

[107] CONTARDO, J.I. 2013. Cit. nota n. 106. p. 566.

[108] CORTE DE APELACIONES DE SANTIAGO, Causa Nº 915-2010, Resolución Nº 113415, de 14 de julio de 2010.

[109] CORTE DE APELACIONES DE TEMUCO, Causa Nº 73/2013, Resolución Nº 37254, de 19 de junio de 2013.

vista del prestador del servicio la infracción establecida en el artículo 23 de la ley N°19.496, desde que se ha vulnerado la garantía y el debido cuidado en la prestación del servicio contratado, ya que es obligación del banco resguardar debidamente el dinero del cuenta correntista, de manera tal de evitar que éste sea sustraído por terceros, utilizando los sistemas informáticos existentes para ese fin.

Si bien es cierto todo sistema informático es vulnerable, como lo demuestra la ocurrencia diaria de defraudaciones a los sistemas operables con tarjetas magnéticas, el prestador, en este caso, el banco denunciado, en cumplimiento de sus obligaciones contractuales, debió al menos detectar de inmediato el mal uso que se estaba haciendo de la cuenta corriente de la denunciante, desde que en un mismo día se efectuaron tres giros desde el extranjero, sumas por las cuales el banco cargó la comisión correspondiente y dentro del país, retiros que exceden el máximo diario permitido conforme a la propia reglamentación del sistema bancario.

Que así las cosas, no puede sino concluirse que la querellada contravencional, infringió el deber establecido en el artículo 23 de la Ley 19.496, ya que no prestó el servicio comprometido en forma eficiente y segura, tomando, como le correspondía, todas las providencias necesarias a fin de no causar menoscabo económico al usuario del servicio".

La Corte de Apelaciones de Santiago, conociendo a propósito de una denuncia del SERNAC al Banco Santander[110], entre sus considerandos reflexiona en torno a la regla contenida en el artículo 23:

"Que, entonces, el supuesto fáctico de la norma que regula la infracción, expresada en el artículo 23 inciso 1° transcrito, se encuentra constituido por el proveedor que,

[110] CORTE DE APELACIONES DE SANTIAGO, Causa Nº 342/2016, Resolución Nº 660114, de 11 de julio de 2016.

en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio. Esto se traduce en que se parte de la premisa que el proveedor, por la circunstancia de asumir dicha iniciativa, genera la prestación del servicio, lo que permite distinguir claramente dos aspectos esenciales, con consecuencias jurídicas relevantes: 1° La actuación reprochada del proveedor del servicio exige que sea efectuada con negligencia, y 2° Que el menoscabo en el consumidor se provoque debido a fallas o deficiencias del servicio ofrecido.

En este caso, el servicio consiste en el otorgamiento por el Banco Santander de tarjetas de crédito, lo que supone que la entidad bancaria preste el servicio ofrecido sin fallas o deficiencias en cuanto, en lo que aquí interesa, a la seguridad, no solamente cuando se celebra el contrato entre las partes, sino en la relación que se establece después, a propósito de su utilización. Es decir, el servicio no puede prestarse sin los cuidados debidos en relación al uso de la tarjeta de crédito por su titular y por los adicionales, puesto que el proveedor, si actúa con negligencia, causando menoscabo al consumidor, puede generar, además de incurrir en una infracción a esta norma legal, en responsabilidad del proveedor hacia el consumidor".

En otro caso conocido por la Corte de Apelaciones de Santiago[111] a propósito de una clonación de tarjetas indicó lo siguiente:

"Efectivamente se ha visto afectado el derecho a la seguridad en el consumo, infracción prevista en los artículos 3° inciso 1° letra d) y 23 de la Ley N° 19.946, desde que las entidades bancarias, atendida la especialidad y complejidad de las

[111] CORTE DE APELACIONES DE SANTIAGO, Causa Nº 1484/2015. Resolución Nº 185742 de marzo de 2016.

operaciones de carácter económico que conforman su giro, deben contar con las herramientas tecnológicas que sean necesarias para evitar los fraudes, en el caso en comento, la clonación de un plástico, a fin de evitar que se verifiquen transacciones que perjudiquen los intereses patrimoniales de sus clientes y, asimismo, con mecanismos que le permitan identificar las tarjetas utilizadas en los giros o compras a objeto de probar su propia afirmación en orden a que ella habría sido usada por el *cliente y no por un tercero, dado que la prueba contraria resulta imposible de obtener para el consumidor; exigencias cuya satisfacción no fue acreditada en el caso que nos ocupa por la denunciada".*

La Corte de Apelaciones de Coyhaique, en fallo de julio de 2017[112], a propósito de una denuncia infraccional en contra del Banco BCI, por mantener en el boletín comercial la deuda de un cliente que ya fue pagada. Al respecto, y a propósito de la aplicación del artículo 23, la Corte indicó lo siguiente:

"Como la ley protege la seguridad respecto del servicio, cuando éste es defectuoso se origina precisamente una responsabilidad infraccional, pues el perjuicio es causado en la persona del consumidor debido a que el banco suministrador del producto, en este caso, el Banco de Crédito e Inversiones, quién emitió la tarjeta de crédito que ocasionó los perjuicios, debe responder si ha actuado con negligencia, y evidentemente que al no haber comunicado al boletín comercial, en la oportunidad en que fue cancelado por su cliente una deuda pendiente, y al hacerlo casi un año después, ese actuar ha sido con negligencia pues durante todo ese tiempo el consumidor figuraba en el Dicom con una deuda pendiente la cual se encontraba pagada, y como el ámbito de aplicación del artículo 23 de la Ley del Consumidor se hace extensible a la seguridad y calidad en los servicios, naturalmente el prestado

[112] CORTE DE APELACIONES DE COYHAIQUE, Causa Nº 14/2017, Resolución Nº 5508 de 18 de julio de 2017.

por la señalada entidad bancaria se hizo con medidas que resultaron atrasadas en el tiempo e inadecuadas para la condiciones de seguridad que el servicio requería, resultando el cliente afectado por tales riesgos al no adoptarse las providencias adecuadas".

La Corte de Apelaciones de Arica, en fallo de junio de 2012[113], ante una demanda infraccional en contra del Banco Estado por la realización de un traspaso no autorizado de $1.000.000.- a una chequera electrónica de un tercero desconocido por el cliente, se ha encargado de definir qué ha de entenderse por "negligencia" de manera que resulte aplicable el artículo 23 de la Ley 19.496.

"Que de los hechos ya establecidos, no cabe sino concluir que el Banco Estado infringió el articulo 23 recién transcrito, toda vez que en la prestación del servicio de cartola electrónica contratado con la denunciante, actuó con negligencia causándole con ello un menoscabo a esta, debido a fallas en la seguridad del servicio contratado.

Que por otra parte, es dable tener presente que, al no haber definido la ley Nº 19.496, que debe entenderse por "negligencia", debemos recurrir a las normas de interpretación establecidas en el artículo 20 del Código Civil, esto es, que debemos entender dicho concepto en su sentido natural y obvio, según el uso general de dicha palabra, y tal sentido está dado por el Diccionario de la Lengua Española de la Real Academia Española (sic), el cual define "negligencia" como "descuido, omisión" y "falta de aplicación", estimando estos sentenciadores que el Banco demandado actuó con falta de aplicación al no poder dar una respuesta satisfactoria del destino de los fondos que fueron traspasados desde la cuenta de la demandada, no obstante ser un hecho público y notorio que dicha entidad cuenta con un sistema informático

[113] CORTE DE APELACIONES DE ARICA, Causa Nº 24/2012, Resolución Nº 6714, el 20 de junio de 2012.

conectado a través de todo el país, el cual le permite detectar en forma inmediata las transacciones efectuadas en cada una de las cuentas que dicha institución bancaria mantiene".

Por último, y en un fallo más reciente, la Corte de Apelaciones de Santiago, en diciembre del 2020[114], conociendo a propósito de un caso de *Phishing*[115] en que la víctima, al entrar a una página que aparentemente era del Banco de Chile, en circunstancias que, en verdad, era un portal falso en el cual mientras ingresaba sus datos en la verdadera página estaban actuando delincuentes que sustrajeron más de $7.000.000.

Ante este caso, el banco se defendió argumentando que fue la víctima quien en una página falsa ingresó su *digipass*, siendo así víctima de un fraude en el cual el Banco no tuvo participación ni responsabilidad alguna. Al respecto la Corte indicó lo siguiente:

"Que el proveedor no puede asilarse para desligar su responsabilidad en que fue el titular de la cuenta quién cursó los giros, el proveedor mantiene su obligación de actuar con la debida diligencia y cuidado, de manera seria y responsable, tomando todas las medidas para evitar que sus clientes-consumidores sean víctimas de delincuentes que logren materializar sucesivas transacciones en un reducido lapso de tiempo, sin que se verifique la legitimidad de las mismas y más aún se niegue a proporcionar datos que permitan perseguir a los defraudadores.

Que, así las cosas, el Banco no ha cumplido con su deber de cuidar los intereses de su cliente, puesto que le es exigible tomar todas las medidas necesarias para evitar este tipo de operaciones, ya que es quién tiene los medios y recursos para velar por

---

[114] CORTE DE APELACIONES DE SANTIAGO, Causa Nº 28-2019, diciembre de 2020.

[115] Método que los ciberdelincuentes utilizan para engañar y conseguir que se revele información personal, como contraseñas, datos de tarjetas de crédito o de la seguridad social y números de cuentas bancarias, entre otros.

los intereses de quienes confiaron en su sistema operativo y que, en el evento de producirse una operación como la que nos ocupa, asuma la responsabilidad que le cabe como proveedor del servicio y sea coadyuvante con el cliente en la investigación".

Luego, el párrafo 5 del Título III de la Ley 19.496 se hace cargo de regular las disposiciones relativas a la seguridad tanto de productos como servicios.

Entre las reglas contenidas en este párrafo está el artículo 45, en cuyo inciso 2 hace referencia a las medidas necesarias para que la prestación de servicios se de en condiciones de seguridad adecuadas.

"En lo que se refiere a la prestación de servicios riesgosos, deberán adoptarse por el proveedor las medidas que resulten necesarias para que aquélla se realice en adecuadas condiciones de seguridad, informando al usuario y a quienes pudieren verse afectados por tales riesgos de las providencias preventivas que deban observarse".

La ley no define qué ha de entenderse por "servicio riesgoso". Sin embargo, de acuerdo con el Diccionario de la Real Academia Española, que algo sea "riesgoso" implica, entre otras cosas, *que entrañe contingencia o proximidad de un daño.* De la misma forma, al definir la noción de "riesgo" indica que se trata de la "*contingencia o proximidad de un daño".*

Luego, como indicamos anteriormente, los daños no necesariamente se refieren a lesiones corporales o la muerte, el daño también puede tener implicancias en la afección a derechos fundamentales, así como, también, tener consecuencias patrimoniales.

BARROS, a propósito de los servicios riesgosos ha sostenido que los servicios no se encuentran usualmente cubiertos por los estatutos especiales de protección del consumidor. Sin perjuicio de ello, la ley chilena de derecho de consumo ha incluido los servicios riesgosos en su disposición relativa a la seguridad. En analogía con la peligrosidad

de los productos, dice BARROS, puede entenderse que bajo la noción de servicios riesgosos se encuentran aquellos que amenazan entre otras cosas, la seguridad de sus bienes.

El prestador de estos servicios riesgosos tiene el deber de informar respecto de las condiciones de seguridad, dando a conocer las medidas preventivas necesarias a quienes pudieren verse afectados[116].

Si bien a primera vista podría no considerarse como tal, de la lectura del artículo 45, en concordancia con las definiciones de la Real Academia Española consideramos que no es del todo descabellado calificar los servicios bancarios como riesgosos, toda vez que, de no tomarse las medidas de seguridad adecuadas puede acarrear contingencias lamentables tanto a nivel económico como también en ámbitos no patrimoniales como sería en materia de privacidad, honra y protección de datos personales de los clientes afectados. En tal sentido, indica CORRAL, que para hacer efectiva la responsabilidad del proveedor habrá que acreditar la negligencia, la cual corresponde a la no adopción de medidas que resulten necesarias para la prestación del servicio en adecuadas condiciones de seguridad, o en caso de omitirse la información al usuario y terceros afectados respecto de las medidas preventivas que debían observarse[117].

Además, a los proveedores de servicios bancarios y financieros se les exige, ex ante, altos estándares de diligencia en materia de seguridad de acuerdo con la ley. A este respecto, CORRAL, sostiene que, para la prestación de servicios, la ley también obliga al proveedor a minimizar los riesgos que estos puedan ocasionar. Se refiere precisamente a aquellos

---

[116] BARROS. E. 2006. Tratado de Responsabilidad Extracontractual. Santiago, Editorial Jurídica de Chile, 1364p. p. 758.

[117] CORRAL, H. 1999. Ley de protección al consumidor y responsabilidad civil por productos y servicios defectuosos. En: Cuaderno de Extensión Jurídica: Derecho del Consumo y Protección del Consumidor (3), Universidad de los Andes. pp. 163 – 212. p. 197.

servicios que ordinariamente son susceptibles de ocasionar daños a los usuarios o a terceros. De allí la calificación de servicios o productos "riesgosos".

La obligación del proveedor en estos casos, y de modo similar a lo que se hace respecto de los productos, se refiere a la información que debe darse tanto al usuario como a los terceros que pudieran verse afectados respecto de las providencias preventivas que deben observarse para precaver los daños.

Sin embargo, de acuerdo con CORRAL, este deber de información no es suficiente. El proveedor, además, ha de adoptar las medidas que resulten necesarias para que la prestación de servicios se realice en condiciones de seguridad adecuadas. El juicio de adecuación deberá tomar en cuenta la utilidad del servicio y los riesgos inherentes a la actividad[118].

Luego, cabe tener presente que el inciso final del artículo 45 dispone multas de hasta 2.250 Unidades Tributarias Mensuales (UTM) en caso de que se incumpla el deber de informar y adoptar medidas de seguridad para los productos peligrosos y servicios riesgosos.

> *"El incumplimiento de las obligaciones establecidas en los dos incisos precedentes será sancionado con multa de hasta 2.250 unidades tributarias mensuales".*

A continuación, el siguiente artículo al que conviene prestar atención para definir el régimen regulatorio de la seguridad en el consumo en el contexto de la contratación de créditos de consumo es el artículo 46 de la Ley 19.496, el cual se hace cargo de definir los deberes del proveedor, de los cuales en este punto nos interesa el deber de dar aviso oportuno en caso de brechas de seguridad y la existencia de peligros o riesgos no previstos oportunamente.

---

[118] CORRAL, H. 2013. Artículo 45, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile, pp. 925 - 928. p. 925.

"Artículo 46.- Todo fabricante, importador o distribuidor de bienes o prestador de servicios que, con posterioridad a la introducción de ellos en el mercado, se percate de la existencia de peligros o riesgos no previstos oportunamente, deberá ponerlos, sin demora, en conocimiento de la autoridad competente para que se adopten las medidas preventivas o correctivas que el caso amerite, sin perjuicio de cumplir con las obligaciones de advertencia a los consumidores señaladas en el artículo precedente".

De acuerdo con CORRAL, la ley establece que los sujetos obligados a adoptar medidas de prevención, corrección o advertencia, respecto de los bienes o productos, el fabricante, el importador y el distribuidor y, respecto de los servicios, el obligado es el prestador de los mismos.

La norma impone la obligación, en la medida en que los sujetos responsables, "se percaten" de la existencia de riegos no previstos oportunamente. Bastaría, por lo tanto, con que aparezca la probabilidad o a veces incluso la simple posibilidad de que se genere el daño para que el proveedor esté obligado a adoptar las medidas preventivas, correctivas o de advertencia[119].

Entre las medidas de prevención o corrección, los sujetos obligados deben, en primer lugar y sin demora, poner en conocimiento de la autoridad competente los riesgos sobrevinientes que se temen, a fin de que esta autoridad adopte las medidas preventivas o correctivas que el caso amerite.

Al respecto se advierte que la ley no precisa cuál es la autoridad competente. Su determinación, de acuerdo con CORRAL, correspondería a la naturaleza del bien o servicio

[119] CORRAL, H. 2013. Artículo 46, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile, pp. 929 - 932. pp. 930 – 931.

de que se trate y a las regulaciones especiales que existan sobre ellos[120]. Así, para el caso que motiva este estudio la autoridad competente sería la Comisión para el Mercado Financiero (CMF) al ser la autoridad a cargo de velar por la adopción de medidas tanto correctivas como preventivas.

Adicionalmente, el artículo 46 hace mención del cumplimiento de obligaciones de advertencia a los consumidores.

En materia de servicios como los que se analizan en este estudio, la norma puede concebirse, de una parte, como que el servicio podrá seguir contratándose, incorporándose las advertencias correspondientes para que su prestación impacte lo menos posible en la seguridad de los consumidores o usuarios. De otra parte, la norma puede entenderse en el sentido de que, una vez que ha iniciado la prestación del servicio, se advierta a los consumidores y usuarios respecto de los riesgos descubiertos para que se adopten las medidas especiales de cuidado en atención a los riesgos[121].

Por último, la norma que cierra el régimen jurídico de la seguridad en el consumo es el artículo 47, el cual define la responsabilidad civil que se produce para el prestador del servicio ante el caso daños o perjuicios ocasionados al consumidor por infringirse los deberes de seguridad.

> *"Declarada judicialmente o determinada por la autoridad competente de acuerdo a las normas especiales a que se refiere el artículo 44, la peligrosidad de un producto o servicio, o su toxicidad en niveles considerados como nocivos para la salud o seguridad de las personas, los daños o perjuicios que de su consumo provengan serán*

[120] CORRAL, H. 2013. cit. nota n. 119, p. 931

[121] CORRAL, H. 2013. cit. nota n. 119, p. 932.

de cargo, solidariamente, del productor, importador y primer distribuidor o del prestador del servicio, en su caso.

Con todo, se eximir de la responsabilidad contemplada en el inciso anterior quien provea los bienes o preste los servicios cumpliendo con las medidas de prevención legal o reglamentariamente establecidas y los demás cuidados y diligencias que exija la naturaleza de aquellos".

Este precepto aborda la responsabilidad civil que se ocasiona cuando un servicio riesgoso causa daños a los consumidores o usuarios u otras personas relacionadas.

En el derecho comparado esta responsabilidad se trata dentro de la responsabilidad por productos defectuosos. Se advierte así que el producto peligroso no genera un régimen especial de responsabilidad en cuanto tal, sino que, al igual que los productos no peligrosos, cuando adolece de un defecto que lo vuelve inseguro, en el sentido de que no ofrece la seguridad que podría legítimamente esperarse de él. Es una forma de responsabilidad estricta u objetiva, pero calificada por el defecto. La víctima no debe probar culpa, pero sí que el producto era defectuoso y que entre el defecto y el daño media un nexo de causalidad.

Este régimen especial se aplica a los productos, pero no a los servicios. Los servicios son sometidos, normalmente, a las reglas generales de la responsabilidad civil fundadas en la falta de deberes de cuidado que generan culpa o negligencia.

La norma chilena, sin embargo, se aplica tanto a los productos como a los servicios pero que sean calificados como peligrosos o tóxicos. La responsabilidad por los daños causados se desmarca sólo parcialmente del factor de imputación basado en la culpa[122].

[122] CORRAL, H. 2013. Artículo 47, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile, pp. 925 - 928. p. 925.

De este modo, los criterios jurisprudenciales en materia de seguridad del consumo pueden ser sintetizados en los siguientes términos:

Artículo 3 letra d) Son derechos y deberes básicos del consumidor: La seguridad en el consumo de bienes o servicios, la protección de la salud y el medio ambiente y el deber de evitar los riesgos que puedan afectarles.	• Seguridad como deber del consumidor de evitar riesgos que puedan afectarle. (C.A. Santiago, causa 5697-9-2017; C.A. Coyhaique, causa 77-2019; C.A. Chillán, causa 15; Juzgado de letras de Los Andes, sentencia C-372-2012; Tercer Juzgado de Policía local Temuco, sentencia 20703; Primer Juzgado de Policía local de Antofagasta, sentencia 5101-17-7).
	• La seguridad como deber del proveedor de brindar seguridad al consumidor. (C.A. La Serena, causa 181-2008). • En la prevención de fraudes, son los bancos los que deben contar con sistemas adecuados. (C.A. de Concepción, causa 497-2015).

Artículo 23. Comete infracción a las disposiciones de la presente ley el proveedor que, en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o a deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio.	• Misma entidad bancaria ha reconocido que el problema se produjo por error y falla operativa (C.A. Santiago, causa 915-2010). • Giros fraudulentos en cajeros automáticos constituyen una infracción al debido cuidado en la prestación del servicio. (C.A. de Temuco, causa 73-2013). • El supuesto fáctico del artículo supone 1. Que la actuación reprochada sea efectuada con negligencia y 2) que el menoscabo al consumidor se provoque por esa falla o deficiencia. (C.A. de Santiago, causa 342-2016). • Entidades bancarias, atendida su especialidad y complejidad deben contar con herramientas tecnológicas para evitar fraudes. (CA. Santiago, causa 1484-2015).

3.2. Seguridad y protección de datos personales.

La seguridad se cierne como uno de los principios que configuran el contenido esencial de la protección de datos. Al respecto, el artículo 11 de la Ley 19.628 dispone lo siguiente:

> "*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".*

Sin embargo, la ley, alejándose del estándar internacional, no consagra los requerimientos de cuidado o medidas concretas que los responsables del tratamiento de datos deban

adoptar con el fin satisfacer el principio de manera que permita velar por la seguridad de los datos o para prevenir su daño.

Así las cosas, se ha dicho que la obligación de seguridad, en conformidad a la ley vigente, se basaría en la noción de "debida diligencia" construida en torno a la noción del "buen padre de familia", lo cual acarrea que el responsable del tratamiento responda de culpa leve al implementar medidas de seguridad[123].

Así, serán los tribunales los llamados a definir, caso a caso, si se han tomado las medidas suficientes para satisfacer el principio de seguridad[124]. Será el tribunal el llamado a determinar lo que haría un hombre o una mujer razonable en una situación particular para encontrar la seguridad de los demás. Para ello, resulta indispensable comprender las amenazas y riesgos actuales asociadas a las operaciones de tratamiento de datos personales que se están realizando, de manera de poder determinar las medidas de seguridad que permiten protegerse contra dichas amenazas y riesgos.

En el contexto jurisprudencial, a propósito de la debida diligencia en la aplicación de medidas de seguridad, los tribunales nacionales se han pronunciado al respecto en pocas ocasiones.

En un caso conocido por el 16º Juzgado Civil de Santiago (C-29221-2015) se condenó a un banco a indemnizar por daño moral a 3 clientes por el abandono en la vía pública de documentos en cuyo contenido había datos personales.

---

[123] JIJENA, R. 2002. Comercio electrónico, firma digital y derecho: Análisis de la Ley 19.799. Santiago, Editorial Jurídica de Chile, 467p. p. 86.

[124] VIOLLIER, P. 2017. El estado de la protección de datos personales en Chile [en línea], Santiago, Derechos Digitales, <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf> p. 23. [consulta 5 de marzo 2021].

De acuerdo con el razonamiento del Juzgado, se habría infringido la obligación de seguridad que establece el artículo 11 de la Ley 19.628.

> *"Undécimo: Que el Banco Santander Chile, en el curso de las actividades de su giro, recibe y almacena una gran cantidad de datos personales y sensibles de sus clientes o solicitantes. Mantiene información de contacto personal, como domicilios, correos electrónicos y teléfonos, información financiera, como estados de cuenta, de créditos e historial de pagos, e incluso datos sensibles, como información referida a la composición de la familia, datos laborales y educacionales, tanto de sus clientes, por ejemplo, cuentacorrentistas, como de personas que no son más que meros solicitantes, personas que quieren optar a un crédito y buscan opciones entre distintos Bancos, por ejemplo. En conjunto, Banco Santander Chile, notoriamente uno de los más grandes del país, cuenta con un vasto banco de datos sobre una multitud de personas.*
>
> *Como banco de datos, está dentro del ámbito de aplicación de la Ley 19.628, la cual lo obliga a observar una debida diligencia respecto a los datos que recopila, desde su almacenamiento hasta su destrucción o cancelación, incluyendo todo tratamiento de datos que ocurra en el intertanto. Tiene el deber institucional de dar pleno cumplimiento en el artículo 11 de la citada ley, de esta forma, aun cuando los documentos hayan sido tomados por error por parte del chofer (quien luego además incumpliría su propia obligación de depositar los escombros encomendados en un vertedero autorizado), correspondía al Banco Santander Chile la obligación de tener el cuidado suficiente con los datos personales y sensibles de sus clientes de tal forma que fuese imposible que se produjese la confusión alegada.*
>
> *Sobre este particular, el hecho que una persona haya podido confundir cajas con documentos sensibles con escombros da cuenta de negligencia en el almacenamiento de los mismos, ya que no se encontraban resguardados*

debidamente y, aun en el caso que estuviesen dispuestos para destrucción, como el mismo absolvente del banco declara, no estaban trituradas, sino íntegras y por tanto, legibles y accesibles.

En otras palabras, la cadena de actos que culminó con los documentos que contenían información privada de los demandantes se inicia por el descuido del banco, esto es, habría sido imposible que acabaran en un basural clandestino en la Cuesta Barriga si Banco Santander Chile hubiese tratado los papeles en cuestión con la diligencia esperable de una institución importante que trabaja con datos sensibles. El dejar cajas con papeles íntegros con información privada, junto con escombros y basura de una remodelación, está lejos de aquello que la experiencia de un hombre medio dicta como adecuado o correcto".

Otro caso, del ámbito laboral, conocido por el Juzgado de Letras del Trabajo de Calama (2018 RIT T-60-2018) a propósito de la filtración de datos personales de un trabajador a través de una publicación en Internet de una captura de pantalla extraída del sistema de la empresa implicó, de acuerdo con el tribual, la infracción al estándar del artículo 11 de la Ley 19.628.

"*Undécimo: Que, en definitiva, conforme a lo expuesto se ha logrado acreditar que el demandado incumplió con la obligación de seguridad establecida en el artículo 11, toda vez que es posible advertir la falencia en el sistema SAP, además de la deficiente investigación que pudo advertir la Inspección del Trabajo, toda vez que el informe de investigación que tuvo a la vista el organismo fiscalizador mantenía una serie de falencias formales, conforme se indicó en el considerando octavo, además del hecho que el demandado contaba con un universo más limitado, esto es, entre 13 o 14 personas y no los 294 trabajadores que indicó para efectos de determinar el responsable de la filtración de información al que se vio afectado el demandante y*

que, por lo demás, no solamente aquél, sino a otro trabajador conforme lo advierte la propia investigación".

De la revisión de la Ley 19.628, artículos 7 y 11, se colige que el responsable del tratamiento, para dar cumplimiento tanto a los deberes de seguridad como a los de secreto y confidencialidad respecto de los datos tratados, necesariamente deberá tomar las medidas adecuadas conducentes a satisfacer las obligaciones de seguridad y confidencialidad. El problema está, como se ha dicho, en que la ley no se hace cargo de mencionar cuáles serían las medidas o estándares a adoptar, lo que lleva a la necesidad de efectuar una ponderación del tratamiento y de los intereses en juego.

De acuerdo con BENUSSI[125], las principales críticas que se puede hacer a la Ley 19.628 por estructurar las obligaciones de seguridad sobre la base del estándar de debida diligencia son las siguientes:

1. **Ausencia de una obligación que requiera establecer medidas concretas y precisas de seguridad por parte del responsable**, que atiendan a criterios mínimos como el estado de arte, los costos de implementar medidas, la naturaleza de los datos personales, el tipo de tratamiento o a los posibles riesgos que éste conlleva. El estándar actual supone una evaluación caso a caso por los tribunales, en la que los jueces no tienen parámetros específicos de control. En una sociedad en que los tratamientos de datos son cada día más complejos, es necesario entregar herramientas sobre las cuales los responsables, jueces y la eventual autoridad

[125] BENUSSI, C. 2020. Obligaciones de Seguridad en el Tratamiento de Datos Personales en Chile [en línea] Revista Chilena de Derecho y Tecnología, Vol. 9 N° 1 <https://webcache.googleusercontent.com/search?q=cache:5r3oYSyqCbgJ:https://revistas.uchile.cl/index.php/RCHDT/article/download/56660/61350/+&cd=9&hl=es-419&ct=clnk&gl=cl> [consulta 13 de febrero 2021]

administrativa, puedan aterrizar el estándar requerido, de modo de aplicar y calificar correctamente la obligación de seguridad.

2. **Ausencia de obligaciones asociadas al reporte de vulneraciones que afecten medidas de seguridad a una autoridad o a los titulares de datos afectados,** de forma que puedan tomar aquellos resguardos que permitan atenuar los efectos adversos derivados de la vulneración.
3. **Ausencia de la posibilidad de que los titulares exijan a los responsables la aplicación de medidas de seguridad específicas** para garantizar la seguridad de los datos tratados.
4. **Ausencia de obligaciones de seguridad particulares para el mandatario o encargado que trata los datos personales** en lugar y nombre del responsable del banco de datos.
5. **Ausencia de un principio de seguridad que inspire el tratamiento de los datos personales** por los responsables del banco de datos y los mandatarios.

Así las cosas, se advierte que la Ley 19.628 presenta importantes vacíos respecto a las obligaciones de seguridad, generando que, en la práctica, el establecimiento de medidas de seguridad adecuadas y robustas para el tratamiento de datos personales en Chile se configure como un acto cuasi voluntario cuya inobservancia no tiene consecuencias adversas, o las probabilidades de que ellas se materialicen son muy reducidas dado el estatuto jurídico vigente, la falta de adhesión al tema de los operadores jurídicos y el costo transaccional que importa accionar judicialmente.

Sin embargo, a partir del derecho comparado y los estándares internacionales en materia de seguridad de la información, es perfectamente posible establecer que la seguridad se logra mediante la implementación de medidas de seguridad destinadas a lograr la instauración del triángulo CID: Confidencialidad, Integridad y Disponibilidad. Así, todos los controles de seguridad, los mecanismos y las salvaguardias se aplican para asegurar uno o más de estos elementos, y al mismo tiempo, todos los riegos, amenazas y vulnerabilidades

se miden por su potencial capacidad para comprometer uno o todos los elementos del triángulo CID.

La confidencialidad, también llamada exclusividad, se refiere a los límites en cuanto a quién y a qué tipo de información se puede acceder. La confidencialidad garantiza que se aplique el nivel necesario de privacidad en cada elemento de procesamiento de datos y previene la divulgación no autorizada. El nivel de confidencialidad debe prevalecer mientras que los datos residan en los sistemas y dispositivos de la red, cuando se realice la transmisión, y una vez que llegue a su destino[126].

La integridad se refiere a estar completa o ser coherente con un estado previsto de la información. Cualquier modificación no autorizada de los datos, ya sea deliberada o accidental, es una violación de la integridad de los datos. Integridad significa que la información es original, completa e intacta (no necesariamente correcta). Significa que no se ha perdido nada de información, está completo y tal cual como fue generada[127].

Por último, la Disponibilidad tiene que ver con que la información sea oportuna (está disponible cuando se le necesite), continua (el personal puede seguir trabajando en caso de una falla) y robusta (hay capacidad suficiente para permitir trabajar a todo el personal en el sistema o aplicación)[128].

Finalmente, complementando el triángulo CID se suele agregar como elemento integrante del principio de seguridad el deber de que los sistemas mantengan un registro de las operaciones que se realizan sobre ellos, de forma que siempre se pueda conocer quién ha accedido a los datos, qué datos se han modificado y qué valores han sido reemplazados por

---

[126] COLUMBA, E. 2016. Fundamentos de Seguridad de la Información basados en ISO 27001/27002: Guía de referencia para rendir el examen de Fundamentos de Seguridad de la Información basado en ISO/IEC 27002. Kindle, Posición 235 de 2919.

[127] COLUMBA, E. 2016., cit. nota n. 126, Posición 263 de 2919.

[128] COLUMBA, E. 2016., cit. nota n. 126, Posición 299 de 2919.

otros nuevos. No solamente hay que ser honrado, sino que hay que poder demostrarlo. Si no existiera un sistema de prueba o verificación en el tratamiento de un fichero de datos personales, no habría forma de demostrar que unos datos incorrectos no han sido manipulados fraudulentamente, sino que habían sido inicialmente grabados con esos valores. Este aspecto de la seguridad implica la grabación en ficheros de acceso de todas las operaciones que se realicen sobre los datos, haciendo constar la fecha, hora, identificador del operador o proceso, contenido de los datos visualizados y contenido, si lo hubiese, de los nuevos valores actualizados[129].

Así, la obligación para el responsable del tratamiento de datos reside en implantar medidas de seguridad, de orden técnico y organizativo, que permitan garantizar la seguridad y protección de los datos personales tratados en las diferentes operaciones de manera de evitar los posibles incidentes que puedan provocar la pérdida, alteración o acceso no autorizado a los mismos y, al mismo tiempo, pudiendo demostrar la forma en que se han realizado todas las operaciones de tratamiento de datos.

En consecuencia, queda en evidencia que la diligencia ordenada por la ley para quien trata datos personales está dotada de un contenido que dependerá en el caso concreto de la situación en la cual se encuentre el responsable del tratamiento de los datos y de la habitualidad con que efectúe las operaciones de tratamiento de datos, siéndole exigibles medidas de seguridad más sofisticas en la medida que haya habitualidad, se trate de grandes volúmenes de datos tratados y la sensibilidad que puedan tener los datos tratados. Dicho en términos muy simples, aun cuando la ley no ordene medidas de seguridad específicas a partir de la posible afectación de derechos a causa de la posible pérdida, alteración o acceso no autorizado a los datos a partir de los estándares internacionales es

[129] TRONCOSO. A. 2009. La declaración de los ficheros de datos personales: acerca de un modelo centralizado o descentralizado. Revista de la Agencia de Protección de Datos de la Comunidad de Madrid. Madrid. Agencia de Protección de Datos de la Comunidad de Madrid, Seguridad y Protección de Datos Personales (38). p. 52.

posible definir el tipo de medidas de seguridad que debe cumplir el responsable para demostrar en sede judicial la debida diligencia.

Así, el hecho de que la ley no señale cuáles son las medidas de seguridad que deben cumplir los responsables del tratamiento, ello está lejos de significar que éstos no deben cumplir con ellas o que no pueda ser posible prever que medidas deben ser aplicadas para asegurar que los derechos de las personas no se vean afectados a causa de la pérdida, alteración o acceso no autorizado a los datos.

Así, la diligencia debida importa la necesidad de adoptar todas las medidas de seguridad necesarias para para garantizar la confidencialidad, integridad y disponibilidad de los datos y con ello evitar la afectación de derechos por las operaciones de tratamiento de datos realizadas, siendo en consecuencia exigida una obligación de resultado. Para ello, se deberá tener en cuenta el estado de la técnica, los costos asociados a la implementación, y la posible afectación de los derechos y libertades de las personas y el rol del responsable y el encargado del tratamiento[130].

Lo anterior cobra especial importancia para el tratamiento de datos personales de carácter económico, financiero, bancario o comercial, dado que la Ley 20.575 establece que la forma en que el responsable del tratamiento de los datos implemente el principio de seguridad será una cuestión que deberá ser considerada por el juez como un antecedente para determinar si existió la debida diligencia en el tratamiento de datos personales, siendo deber del responsable probar ante el juez que dio cumplimiento a las obligaciones de seguridad y que actuó con la debida diligencia en el tratamiento de los datos respectivos.

[130] Estos criterios son los considerados por el artículo 32 del Reglamento General de Protección de Datos de la Unión Europea y determinan aquellos que deben tenerse en consideración a los efectos de elegir las medidas de seguridad a ser implementadas.

En cuanto a la protección de los datos personales aplicada específicamente en el ámbito de la contratación de créditos de consumo, el artículo 37 establece los aspectos mínimos a informar por parte del proveedor al consumidor.

Esto es de suma importancia toda vez que a nivel jurisprudencial se ha concebido como información básica comercial, así por ejemplo la Corte de Apelaciones de Temuco ha sostenido que la información a entregar en cumplimiento del artículo 37 ha de entenderse como información básica comercial.

> *"12º) Que, en cambio, analizados los antecedentes documentales aportados por la querellante y actora civil, y el Sernac, se puede concluir inequívocamente que la querellada incumplió con las obligaciones que le imponen los artículos 23 inciso primero, 37 y 58 de la ley N. 19.496, en especial con proporcionar la información básica comercial que le requirió el querellante y el Sernac, en lo que atañe a las condiciones en que se ejecutaba el contrato de crédito en cuestión y la justificación de los cargos efectuados luego del pago adelantado del total de lo adeudado por parte de la cliente.*
>
> *13º) Que conforme con lo que se lleva relacionado, y ponderando los documentos acompañados por la querellante y demandante civil y el Sernac según las reglas de la sana crítica, dada su multiplicidad, gravedad, precisión y concordancia, y por no estar contradichos con prueba alguna en contrario, estima esta Corte plenamente acreditado con ellos que la sociedad querellada y demandada civil ha infringido la Ley 19.496, al haber desconocido el derecho de la consumidora de recibir la información básica comercial, en los términos que exige el artículo 1, en relación al 37; y, al mismo tiempo, al haber negado esa información en los términos que señalan las normas precedentes, a la misma consumidora y al propio Servicio Nacional del*

Consumidor en los términos ya expuestos, y de acuerdo a lo prescrito en el artículo 58 de la ley"[131].

Ahora bien, a propósito del derecho a la protección de datos personales en el contexto de la contratación de un crédito de consumo, el artículo 37, en su inciso 3 se remite expresamente a la Ley 19.628 para referirse al deber del proveedor de informar las modalidades y procedimientos en que se desarrollará la cobranza de los créditos contratados:

> *"Entre las modalidades y procedimientos de la cobranza extrajudicial se indicará si el proveedor la realizará directamente o por medio de terceros y, en este último caso, se identificarán los encargados; los horarios en que se efectuará, y la eventual información sobre ella que podrá proporcionarse a terceros de conformidad a la Ley 19.628, sobre protección de los datos de carácter personal".*

La parte final de este inciso es especialmente relevante, pues impone el deber de indicar al consumidor "la eventual información sobre ella que podrá proporcionarse a terceros de conformidad a la Ley 19.628 sobre protección de los datos de carácter personal".

Esta expresa referencia permite el uso de registros de información comercial negativa, obligación que se entiende cumplida por el simple hecho de señalar cuál es la información que sobre la cobranza extrajudicial se dará a los encargados del tratamiento de datos de carácter personal relativos a obligaciones económicas, financieras o comerciales. Por lo tanto, el tratamiento de tales datos debe cumplir rigurosamente lo dispuesto en la ley N. 19.628 citada y también debe ajustarse a lo dispuesto en la ley N. 20.575 de 2012, que Establece el Principio de Finalidad en el Tratamiento de Datos Personales[132].

---

[131] CORTE DE APELACIONES DE TEMUCO, Causa nº 1344-2009, de 6 de noviembre de 2009, que confirma la sentencia de primera instancia.

[132] ESCALONA, E. 2013., cit. nota n. 9 pp. 824-825.

3.3.- Medidas técnicas y organizativas.

Las medidas de seguridad con que se busca proteger los datos personales pueden ser técnicas u organizativas, teniendo en consideración que la seguridad del tratamiento no es algo estático, sino que los avances tecnológicos configuran la seguridad como algo extraordinariamente dinámico que tendremos que plantear de idéntica manera[133].

Las medidas de seguridad técnicas son aquellas medidas y controles proporcionados a los sistemas y aspectos tecnológicos de una empresa, como dispositivos, redes y hardware. Estas medidas incluyen tanto la seguridad física como informática.

Por su parte, las medidas organizativas son el enfoque que una organización da para evaluar, desarrollar e implementar controles que protejan los datos personales con el fin de prevención o prohibición.

Ahora bien, las medidas de seguridad que se implementen obviamente deben hacerse cargo de las diferentes condiciones y realidades que tienen los diferentes responsables del tratamiento de los datos, por lo que las medidas de seguridad deberán definirse en función de la naturaleza de los datos tratados, así como en relación con la mayor o menor necesidad de garantizar la confidencialidad, integridad y disponibilidad de los datos. En función de ello, resulta bastante habitual en el concierto internacional distinguir entre medidas de seguridad de nivel bajo, medio y alto. Con todo, resulta importante tener en consideración que el Reglamento Europeo de Protección de Datos ha evolucionado en lo que se refiere a las medidas de seguridad y ha dejado de considerar el tipo de medidas específicas que deben implementar los responsables del tratamiento de datos para dar paso a un modelo de evaluación de riesgos en que se hace necesario considerar el nivel de seguridad parar

[133] PARRONDO, F. 2019. La protección de datos personales al descubierto: Manual para el cumplimiento del RGPD y la LOPDGDD (Spanish Edition) (p. 50). Edición de Kindle.

cada caso concreto en atención a los riesgos específicos que presente el tratamiento de los datos personales.

Para los efectos de nuestro análisis, y considerando el nivel de adopción de la normativa de protección de datos en el país, creemos que resulta útil proponer un sistema sobre la base de diferenciar entre los diferentes niveles de exigencia en consideración al tipo de datos tratados, las características que tienen los responsables del tratamiento, el volumen de datos tratados, el mayor o menor riesgo de afectación de derechos a causa del tratamiento de los datos y si las operaciones de tratamiento se realizan en forma automatizada o no.

Bajo los criterios antes señalados, estimamos que las medidas de seguridad deben agruparse para el crédito de consumo considerando el ciclo de vida del dato.

La siguiente tabla propone una taxonomía modelo a partir del Anexo I Medidas de Seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados[134].

REQUISITO		**MEDIDAS**
RECOLECCIÓN DE DATOS		
INTEGRIDAD	Mecanismos para asegurar la completitud.	1. Verificar que los campos que componen el formulario de recolección de datos permitan el ingreso completo de los datos requeridos.
	Mecanismos para minimizar los errores de ingreso.	1. Indicar en forma clara y concreta el tipo de información a ingresar y el formato de la misma.

[134] AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA DE ARGENTINA. Resolución 47/2018.

	Mecanismos para asegurar la integridad.	1. Verificar la exactitud del dato ingresado en caso de que el tipo de registro lo permita.
CONFIDENCIALIDAD	Mecanismos para asegurar la confidencialidad durante el proceso de recolección.	1. Cifrar la comunicación cliente-servidor durante la recolección.
	Limitar el acceso a la recolección de los datos	1. Limitar cache del formulario en el cliente únicamente al momento de carga de datos. 2. Limitar la carga de datos en el cliente a una sola sesión de usuario.
	Mecanismos para limitar el acceso no autorizado durante la recopilación	1. Utilizar certificados digitales seguros y validados por entidades autorizadas. 2. Cifrar la comunicación durante el traslado desde el servidor de aplicación hacia la base de datos.
CONTROL DE ACCESO		
IDENTIFICACIÓN DE ACTIVOS	Mecanismos para identificar los activos	1. Elaborar un inventario de activos informáticos que almacenen o gestionen datos personales.
	Definir responsabilidades y responsables	1. Definir propietarios de activos informáticos que almacenen o gestionen datos personales. 2. Notificar a los propietarios de activos informáticos que almacenen o gestionen datos personales. 3. Especificar a los propietarios de activos informáticos autorizaciones de acceso (tipo de acceso y validez).
	Mecanismos para verificar la aplicación de controles	1. Elaborar un procedimiento de actualización periódica del inventario.

		2. Elaborar un procedimiento de verificación de autorizaciones. 3. Elaborar un procedimiento para nuevos activos informáticos, definiendo responsable asignado y autorizaciones.
ACCESO A LOS DATOS	Mecanismos para gestionar los accesos a los Sistemas	1. Elaborar un documento interno que defina los controles de acceso a cada sistema. 2. Definir e identificar aquellos usuarios que por su rol de superusuarios (administradores) puedan evadir los controles de acceso definidos para el propietario. 3. Controlar y monitorear a los superusuarios (registrando accesos y actividad).
	Mecanismos para asignar los permisos	1. Disponer de una notificación concreta y formal de las responsabilidades asumidas por cada usuario que acceda internamente a los sistemas (notificación fehaciente).
	Mecanismos para verificar la identificación y autorización	1. Disponer de un sistema que identifique inequívocamente a cada usuario. 2. Establecer una política de contraseñas seguras. 3. Disponer de un registro de acceso a los sistemas. 4. Disponer de un registro de uso de los sistemas 5. Disponer de un procedimiento de Alta, Baja, Modificación de usuarios. 6. Limitar el acceso de los superusuarios a los datos personales o establecer un seguimiento de su actividad. 7. Asegurar la implementación de la política de contraseñas seguras en todos los sistemas. 8. Evitar el uso de usuarios genéricos.

	Mecanismos para controlar el acceso físico al centro de datos	1. Disponer de un control de acceso físico al centro de datos. 2. Elaborar un procedimiento de control de acceso físico. 3. Disponer de un registro de los accesos físicos (identificando día, hora, ingresantes y motivo). 4. Asegurar el sistema de registro del control de acceso.
	Mecanismos para monitorear la actividad	1. Definir un procedimiento de limpieza de cuentas inactivas con privilegios de acceso. 2. Limitar el acceso interno a los sistemas con un mismo usuario a una sola sesión concurrente. 3. Monitorear y controlar las cuentas de usuario que dispongan de privilegios especiales, identificarlas en forma diferencial. 4. Identificar y analizar intentos de autenticación fallidos.
CONTROL DE CAMBIOS		
CONTROL DE CAMBIOS	Mecanismos para verificar que los cambios aseguren la integridad	1. Verificar que los cambios a realizar en entornos productivos mantengan y aseguren la integridad de los datos.
	Mecanismos para asegurar en los procesos de cambio las medidas de recolección y control de acceso	1. Asegurar durante los procesos de cambio las medidas de Recolección de datos y Control de acceso.

	Mecanismos para registrar las verificaciones y/o pruebas realizadas para asegurar la integridad, disponibilidad y confidencialidad de los datos	1. Disponer de un registro de las verificaciones y/o pruebas realizadas para asegurar la integridad, disponibilidad y confidencialidad de los datos.
	Disponer de un procedimiento de control de cambios en entornos productivos	1. Definir un responsable de control de entornos productivos. 2. Disponer de un procedimiento de control de cambios en entornos productivos.
RESPALDO Y RECUPERACIÓN		
COPIAS DE RESPALDO Y PROCESO DE RECUPERACIÓN	Mecanismos para asegurar un proceso formal de respaldo y recuperación	1. Disponer de un procedimiento de resguardo de información donde se identifique: a. Qué tipo de información se resguardará. b. Qué medio físico se utilizará. c. Cantidad de copias de resguardo que se realizaran. d. periodicidad de las ejecuciones de copias de resguardo. e. descripción del proceso de la realización de copias de resguardo. 2. Definir y verificar procedimiento de pruebas de recuperación. 3. Disponer de un registro de pruebas de recuperación realizadas identificando: a. Tipo de información recuperada. b. Lugar y fecha donde se realizaron las pruebas de recuperación

		c. Resultado de las pruebas de recuperación d. Responsable de la realización de las pruebas de recuperación e. Personal interviniente en las pruebas de recuperación. f. Notificación al responsable de datos 4. Disponer de un inventario que identifique las copias de seguridad, su ubicación real y el medio físico en donde se encuentran.
	Mecanismos para asegurar control de acceso en los medios	1. Aplicar las medidas de Control de acceso a las copias de resguardo. 2. Cifrar las copias de resguardo utilizando herramientas seguras. 3. Asegurar los entornos de prueba de recuperación utilizando las mismas medidas de seguridad que un entorno productivo. 4. Eliminar en forma segura la información recuperada durante las pruebas una vez verificada su exactitud. 5. Disponer medidas de protección contra incendios o inundaciones en el sitio de almacenamiento de los medios físicos que contienen las copias de resguardo. 6. Almacenar las copias de resguardo en una locación física diferente a la del sistema productivo. 7. En caso de traslado de copias de resguardo, disponer de un procedimiento de registro y control del tránsito. 8. Asegurar los entornos de prueba de recuperación utilizando las mismas medidas de seguridad que un entorno productivo.

GESTIÓN DE VULNERABILIDADES		
GESTIÓN DE VULNERABILIDADES	Mecanismos para prevenir incidentes de seguridad desde el diseño	1. Considerar y analizar las posibles amenazas a la que estarán expuestos los sistemas informatizados. 2. Disponer de un mapa conceptual que permita conocer el flujo de la información entre los distintos sistemas informatizados. 3. Establecer un documento de seguridad que indique las medidas de seguridad adoptadas para los sistemas de información.
	Mecanismos para asegurar una protección adecuada	1. Establecer controles de seguridad para las aplicaciones que procesen datos personales, entre ellas: a. Segmentación de roles y perfiles. b. Autenticación segura. c. Gestión de sesiones. d. Gestión de mensajes de error en aplicaciones. 2. Implementar reglas y controles de seguridad en los servidores que estén conectados a una red externa y almacenen o gestionen datos personales, programando alertas ante posibles ataques. 3. Segmentar en forma física o lógica la red de la entidad, separando las áreas públicas de las privadas. 4. Separar los ambientes de Producción, QA, Prueba y Desarrollo. 5. Implementar controles para la prevención de virus informáticos en los servidores que almacenen o gestionen datos personales.

		6. Implementar controles para la prevención de ataques en las estaciones de trabajo que gestionen datos personales. 7. Implementar controles para la prevención de virus informáticos en las estaciones de trabajo que gestionen datos personales. 8. Establecer y ejecutar un procedimiento de actualización periódica de software/hardware de todo el equipamiento. 9. Definir a una persona responsable del cumplimiento de las medidas de seguridad.
	Mecanismos para detectar posibles incidentes de seguridad	1. Disponer de un sistema de auditoria de incidentes implementando un sistema de registro que permita realizar un seguimiento ante eventos o acciones de un posible incidente (sistema de logs). 2. Sincronizar todos los servidores/equipamiento con un servidor de horario público para asegurar una correcta trazabilidad en caso de realizar una auditoría. Implementar un proceso de denuncia que permita que los usuarios alerten eventos de seguridad. 3. Disponer de un sistema de gestión de incidentes capaz de mostrar fecha de registro, documentación relevante, personas involucradas, activos afectados.
	Mecanismos para garantizar medidas eficaces y perdurables	1. Implementar periódicamente procesos de auditoria interna para verificar el cumplimiento de lo mencionado con anterioridad, exportando informes y resguardándolos. 2. Realizar auditorías externas a fin de evaluar la seguridad de los sistemas internos.

DESTRUCCIÓN DE LA INFORMACIÓN		
ASEGURAR LA DESTRUCCIÓN DE LA INFORMACIÓN	Modelo/formato de destrucción	1. Establecer un procedimiento de destrucción de datos en donde se identifique: a. Tipo de información a destruir. b. Medio que contiene la información. c. Responsable de la destrucción. d. Descripción del proceso y método de destrucción utilizado.
	Mecanismos seguros de eliminación	1. Implementar un proceso de destrucción físico o lógico de la información que asegure el borrado total de la información sin posibilidad de recuperación de la misma cumpliendo tres premisas: a. Irreversibilidad. b. Seguridad. c. Confidencialidad.
	Mecanismos de monitoreo del proceso	1. Disponer de un inventario que identifique los medios destruidos.
	Responsable de destrucción	1. Establecer una persona autorizada para la destrucción y documentar su autorización.
	Mecanismos de descarte de medios magnéticos	1. Implementar un proceso de destrucción lógico de reescritura continua, de modo que los datos originales no puedan ser recuperados, pudiendo reutilizar el medio magnético. 2. En caso de no poder realizar el proceso de destrucción lógica, implementar un proceso de destrucción física utilizando técnicas de

		desmagnetización, desintegración, incineración, pulverización, trituración o fundición
INCIDENTES DE SEGURIDAD		
NOTIFICACIÓN ANTE INCIDENTES DE SEGURIDAD	Establecer responsabilidades y procedimientos	1. Elaborar un procedimiento de gestión ante incidentes de seguridad. 2. Establecer una persona responsable de la comunicación.
	Elaborar informe	1. Elaborar un informe del incidente de seguridad que tenga de contenido mínimo: a. Número único identificador del incidente (asignado por la SBIF). b. Nombre de la entidad informante. c. Descripción del incidente. d. Fecha y hora de inicio del incidente. e. Causas posibles o identificadas. f. Productos o servicios afectados. g. Tipo y nombre de proveedor o tercero involucrado (si corresponde). h. Tipo y número estimado de clientes afectados. i. Dependencias y/o activos afectados (si corresponde). j. Medidas adoptadas y en curso. k. Otros antecedentes.
	Mecanismos para enviar notificaciones	1. A la CMF mediante la casilla habilitada por a través de su Extranet, en cualquier horario, tanto en días hábiles como inhábiles, en el plazo máximo de 30 minutos luego de su ocurrencia.

		2. A la Industrial a través del Sistema de Alertas de Incidentes. 3. A clientes o usuarios.

Así, es posible advertir que las medidas de seguridad están orientadas a prevenir la confidencialidad, integridad y disponibilidad de los datos. Sin embargo, las obligaciones respecto a la seguridad no acaban en el plano preventivo, igualmente existe una obligación de comunicación de las violaciones producidas en materia de protección de datos[135].

En lo que se refiere a la notificación de los incidentes de seguridad la Comisión para el Mercado Financiero en RAN 20-8 establece que:

> "*Las entidades deberán comunicar a esta Superintendencia los incidentes operacionales que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la institución. El banco, en caso de incidentes, será responsable de mantener informada a esta Superintendencia de la situación en desarrollo y de las medidas o acciones de detección, respuesta y recuperación del incidente. A modo de ejemplo, y sin el objeto de ser exhaustivos ni taxativos, deberán ser reportadas las fallas en el servicio de proveedores críticos, problemas tecnológicos que afecten la seguridad de la información; la indisponibilidad o interrupción de algún servicio o producto que afecte a los clientes, en cualquier canal; pérdidas o fugas de información del banco o de clientes; los incidentes que afecten el patrimonio de la entidad producto de fraudes internos o externos, o los eventos que gatillen planes de contingencia, entre otros. Asimismo, deben ser informados los incidentes que afecten a un grupo de clientes que puedan impactar la imagen y reputación de la entidad en forma inmediata, o con posterioridad a ocurrido un determinado evento. Una vez comunicado el evento, la*

[135] PARRONDO, F. 2019., cit. nota n. 133, p. 52.

institución es responsable por establecer un canal permanente de comunicación con la Superintendencia".

El Proyecto de ley Boletín 11.144-07 que regula la protección y el tratamiento de datos personales y crea la Agencia de Protección de Datos Personales, actualmente en tramitación en el Congreso, incorpora un nuevo artículo 14 sexies a la Ley 19.628 disponiendo:

"*El responsable y el encargado de datos deberán reportar al Consejo para la Transparencia y la Protección de Datos Personales, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no autorizados a dichos datos, cuando exista un riesgo razonable para los derechos y libertades de los titulares.*

El responsable y el encargado de datos deberán registrar estas comunicaciones, describiendo la naturaleza de las vulneraciones sufridas, sus efectos, las categorías de datos y el número aproximado de titulares afectados y las medidas adoptadas para gestionarlas y precaver incidentes futuros.

Cuando dichas vulneraciones se refieran a datos personales sensibles, datos relativos a niños y niñas menores de catorce años o datos relativos a obligaciones de carácter económico, financiero, bancario o comercial, el responsable y el encargado de datos deberán también efectuar esta comunicación a los titulares de estos datos. Esta comunicación deberá realizarse en un lenguaje claro y sencillo, singularizando los datos afectados, las posibles consecuencias de las vulneraciones de seguridad y las medidas de solución o resguardo adoptadas. La notificación se deberá realizar a cada titular afectado y si ello no fuere posible, se realizará mediante la difusión o publicación de un aviso en un medio de comunicación social masivo y de alcance nacional".

De este modo, se advierte que, frente a una violación de datos personales en el marco de un proceso de contratación de un crédito de consumo, de prosperar la regulación en los

términos señalados precedentemente, la institución financiera que otorga el crédito (responsable del tratamiento) deberá reportar la brecha de seguridad a:

1. Comisión para el Mercado Financiero (regulador sectorial) dentro de los 30 minutos siguientes a ocurrido el hecho.
2. A los clientes:
    a. De acuerdo con la RAN 20-8, "*en forma oportuna*".
    b. De acuerdo con el Proyecto de ley Boletín 11.144-07 "*por los medios más expeditos posibles y sin dilaciones indebidas"*. Está notificación también deberá hacerse al Consejo para la Transparencia y la Protección de Datos.

Sin duda se hace necesario una revisión sistémica de la regulación existente y la pretendida de manera de evitar que se deba notificar a diferencias agencias y con la finalidad de despejar meridianamente cuál de ellas será la encargada de adoptar las medidas que permitan asegurar que los derechos de los titulares de datos (clientes de créditos de consumo) no se vean lesionados a causa de la violación de seguridad.

3.4.- Acciones de clase para la Protección de Datos Personales

A propósito del derecho a la Protección de Datos Personales en contexto de consumo, conviene prestar atención al Proyecto de ley Boletín 12.409-03 que establece medidas para incentivar la protección de los derechos de los consumidores, actualmente en tramitación en el Congreso, el cual, en su artículo 15 bis, indica lo siguiente a propósito de la aplicación de las reglas de protección de datos personales en materia de consumo:

> *"Artículo 15 bis.- Las disposiciones contenidas en los artículos 2 bis letra b), 58 y 58 bis de la presente ley, serán aplicables respecto de los datos personales de los consumidores, en el marco de las relaciones de consumo, salvo que las facultades contenidas en dichos artículos se encuentran en el ámbito de competencias legales de otro órgano".*

El artículo 2 bis letra b) al que hace mención este artículo, indica que la ley 19.496 de protección a los derechos de los consumidores se aplicará aun cuando exista legislación especial.

> *"Artículo 2º bis letra b).- No obstante lo prescrito en el artículo anterior, las normas de esta ley no serán aplicables a las actividades de producción, fabricación, importación, construcción, distribución y comercialización de bienes o de prestación de servicios reguladas por leyes especiales, salvo:*
>
> *b) En lo relativo al procedimiento en las causas en que esté comprometido el interés colectivo o difuso de los consumidores o usuarios, y el derecho a solicitar indemnización mediante dicho procedimiento".*

De acuerdo a la redacción de esta norma citada, el procedimiento para la defensa de los intereses colectivos o difusos de los consumidores debiese aplicarse de manera preferente a cualquier otra acción de clase, incluso cuando exista legislación especial que contemple este tipo de procedimiento[136].

De acuerdo a MOMBERG, la redacción de esta norma, redactada en términos imperativos, supone entender que, cuando el sujeto activo es un grupo de consumidores debe aplicarse las acciones de clase siempre. De hecho, sostiene MOMBERG, esto quedaría de manifiesto al contrastar el literal b) del artículo 2 bis con su literal c), el cual prescribe expresamente la supletoriedad de la aplicación del procedimiento para la protección de los intereses individuales de los consumidores[137].

---

[136] JARA, R. 2006. Ámbito de aplicación de la ley chilena de protección al consumidor: aplicación de la ley 19.496 y modificaciones de la ley Nº 19.555. En La protección de los derechos de los consumidores en Chile, Cuadernos de Extensión Jurídica 12, Facultad de Derecho de la Universidad de Los Andes, pp. 31-32

[137] MOMBERG, R. 2013. Artículo 2º bis, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile, pp. 77-83. p. 82

En el entorno nacional, tanto en la ley 19.496 de protección a los derechos de los consumidores como en la ley 19.628 sobre protección a la vida privada, hay una ausencia de referencias expresas a la interposición de acciones colectivas por infracciones en el tratamiento de datos personales.

No obstante, el SERNAC ha interpuesto acciones colectivas en contra de proveedores por infracciones a la normativa de protección de datos personales. Destacan en este sentido dos fallos en contra de dos compañías ticketeras: uno en contra de Ticketmaster y otro en contra de Ticketek, finalmente resueltos por la Corte Suprema.

En Ambos casos, el SERNAC, en atención a que no existe una norma expresa que habilite el ejercicio de acciones de clase para la protección de datos personales, argumentó lo siguiente[138]:

a. Que entre las compañías y titulares había una relación de consumo.
b. Que las políticas de privacidad de estas compañías eran contratos de adhesión en cuyo contenido había cláusulas abusivas.

Cabe advertir que la jurisprudencia de la Corte Suprema no ha sido consistente, toda vez que ha fallado en direcciones opuestas.

En el caso de Ticketmaster, la Corte Suprema, en fallo de julio de 2016[139], consideró como abusivas aquellas cláusulas de la Política de Privacidad que permitían recopilar todo tipo de información personal, sin limitaciones de tipo o cantidad y revelarla a terceros. Al respecto la Corte sostuvo lo siguiente:

---

[138] FRIGERIO, C y BERTSCHIK, S. 2021. Acciones colectivas en materia de protección de datos personales [en línea] FerradaNehme, 30 de junio de 2021, <https://www.fn.cl/publicaciones/acciones-colectivas-en-materia-de-proteccion-de-datos-personales/> [consulta 30 de junio 2021].

[139] CORTE SUPREMA, Causa Nº 1533-2015, Resolución Nº 367725, del 7 de julio de 2016.

"11º […] Tal renuncia a la privacidad de los datos personales sólo es válida si es otorgada de forma explícita y específica".

Además, consideró como abusiva aquella cláusula que permitía recolectar información derivada de los gustos, preferencias y en general de la utilización de los servicios, por infringir el principio de proporcionalidad en el tratamiento de datos:

"12º […] se trata por otra parte de información que excede de la necesaria para concluir las transacciones de compraventa de entrada, resultando abusivas por buscar obtener tal consentimiento en forma atada a una operación comercial con un objeto diferenciado".

En el caso de Ticketeck, por su parte, en fallo de diciembre del 2016[140], la Corte Suprema estimó que la ley 19.628 regula una cuestión esencialmente individual, indicando que no procedería la aplicación de procedimientos de interés colectivo al sostener lo siguiente:

"*6º La ley 19.628 regula una cuestión esencialmente individual, desde que protege a cada persona cuya información pueda estar en poder y ser administrada por los titulares de bancos de datos estableciendo un procedimiento que nace del interés individual, lo cual deja en evidencia que no es posible asumir que la ley especial pueda ceder ante la general, aún en el caso de procedimientos de interés colectivo o difuso de los consumidores, puesto que la naturaleza de los asuntos regulados por la ley 19.628 es esencialmente individual, sin que tengan cabida los procesos colectivos, por lo que únicamente puede aplicarse la ley especial en los casos en que puedan verse afectados los datos de carácter personal de un individuo y, por lo mismo, los sentenciadores no han incurrido en un error de derecho al desechar el reclamo de*

[140] CORTE SUPREMA, Causa Nº 26932-2015, Resolución 702286, del 6 de diciembre de 2016.

abusividad de la cláusula octava del contrato de adhesión por carecer el SERNAC de legitimación en este aspecto".

Así, al menos con la normativa actualmente vigente, no es posible definir si aplican o no las acciones de interés colectivo o difuso, propias del derecho de consumo, de cara a infracciones a la normativa de protección de datos personales.

En este sentido, Donoso ha planteado que el proyecto de ley, Boletín 12.406-03, solucionaría el problema de jurisprudencia contradictoria al que se hizo mención, justamente respecto a las facultades del SERNAC[141].

Sin embargo, tendría entre los principales déficits, que el SERNAC no es un organismo autónomo, como exige el estándar internacional ya que su director es nombrado por el Presidente de la República. En tal sentido, debiera ser un órgano de protección de datos especializado e independiente el que debiera tener esa facultad[142].

En derecho comparado, el Reglamento General de Protección de Datos, que hoy se erige como el principal referente internacional sobre la materia, establece en su artículo 80 que las acciones de clase podrán presentarse por organismos sin fines de lucro dedicados a la protección de datos personales.

> *"Artículo 80: El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos*

[141] RIVAS, C. 2021. Expertas enjuician el polémico artículo que entrega al Sernac facultades de protección de datos, Diario Financiero, jueves 1 de julio de 2021, p. 11.

[142] RIVAS, C. 2021., cit. nota 141. p 11.

personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro".

Desde su entrada en vigor, se han interpuesto una serie de acciones colectivas por vulneraciones al Reglamento en distintos países de la Unión Europea, como por ejemplo el caso de British Airways en Reino Unido por la filtración de información financiera de más de 400.000 clientes el año 2018 o el caso Facebook presentado en Irlanda por una filtración de datos que afectó a más de 530 millones de usuarios a nivel mundial el 2019[143].

3.5. Pymes y protección de datos personales.

En febrero de 2010 se promulgó la ley 20.416 que fija normas especiales para las empresas de menor tamaño.

Esta ley distingue entre microempresa, pequeña empresa y mediana empresa categorizándolas en atención a sus ingresos por venta:

a. Microempresa: es aquella cuyos ingresos anuales por ventas y servicios sea de hasta 2.400 UF, descontándose IVA e impuesto específico.
b. Pequeña empresa: es aquella cuyas ventas anuales oscilen entre 2.401 y 25.000 UF.
c. Mediana empresa: es aquella cuyas ventas anuales oscilen entre 25.001 y 100.000 UF.

Entre otras cosas, esta ley tiene como finalidad la protección de las PYMES en calidad de parte más débil en la relación contractual. De acuerdo con el artículo noveno de esta ley, se hace extensiva la aplicación de la Ley 19.496 de protección a los consumidores a las Pequeñas y Medianas Empresas, al considerar que, en determinados casos, las PYMES se

[143] FRIGERIO, C y BERTSCHIK, S. 2021. cit. nota n. 138

encuentran en una situación similar a la de los consumidores. Al respecto, el artículo 9 indica lo siguiente:

"Artículo Noveno. - Rol de Consumidoras. Establécese la protección a las micro y pequeñas empresas en rol de consumidoras, en los términos que siguen:

1) *Ámbito de Aplicación. El presente artículo tiene por objeto normar las relaciones entre micro y pequeñas empresas y sus proveedores, establecer las infracciones en perjuicio de aquellas y señalar el procedimiento aplicable en la materia.*

   Para los efectos de esta ley se entenderá por proveedores las personas naturales o jurídicas que, definidas de acuerdo con el artículo 1° de la Ley 19.496, desarrollen las actividades allí señaladas respecto de micro y pequeñas empresas.
2) *Normas Aplicables. Serán aplicables a los actos y contratos celebrados entre micro o pequeñas empresas y sus proveedores las normas establecidas en favor de los consumidores por la ley sobre Portabilidad Financiera y la Ley 19.496 en los párrafos 1°, 3°, 4° y 5° del Título II, y en los párrafos 1°, 2°, 3° y 4° del Título III o, a opción de las primeras, las demás disposiciones aplicables entre partes. En ningún caso serán aplicables las normas relativas al rol del Servicio Nacional del Consumidor. La aplicación de las disposiciones señaladas precedentemente será irrenunciable anticipadamente por parte de las micro y pequeñas empresas.*

   Para todos los efectos legales, las normas relativas a los medios de prueba contenidas en el Código de Comercio serán también aplicables a los litigios judiciales referidos en el párrafo anterior.
3) *Sanciones. Las infracciones a lo dispuesto en esta ley serán sancionadas con arreglo al artículo 24 de la Ley 19.496.*
4) *Juez competente. En caso de que el titular de la micro o pequeña empresa opte por la aplicación de las normas de la Ley 19.496, será competente el juez de policía local del lugar en que se haya producido la infracción, celebrado el acto o contrato o dado*

inicio a su ejecución, a elección del actor. En caso contrario regirán las normas generales.

5) *Procedimiento Aplicable. Las acciones que surjan por aplicación de este artículo, incluida la acción civil que se deduzca para la indemnización de los daños causados, se tramitarán de acuerdo con lo dispuesto en las normas del párrafo 1° del Título IV de la Ley 19.496, cuando sea procedente.*

   En caso de existir un grupo de micro o pequeñas empresas que cumplan con los requisitos establecidos por la Ley 19.496, podrán interponer acciones colectivas en los términos de los artículos 50 y siguientes del mismo cuerpo normativo, sin perjuicio de lo señalado en el numeral 2) del presente artículo. También podrán iniciar dichas acciones, en representación de sus afiliados, las entidades de carácter gremial que los agrupen.

6) *Deber de Profesionalidad. Si las infracciones a lo dispuesto en este artículo se refieren a la adquisición o contratación de bienes o servicios que se relacionan directamente con el giro principal de la micro o pequeña empresa, el tribunal deberá considerar en la aplicación de la multa que proceda, que el deber de profesionalidad de la micro o pequeña empresa es equivalente al del proveedor que cometió la infracción.*
7) *Prevención. Las normas de esta ley en ningún caso restringen o disminuyen la responsabilidad que las micro y pequeñas empresas tengan como proveedores en sus relaciones con consumidores finales de bienes y servicios".*

Respecto del artículo 15 bis al que se hizo mención en el apartado anterior, a propósito del Proyecto de ley Boletín 12.409-03, surge la duda respecto a si, por aplicación de la ley 19.628 a la normativa de consumo, en atención a lo dispuesto en el estatuto PYME, se haría extensiva la aplicación de la normativa de protección de datos personales a este tipo de empresas, calificándolas como "titulares de datos".

Ahora bien, en respuesta a la pregunta que surge a propósito del estatuto PYME y la aplicación de reglas de protección de datos, consideramos que la Ley 19.496, prevé expresamente quién ha de considerarse como "titular de los datos" en la letra ñ de su artículo 2 al indicar que:

> *"Para los efectos de esta ley se entenderá por Titular de los datos, la persona natural a la que se refieren los datos de carácter personal".*

Conviene tener presente que el artículo 9 nº 2 de la ley 20.416 que fija normas especiales para las empresas de menor tamaño, excluye expresamente al SERNAC como ente fiscalizador en aquellos casos que, en contexto de una relación de consumo, se activarían a favor de PYMES al indicar que

> "*En ningún caso serán aplicables las normas relativas al rol del Servicio Nacional del Consumidor".*

A partir de esta exclusión se colige que tampoco habría de hacer extensivo a las PYMES la normativa de protección de datos.

Por último, al prestar atención al proyecto de ley Boletín 12.409-03 al que ya se hizo mención, especialmente al artículo 15 bis, que se analizó en el apartado anterior, se advierte que el artículo 58 bis al que hace este artículo indica que los organismos fiscalizadores sectoriales que tengan facultades sancionatorias deberán remitir al SERNAC copia de las resoluciones en que impongan sanciones. Con ello, la futura Agencia de Protección de Datos se encontraría en la obligación de remitir al SERNAC copia de aquellas resoluciones en que impongan sanciones a proveedores[144].

---

[144] ARRIETA, R., CÓRDOVA, D y PÉREZ, J. 2020. Consumidores y protección de datos personales, un peligroso camino que hemos comenzado a recorrer [en línea] El Mercurio Legal, 27 de noviembre de 2020. <https://www.elmercurio.com/legal/noticias/opinion/2020/11/27/consumidores-y-proteccion-de-datos-personales-un-peligroso-camino-que-hemos-comenzado-a-recorrer.aspx> [consulta 29 de marzo 2021]

Sin embargo, de acuerdo a lo que se ha sostenido, la futura Agencia de Protección de Datos conocerá de casos de infracción a la normativa de Protección de Datos Personales y, de acuerdo a esta normativa, tanto si se considera la ley vigente como el proyecto que actualmente se tramita en el Congreso, se concibe al titular de los datos como la persona natural, identificada o identificable, a quien conciernen o a la que se refieren los datos personales.

Por lo tanto, la Agencia de Protección de Datos, al hacerse cargo únicamente de casos que digan relación con infracciones relativas a personas naturales. En contexto de consumo jamás llegará a remitir al SERNAC casos relativos a PYMES, debiendo concluirse, por lo tanto, que la regla del artículo 15 bis del proyecto de ley en comento no se haría extensivo, por aplicación de la ley 20.416 a pequeñas y medianas empresas.

Finalmente, y a título de conclusión podemos advertir que la seguridad es un elemento que en general es bastante olvidado a la hora de conceptualizar jurídicamente la forma en que la contratación electrónica de los créditos de consumo y que, sin embargo, aparece como común denominador en las regulaciones de referencia es la seguridad, es más en materia de protección de datos personales aparece como un elemento que dota de contenido esencial al derecho.

No obstante, en nuestra opinión se trata más bien de un olvido desde el punto de vista de las exigencias que imponen los operadores jurídicos o la exigibilidad que hacen de ella los tribunales de justicia, porque tal como analizamos en las páginas precedentes la Ley 19.496 y la Ley 19.628 permiten construir un gravoso sistema de seguridad que en caso de ser vulnerado permite reclamar judicialmente los perjuicios que se ocasionan como consecuencia de los daños que el producto es capaz de producir y/o la falta de diligencia de parte del proveedor del crédito de consumo en el cuidado debido de los datos personales.

Conclusiones

En relación con el objetivo de este estudio, cual era demostrar que la regulación vigente permite dotar de certeza jurídica y seguridad a la contratación de créditos de consumo a través de medios electrónicos, la investigación ha arrojado los siguientes resultados:

1.- Si bien existe una profusa normativa, el régimen regulatorio aplicable a la contratación electrónica no se encuentra desarrollado de manera uniforme ni sistemática. Muy por el contrario, para fijar su regulación hay que prestar atención a las normas diversas.

2.- Adicionalmente, al tratarse de un mercado dinámico, su régimen regulatorio está en constante evolución y cambio. Prueba de ello es que, junto a las leyes vigentes, habrá que prestar atención a reformas legislativas en materia de consumo como el boletín 12.409-03 y en materia de protección de datos con el Boletín 11.144-07 de cara a terminar de definir el régimen regulatorio aplicable a los contratos objeto de este estudio. Esta circunstancia demanda constantes actualizaciones tanto de los sistemas de apoyo como de las estructuras profesionales y administrativas que los soportan.

3.- No obstante la dispersión normativa, principalmente por su componente electrónico, la seguridad aparece como columna vertebral de la regulación, ya sea como derecho o principio que inspira su contenido.

4.- De esta manera, los aspectos normados, ya sea a través de ley o norma técnica permiten sostener que el estándar de seguridad en la celebración de este tipo de contratos se puede estructurar de la siguiente manera:

a. Respecto de la protección de derechos del consumidor.

   El derecho a la seguridad en el consumo supone la exigencia a los proveedores de que sus productos o servicios no causen daño, cuestión que se hace plenamente aplicable a los servicios que se prestan a través de Internet, ya que dependiendo de la forma en que éstos se provean podrán resultar significativos

menoscabos en ámbitos tanto en el ámbito patrimonial como no patrimonial de los clientes.

Así, es indispensable que el proveedor se ocupe de brindar seguridad al consumidor, respecto no sólo al producto final que se va a entregar (crédito de consumo) sino que respecto a todo el proceso de negociación y contratación que se hace de éste en forma electrónica. Para ello, resulta esencial para el cumplimiento de este deber que la institución financiera junto con implementar robustas plataformas de contratación electrónica sea capaz a través de sistemas o procedimientos de identificar, evaluar, monitorear y detectar en el menor tiempo posibles operaciones que pueden tener patrones de fraude y que consecuentemente pueden terminar redundando en un daño para el cliente.

b. Respecto de la seguridad documental y aseguramiento de la ejecución.

Probablemente del análisis efectuado de la regulación aplicable a la contratación electrónica de créditos de consumo esta es la materia analizada en este trabajo que tiene una profundidad normativa más grande, encontrándose en nuestra opinión debidamente resguarda la calidad jurídica de los instrumentos privados en que se sustentan esta clase de operaciones financieras. Así, la equivalencia de soportes reconocida en la ley es suficiente para considerar que se cuenta con los elementos necesarios para tener un comercio electrónico seguro.

Sin embargo, estimamos que sin perjuicio de la suficiencia normativa señalada la falta de adopción de la regulación de parte de los operadores jurídicos hace que pese a que la ley es del año 2001 aún tiene una aplicación práctica escasa, con significativos errores de implementación que merman la seguridad jurídica y con decisiones judiciales (tanto en procesos sometidos a conocimiento de los tribunales como en el ejercicio de la facultad disciplinaria de la Corte Suprema y Cortes de Apelaciones) erráticas y con poco sustento y evidencia jurídica.

Finalmente, consecuencia de que la mayor cantidad de operaciones de crédito de consumo se garantizan mediante pagarés, encontramos en el sistema normativo una debilidad al no poder contarse con pagarés electrónicos que gocen de mérito ejecutivo. Ello sin duda se convierte en una limitación no sólo por las consideraciones asociadas al proceso mismo de ejecución en caso de incumplimiento sino también por las provisiones que tienen que considerar las instituciones financieras por riesgo de crédito.

c. En materia de protección de datos personales.

El hecho de que la seguridad no se encuentre desarrollada de manera explícita en la Ley 19.628 y que consecuentemente sea una construcción que se hace a partir del régimen de responsabilidad considerado en la ley, hace que se trate de una materia que tiene una escasa preocupación práctica de parte de los actores involucrados en las operaciones de tratamiento de datos personales.

Adicionalmente, la falta de profundidad en el desarrollo del tema hace que no hayan lineamientos estandarizados ni claros que deben cumplir los diferentes operadores financieros, con lo que se advierte en la práctica que la forma de abordar la materia finalmente tiene que ver con la mayor o menor aversión al riesgo de la institución y a las medidas de ciberseguridad general que se aplican al negocio sin que haya un análisis o vocación especial de cuidado por el hecho de tratarse de datos personales.

No obstante, y tal como se desarrolló a lo largo de este trabajo, el hecho de que no se encuentre establecido de manera reglada las obligaciones asociadas a seguridad que tienen los responsables del tratamiento de datos personales se encuentra muy lejano a poder considerar que no existen obligaciones de este tipo. Muy por el contrario, el hecho de que el estándar fijado sea el demostrar la debida diligencia obliga a los responsables del tratamiento de datos a efectuar una evaluación de riesgo respecto de cada una de las operaciones de esta

naturaleza que se efectúan, de manera de poder dimensionar para el caso concreto cuales son los cuidados que deben adoptarse para asegurar que el tratamiento de los datos no lesione los derechos de los titulares.

De este modo, de acuerdo con lo analizado en este trabajo y sin perjuicio de que el régimen regulatorio aplicable a la contratación electrónica se encuentra contenido en leyes distintas, es posible sostener que su regulación es suficiente para dotar de certeza jurídica y seguridad a los consumidores y usuarios que celebran este tipo de contratos. Así las cosas, la estructura jurídica existente nos permite celebrar este tipo de contratos plenamente ajustado a derecho y de acuerdo a las mejores prácticas sobre contratación electrónica el contrato electrónico del crédito de consumo. Sin embargo, bajo una lógica de *lege ferenda,* consideramos que se podría avanzar en las siguientes reformas normativas, a fin de mejorar la seguridad jurídica, en el ámbito de las certezas que permitirán el desarrollo de este tipo de operaciones de crédito:

a. Mejoras a la ley del consumidor.

   Un aspecto en que podría avanzarse regulatoriamente es en la determinación del momento en que se entiende formado el consentimiento en los contratos de crédito de consumo que se celebran por medios electrónicos.

   En nuestra opinión eso permitiría eliminar asperezas que son la consecuencia de utilizar normas que fueron dictadas cuando las técnicas y medios electrónicos ni siquiera estaban en la imaginación del legislador.

   Así como se discute respecto a si la formación del consentimiento se produce en el momento en que se envía la aceptación o bien cuando la recibe el oferente en el mundo real, en que se presuponen ciertos plazos para que la respuesta que se emite llegue a destino, en el mundo virtual, a pesar de la simultaneidad que puede darse en estas comunicaciones, existe también la falta de certeza de que la respuesta llegue a puerto y, si llega, que el destinatario la abra y lea.

De este modo, podría avanzarse en precisar que la contratación por medios electrónicos se asemeja a la contratación entre presentes y que los derechos y obligaciones que emanan del contrato se hagan vinculantes para las partes sólo una vez que el proveedor o empresa que ofrece el producto o servicio financiero entrega una hoja resumen de la operación con expresa indicación de las principales cláusulas del contrato de manera de que se tome claramente conocimiento sobre las características y condiciones del producto contratado.

Por otra parte, estimamos que se hace necesario regular la forma en que podrá ejercerse el derecho a retracto que permite al consumidor poner término unilateral a los contratos celebrados por medios electrónicos. Ello, porque una vez que el contrato se haya perfeccionado y los fondos hayan sido entregados al consumidor, se hace indispensable establecer la forma en que se dejarán de producir los efectos de obligaciones que son de tracto sucesivo.

Finalmente y de cara al Proyecto de Ley Boletín 12.409-03 que incentiva la protección de los derechos de los consumidores, y buscando coherencia con la ley 19.628 y el proyecto de ley que la modifica (Boletín 11.144), al aplicar las reglas de las acciones de clase en materia de protección de datos, convendría indicar expresamente que éstas no aplicarían a PYMES, independiente de su reconocimiento como titulares de derecho de consumo por aplicación del estatuto PYME, toda vez que no se tratarían de personas naturales, a las cuales protege el derecho a la protección de datos.

b. Avances en materia de documentos electrónicos.

Sin duda representaría un gran avance para la comercialización de los créditos de consumo en forma electrónica que se reconociera el mérito ejecutivo de los pagarés electrónicos, suscritos mediante firma electrónica avanzada y sellado de tiempo. Ambos elementos, que tal como analizamos a lo largo de esta actividad formativa equivalente a

tesis, permiten técnicamente dar seguridad operacional y jurídica respecto de la autoría, integridad, no repudio y momento en el cual un documento electrónico fue otorgado.

No obstante, estimamos que el Proyecto de Ley Boletín 8466 que modifica la Ley 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma y otros textos legales que indica va en esa dirección, estimamos que es insuficiente en lo que se refiere a la modificación propuesta a la Ley 18.092.

Para asegurar su utilidad práctica y garantizar la seguridad y certeza jurídica además de otorgar mérito ejecutivo al pagaré electrónico, estimamos se hace necesario regular:

- El momento en que los impuestos y derechos asociados a la operación de crédito de dinero deberán ser pagados, para lo cual se debe diferenciar entre aquellas operaciones con vencimiento de acuerdo a las reglas generales contenidas en el Decreto Ley 3475 y las que contenga operaciones de crédito de dinero a la vista o sin plazo de vencimiento, donde se debería establecer que el impuesto debe estar enterado en arcas fiscales con anterioridad a su protesto o cobro.
- La creación de un Sistema Nacional de Letras de Cambio y Pagarés Electrónicos en el que se deba hacer la anotación de la extensión, endoso, aceptación o constitución del aval en los instrumentos de crédito. Ello para para asegurar el procesamiento y registro electrónicamente de las letras de cambio y pagarés electrónicos que sean librados, debiendo coordinar y suministrar la información necesaria que permita el endoso, protesto y demostrar el pago del correspondiente impuesto de timbres y estampillas.
- Finalmente, establecer que cada vez que la ley disponga que una determinada actuación debe realizarse en el anverso, dorso o en una hoja de prolongación de la letra de cambio o el pagaré, se entenderá cumplido el requisito en la medida que la letra de cambio o el pagaré se encuentre extendido a través de medios electrónicos y la nueva actuación se haga constar en un documento electrónico que se mantenga vinculado inequívocamente con la letra de cambio o el pagaré.

c. Mejoras a las normas de protección de datos.

A este respecto consideramos que se hace indispensable avanzar en una profundización del principio internacionalmente reconocido de seguridad en el tratamiento de datos personales. Para ello resulta indispensable establecer con claridad que el responsable del tratamiento de datos debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, así como su pérdida, filtración, daño accidental o destrucción. Asimismo, establecer que las medidas de seguridad deben ser sean apropiadas y contestes con el tipo de operaciones de tratamiento de datos personales, el nivel de profesionalismo de quien realiza dichas operaciones y el riesgo implícito de afectación de derechos que ellas conllevan.

Junto a ello, estimamos que se debe dar paso a un sistema de responsabilidad demostrada donde frente a la ocurrencia de un incidente de seguridad, sea el responsable del tratamiento quien deba acreditar la existencia y el funcionamiento de las medidas de seguridad adoptadas en base a los niveles de riesgo y a la tecnología disponible. De este modo, se propone alterar la carga de la prueba.

Adicionalmente, estimamos que por el nivel de desarrollo que tiene la protección de datos en el país, resulta conveniente no recurrir a un sistema en que sea el propio responsable del tratamiento el que deba determinar el tipo de medidas de seguridad a implementar, sino que sea la autoridad pública la que defina las medidas mínimas de seguridad que deban cumplir los responsables y encargados del tratamiento de datos en función de la naturaleza de la actividad a realizar, la posible afectación de derechos a causa del tratamiento de los datos personales y el ciclo de vida de los datos tratados.

Finalmente, estimamos que se debe normar adecuadamente el deber de reportar, por los medios más expeditos posibles y sin dilaciones indebidas, las vulneraciones a las medidas de seguridad que ocasionen la destrucción, filtración, pérdida o alteración accidental o ilícita de los datos personales que trate o la comunicación o acceso no

autorizado a dichos datos, cuando con ocasión de estos incidentes exista un riesgo para los derechos y libertades de los titulares. Así, se trata de profundizar y hacer explícito para los datos personales la de comunicar que tienen las instituciones financieras de comunicar a la Comisión para el Mercado Financiero los incidentes operacionales que afecten o pongan en riesgo la continuidad del negocio, los fondos o recursos de la entidad o de sus clientes, la calidad de los servicios o la imagen de la institución.

BIBLIOGRAFÍA

- ALESSANDRI, A. y SOMARRIVA, M. 1991. Derecho Civil. Parte Preliminar y Parte General. Santiago, Editorial Conosur. Tomo II.
- AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA DE ARGENTINA. Resolución 47/2018
- ARCOS, M. 2012. Contratos de adhesión electrónicos: análisis a los contratos de retail electrónicos y contratos de servicios de suscripción en línea, películas, televisión y otros tipos de entretenimiento audiovisual. Santiago, Fundación Fernando Fueyo, Universidad Diego Portales.
- ARRIETA, R., CÓRDOVA, D y PÉREZ, J. 2020. Consumidores y protección de datos personales, un peligroso camino que hemos comenzado a recorrer [en línea] El Mercurio Legal, 27 de noviembre de 2020, 2020. < https://www.elmercurio.com/legal/noticias/opinion/2020/11/27/consumidores-y-proteccion-de-datos-personales-un-peligroso-camino-que-hemos-comenzado-a-recorrer.aspx>
- BARROS. E. 2006. Tratado de Responsabilidad Extracontractual. Santiago, Editorial Jurídica de Chile.
- BENUSSI, C. 2020. Obligaciones de Seguridad en el Tratamiento de Datos Personales en Chile [en línea] Revista Chilena de Derecho y Tecnología, Vol. 9 núm 1 <https://webcache.googleusercontent.com/search?q=cache:5r3oYSyqCbgJ:https://revistas.uchile.cl/index.php/RCHDT/article/download/56660/61350/+&cd=9&hl=es-419&ct=clnk&gl=cl>
- BIELLI, G. y ORDOÑEZ, C. 2020. Contratos Electrónicos: teoría general y cuestiones procesales. Santiago, Legal Publishing Chile. Tomo I.

- BOZZO, S. 2020. Sobreendeudamiento del consumidor en Chile: Una revisión a la luz del derecho europeo. En Revista de Derecho (Valdivia). Vol. XXXIII – Nº1, junio 2020.
- CAMACHO, S. 2019. Características de la contratación electrónica. En CURSO ONLINE Contratación y mercado digital. Aspectos legales y otras cuestiones de interés. Universitat Autònoma de Barcelona. [en línea] <https://es.coursera.org/lecture/mercado-digital/la-contratacion-electronica-caracteristicas-XbT8E>
- CÁMARA DE COMERCIO DE SANTIAGO. CyberDay 2021 duplica expectativas y se transforma en el evento más importante en la historia del e-commerce chileno. 2021. [en línea] <https://www.ccs.cl/2021/06/03/cyberday-2021-duplica-expectativas-y-se-transforma-en-el-evento-mas-importante-en-la-historia-del-e-commerce-chileno/>
- CÁMARA DE COMERCIO DE SANTIAGO. CyberDay 2021 se inicia el lunes 31 de mayo con 670 participantes. 2021 [en línea] <https://www.ccs.cl/2021/05/25/cyberday-2021-se-inicia-el-lunes-31-de-mayo-con-670-participantes/>
- CANELO, C. 2003. La Eficacia Probatoria y la ley de Firma Electrónica. Revista Chilena de Derecho Informático, Núm 2.
- COLUMBA, E. 2016. Fundamentos de Seguridad de la Información basados en ISO 27001/27002: Guía de referencia para rendir el examen de Fundamentos de Seguridad de la Información basado en ISO/IEC 27002. Kindle.
- COMISIÓN PARA EL MERCADO FINANCIERO. [en línea] <https://www.cmfchile.cl/portal/estadisticas/617/w3-propertyvalue-21028.html>
- COMPUTER SECURITY RESOURCE CENTER. [en línea] <http://csrc.nist.gov/publications/PubsFIPS.html>

- CONTARDO, J.I. 2013. Artículo 23 inciso 1º, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile.
- CÓRDOVA, D. 2016. Régimen de responsabilidad de compañías de descuento por Internet, ¿Proveedores Intermediarios? En Revista de Derecho, Universidad Católica del Norte, Sección Estudios, Año 23.
- CORRAL, H. 1999. ley de protección al consumidor y responsabilidad civil por productos y servicios defectuosos. En: Cuaderno de Extensión Jurídica: Derecho del Consumo y Protección del Consumidor (3), Universidad de los Andes.
- CORRAL, H. 2013. Artículo 3 D). En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile.
- CORRAL, H. 2013. Artículo 45, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile.
- CORRAL, H. 2013. Artículo 46, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile.
- CORRAL, H. 2013. Artículo 47, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile.
- CORTE SUPREMA. 2006. Autoacordado sobre uso de documento y firma electrónica por notarios, conservadores y archiveros judiciales. 10 de noviembre de 2006. [en línea] <https://www.bcn.cl/leychile/navegar?idNorma=255008>

- DAVARA, M.A. 1997. Manual de Derecho Informático. Pamplona, Ed. Aranzadi.
- DE LA MAZA, I. 2013. Artículo 17 B (Letras A, B, C, D, E, F). En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile.
- DE PRADA. V. 2001. Nuevos Campos que abre la informática a la función notarial. En Colegios Notariales de España. Notariado y Contratación Electrónica. Madrid.
- DIVIN. F. 2005. El sellado de tiempo en nuestro derecho. Revista Chilena de Derecho Informático. Santiago. Universidad de Chile.
- DONOSO, L. 2019. Formalismo Jurídico: Autenticación y otras garantías, En: El Derecho de las TIC en Iberoamérica, Marcelo Bauzá Reilly, Fiadi, la ley Uruguay.
- ENTIDAD ACREDITADORA, [en línea] <https://www.entidadacreditadora.gob.cl/>
- ENTIDAD ACREDITADORA, Entidades Acreditadas, [en línea] <https://www.entidadacreditadora.gob.cl/entidades/>
- ESCALONA, E. 2013. Artículo 37, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile.
- ETSI. 2002. TS 102 042 “Policy requirements for certification authorities issuing public key certificates”. [en línea] <https://www.etsi.org/deliver/etsi_ts/102000_102099/102042/01.01.01_60/ts_102042v010101p.pdf>
- FELDSTEIN DE CÁRDENAS, S.L., RODRÍGUEZ, M.S., MEDINA, F.A., SCOTTI, L.B y KLEIN VIERA, L. 2012. El rol de la autonomía de la voluntad en los contratos celebrados por medios electrónicos. [en línea] Suplemento de Derecho Internacional Privado y de

la Integración (71). <https://www.eldial.com/nuevo/lite-tcd-detalle.asp?id=6587&base=50&id_publicar=&fecha_publicar=26/10/2012&indice=doctrina&suple=Privado>

- FERNÁNDEZ, C. 2012. En: Revisa de Derecho UNED, núm. 10. Algunos retos de la protección de datos en la sociedad del conocimiento. En especial detenimiento en la computación en nube (Cloud computing).
- FRIGERIO, C y BERTSCHIK, S. 2021. Acciones colectivas en materia de protección de datos personales [en línea] Ferrada Nehme, 30 de junio de 2021, <https://www.fn.cl/publicaciones/acciones-colectivas-en-materia-de-proteccion-de-datos-personales/>
- GOLDBERG, J.L. 2017. El necesario ajuste de la asignación del riesgo de sobreendeudamiento en la regulación de las tarjetas de crédito: desde un sistema basado en los deberes de información a un modelo de corresponsabilidad. En Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, Nº 49
- GUTIÉRREZ, P. 2018. Vivir con deudas en Chile. Análisis de la estructura, fallas y regulación en el mercado de créditos al consumo (Memoria para optar al grado de Licenciada en Ciencias Jurídicas y Sociales), [en línea], Universidad de Chile, <http://repositorio.uchile.cl/bitstream/handle/2250/150946/Vivir-con-deudas-en-Chile-an%C3%A1lisis-de-la-estructura-fallas-y-regulaci%C3%B3n-en-el-mercado-de-cr%C3%A9ditos-al-consumo.pdf?sequence=1&isAllowed=y>
- JARA, R. 2006. Ámbito de aplicación de la ley chilena de protección al consumidor: aplicación de la ley 19.496 y modificaciones de la ley Nº 19.555. En La protección de los derechos de los consumidores en Chile, Cuadernos de Extensión Jurídica 12, Facultad de Derecho de la Universidad de Los Andes, pp. 31-32

- JIJENA, R. 2002. Comercio electrónico, firma digital y derecho: Análisis de la Ley 19.799. Santiago, Editorial Jurídica de Chile.
- LORENZETTI, R.L. (dir). 2015. Código Civil y Comercial de la Nación, Comentado. Santa Fe, Rubinzal-Culzoni, tomo V.
- MATEU DE ROS, R. 2000. El Consentimiento y Proceso de Contratación Electrónica. En: MATEU DE ROS, R y CONDOYA J.M. Derecho de Internet: Contratación Electrónica y Firma Digital. Navarra. Aranzadi.
- MINISTERIO DE ECONOMÍA FOMENTO Y RECONSTRUCCIÓN. 2002 Decreto Supremo 181, de 2002.
- MOMBERG, R. 2013. Artículo 2º bis, En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile.
- MORENO, J. 1999. Contratos Electrónicos. Madrid, Editorial Marcial Pons.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. [en línea] <https://www.nist.gov/>
- PAILLAS, E. 1979. Estudios de Derecho Probatorio. Santiago, Editorial Jurídica de Chile.
- PANIZA, A. 2003. Contratación a distancia y defensa de los consumidores: Su regulación tras la reforma de la ley de Ordenación de Comercio Minorista y la ley de Servicio de la Sociedad de la Información y Comercio Electrónico. Granada, Editorial Comares.
- PARRONDO, F. 2019. La protección de datos personales al descubierto: Manual para el cumplimiento del RGPD y la LOPDGDD (Spanish Edition) (p. 50). Edición de Kindle.

- PINOCHET, R. 2009. Derecho Civil y Nuevas Tecnologías: la formación del consentimiento electrónico. Santiago, Legal Publishing Chile.
- PIZARRO, C. 2013. Artículo 17 E., En: PIZARRO, C., DE LA MAZA, I. y BARRIENTOS, F. La Protección de los Derechos de los Consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Legal Publishing Chile.
- PLOTT, G. 2005. Manual de Operaciones y Servicios Bancarios. Santiago, Editorial Jurídica de Chile.
- RIBAGORDA. A. 2002. Sistema de certificación: la firma y el certificado digital. En: FERNANDEZ, M., CREMADES, J. e ILLESCAS, R. Régimen Jurídico de Internet. Madrid, Wolters Kluwer.
- RIOSECO. E. 2017. La prueba ante la jurisprudencia: Derecho Civil y Procesal Civil. Santiago, Editorial Jurídica de Chile.
- RIVAS, C. 2021. Expertas enjuician el polémico artículo que entrega al Sernac facultades de protección de datos, Diario Financiero, jueves 1 de julio de 2021
- SERVICIO NACIONAL DEL CONSUMIDOR. 2019. Resolución Exenta Nº 0184 del 21 de marzo 2019, Circular Interpretativa sobre buenas prácticas en Comercio Electrónico. [en línea] <https://www.sernac.cl/portal/617/articles-9195_archivo_01.pdf>
- SILVA, P. 2003. Autonomía de la Voluntad, Contratación Electrónica y Protección del Consumidor. Revista chilena de Derecho Informático (3).
- SIMMONS, G. J. 1992. A survey of information Authentication. En Contemporary Cryptology, The science of information integrytyy, ed. GJ Simmons, IEEE Press, Nueva York.
- TEMBOURY, M. 2000. La Prueba de los Documentos Electrónicos en los Distintos Órdenes Jurisdiccionales, En: Derecho de Internet. Contratación Electrónica y Firma Digital. Navarra, Aranzadi

- TRONCOSO. A. 2009. La declaración de los ficheros de datos personales: acerca de un modelo centralizado o descentralizado. Revista de la Afencia de Protección de Datos de la Comunidad de Madrid. Madrid. Agencia de Protección de Datos de la Comunidad de Madrid, Seguridad y Protección de Datos Personales (38).
- VANINETTI, H.A. 2016. Identidad, reputación y muerte digital. Revista de Derecho de Familia y de las personas- La ley (9).
- VIOLLIER, P. 2017. El estado de la protección de datos personales en Chile [en línea], Santiago, Derechos Digitales, <https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf>

REFERENCIAS JURISPRUDENCIALES

- JUZGADO DE LETRAS DE LOS ANDES, Sentencia Nº C-372-2012 del 18 de junio de 2013;
- PRIMER JUZGADO DE POLICÍA LOCAL DE ANTOFAGASTA, sentencia Rol Nº 5101-17-7, 19 de julio de 2017.
- PRIMER JUZGADO DE POLICÍA LOCAL DE PUDAHUEL, Sentencia rol Nº 5697-9-2017, de agosto de 2018.
- TERCER JUZGADO DE POLICÍA LOCAL DE TEMUCO, sentencia Rol Nº 20703, 10 de noviembre de 2014.
- CORTE DE APELACIONES DE ARICA, Causa Nº 24/2012, Resolución Nº 6714, el 20 de junio de 2012.
- CORTE DE APELACIONES DE CHILLAN, Resolución Nº 15, 17 enero 2020;
- CORTE DE APELACIONES DE CONCEPCIÓN, Causa Nº 497/2015. Resolución Nº 123869, de 31 de agosto de 2015.
- CORTE DE APELACIONES DE COYHAIQUE, Causa Nº 14/2017, Resolución Nº 5508 de 18 de julio de 2017.
- CORTE DE APELACIONES DE COYHAIQUE, Causa Nº 77/2019 (P.local), Resolución Nº 20, de 6 de diciembre 2019.
- CORTE DE APELACIONES DE LA SERENA, Causa Nº 181-2008, Resolución Nº 21.265, de 11 de diciembre de 2008.
- CORTE DE APELACIONES DE SANTIAGO, Causa Nº 28-2019, diciembre 2020.
- CORTE DE APELACIONES DE SANTIAGO, Causa Nº 342/2016, Resolución Nº 660114, de 11 de julio de 2016.

- CORTE DE APELACIONES DE SANTIAGO, Causa Nº 915-2010, Resolución Nº 113415, de 14 de julio de 2010.
- CORTE DE APELACIONES DE SANTIAGO, Causa Nº 1484/2015. Resolución Nº 185742 de marzo de 2016.
- CORTE DE APELACIONES DE TEMUCO, Causa Nº 73/2013, Resolución Nº 37254, de 19 de junio de 2013.
- CORTE DE APELACIONES DE TEMUCO, Causa Nº 1344/2009, de 6 de noviembre de 2009.
- CORTE SUPREMA, Causa Nº 1533-2015, Resolución Nº 367725, del 7 de julio de 2016.
- CORTE SUPREMA, Causa Nº 3362/2006. Resolución Nº 9336 de 16 de Abril de 2008.
- CORTE SUPREMA, Causa Nº 26932-2015, Resolución 702286, del 6 de diciembre de 2016.