UNA PRIMERA MIRADA A LA LEY Nº 19.799

Iñigo de la Maza Gazmuri[♣]

Desde la dictación de la primera ley de firma electrónica en 1995 –la *Utah Digital Signature Act*- ha transcurrido un periodo considerable de tiempo. Al menos si se toma como parámetro el tiempo que Internet ha estado entre nosotros. A esta ley la siguieron un conjunto de cuerpos normativos tanto en Estados Unidos como en Europa y Latinoamérica. En el caso estadounidense actualmente existen la *Federal Electronic Signature Global and National Comerce Act* (E-Sign) y la *Uniform Electronic Transaction Act* (UETA). En el caso europeo en tanto, existieron leyes a nivel estatal como la italiana y alemana de 1997 y la portuguesa de 1999. El 13 de Diciembre de 1999, se dictó la Directiva 1999/93 del Parlamento Europeo y del Consejo en la que se establece un marco comunitario para la firma electrónica que deberían cumplir las futuras legislaciones a nivel estatal. El caso latinoamericano es también prolífico en regulaciones de firma electrónica. Así, por ejemplo, el caso de Perú, Argentina y Chile por mencionar solo algunos.

Este frenesí legislativo a nivel global va aparejado al explosivo desarrollo de las plataformas electrónicas y las crecientes posibilidades de interacción social que ellas permiten. Una de las modalidades de interacción social, la que ha determinado con mayor intensidad la fisonomía que va adquiriendo la Red es el comercio. Cuando la Red era más joven era frecuente escuchar un mantra sobre la nueva economía y las desmesuradas posibilidades del comercio electrónico. La Red era aterritorial, accesible desde cualquier lugar, los costos de transacción nos aproximaban al universo coaseano, bastaba estar allí y quienes no estuvieran simplemente se quedarían afuera de la nueva economía. Un par de años, sin embargo, bastaron para demostrar que no bastaba estar allí y que muchos de quienes estuvieron al principio fueron los primeros en retirarse.

Ahora bien, es cierto que la experiencia nos ha enseñado a ser cautelosos al momento de pronosticar las posibilidades del comercio electrónico, pero de allí no se sigue que no existan posibilidades para el comercio electrónico. Existen según lo demuestran todos los informes sobre la materia. Los informes también concuerdan en el hecho que uno de los principales obstáculos

---

[♣] El presente trabajo corresponde a una exposición del autor con el objeto de presentar la ley nº 19.799. Se ha procurado respetar el ritmo de la exposición oral, por lo mismo no existe remisión a fuentes. Sobre esto puede consultarse, entre otros, MARTINEZ NADAL, A. *La ley de firma electrónica.* Madrid : Civitas ,2001; ARRIETA CORTÉS. "Los prestadores de servicios de certificación de firma electrónica en el derecho chileno" en *Revista Chilena de Derecho Informático.* Nº 2. Centro de Estudios de Derecho Informático. Universidad de Chile, Facultad de Derecho, pp. 109-142; GAETE GONZÁLEZ, E. *Instrumento público electrónico.* Barcelona : Bosch ,2000; MATEU DE ROS, R. y CENDOYA MÉNDEZ DE VIGO, J. (coordinadores). *Derecho de internet : contratación electrónica y firma digital.* Navarra : Aranzadi ,2000; BARRIUZO RUIZ, C. *La contratación electrónica.* Madrid : Dykinson,1998; CONTRERAS STRAUCH, O. "Aspectos probatorios de la contratación electrónica y SANDOVAL LÓPEZ, R. "Análisis del Proyecto de Ley sobre Firma Electrónica y Servicios de Certificación de Firma Electrónica" Ambos en DE LA MAZA GAZMURI, I. (Coordinador) *Derecho y Tecnologías de la Información.* Universidad Diego Portales, Facultad de Derecho. 2002, pp. 197-222 y 225-238.

del comercio electrónico es la confianza. Aquí entra la firma electrónica y las numerosas leyes que la regulan.

Cuando negociamos en plataformas electrónicas, el documento de papel es reemplazado por el documento electrónico y esto nos enfrenta a dos problemas. De una parte ignoramos con quien estamos negociando, de otra no tenemos certeza que el mensaje que estamos recibiendo sea exactamente el mismo que se nos envío. La pantalla de nuestro computador es opaca, no nos permite saber quién está del otro lado, tampoco nos permite saber con exactitud que aquel mensaje que llegó a nuestra casilla de correo electrónico es exactamente el mismo que nos envió el receptor.

La incertidumbre que genera la opacidad de la Red no es una buena aliada del comercio electrónico y determina severas limitaciones a sus posibilidades. Lo que se precisa para que esta actividad disminuya sus fricciones es algún mecanismo que satisfaga las funciones que hace siglos viene cumpliendo la firma autógrafa. Ese mecanismo es la firma electrónica. La firma electrónica y el sistema de confianza que genera contribuyen a disminuir la incertidumbre que generan las plataformas electrónicas, promoviendo la confianza acerca de la identidad de quien envía el mensaje y sobre el contenido de éste.

Para que esto suceda la firma electrónica debe asegurar:

1. que el mensaje proviene de la persona que dice que lo envía
2. que no ha sido alterado en el camino
3. que el emisor del mensaje no podrá negar su envío, ni la persona destinataria su recepción

Los requisitos que debe satisfacer la firma electrónica para cumplir con su cometido son los siguientes:

- **autenticación:** esto es que asegure la identidad del remitente
- **integridad:** esto es que asegure que el mensaje no ha sido alterado en el tránsito
- **no rechazo:** esto es que la parte que lo ha enviado no pueda negar su actuación

1. La ley nº 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

En los minutos que siguen me interesa detenerme sobre la firma electrónica, aunque no en términos generales, sino a su regulación en la ley chilena. Específicamente a la ley nº 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (en adelante la Ley). Por lo mismo mi examen de la firma electrónica quedará comprendido dentro de una descripción de dicha ley.

Para examinar la Ley me detendré en primer lugar, y brevemente, en los principios que la informan; en segundo lugar examinaré los modelos de firma electrónica que regula; en tercer lugar, me revisaré los actores que vincula el sistema de confianza que pretende instaurar la Ley: los certificadores, la entidad acreditadora y los usuarios; finalmente, en cuarto lugar, daré noticia de la tecnología que actualmente utiliza la firma electrónica avanzada.

La opción de explorar la ley completa y no detenerme únicamente en la firma electrónica se justifica por dos razones estrechamente vinculadas. La primera de ellas es que no resulta posible entender la forma en que la firma electrónica cumple su función sin referirse a los demás puntos. La segunda es que la firma electrónica es solo una de las partes del sistema de confianza y es el sistema en su conjunto y no solo la firma lo que contribuirá a aligerar las aprehensiones de los usuarios y, esperemos, a generar las condiciones para que en el futuro el comercio electrónico alcance sus potencialidades.

Dos advertencia antes de comenzar. En general, esta exposición no analiza la ley, más bien la expone sistemáticamente. El tiempo de este seminario solo permite intentar exponer ordenadamente este cuerpo normativo. Una aproximación más crítica deberá esperar otra oportunidad. En segundo lugar prescindiré del Título II –Uso de firmas electrónicas por los órganos del Estado. La razón de lo anterior es por una parte el tiempo de esta exposición y, por otra, el hecho que el examen de este título resulta innecesario para comprender la forma en que funciona la firma electrónica, la función del Título II es permitir el uso de la firma electrónica por los órganos del Estado, comprendiendo cómo funciona la firma electrónica el Título se lee sin dificultades.

Dicho eso es posible comenzar a exponer la ley.

2. Los principios de la ley Nº 19.799

En su primer artículo la Ley establece cinco principios, a saber: libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al legal. El legislador se preocupó de señalar expresamente la función hermenéutica que cumplen estos principios al establecer que cualquier interpretación de los preceptos de esta ley deberá guardar armonía con ellos.

El primer principio –la libertad de prestación de servicios- guarda relación con una disputa frecuente a nivel comparado al momento de regular las firmas electrónicas: la necesidad de que el Estado autorizará a quienes emitieran firmas electrónicas. Las opciones más frecuentes eran dos. En la primera solo podían emitir firmas electrónicas quienes tuvieran autorización del Estado. En la segunda podían emitir firmas electrónicas todos quienes lo desearan. La solución chilena se situó en la mitad de ambos extremos, intentando equilibrar las bondades del mercado con la necesidad de promover confianza en el comercio electrónico. De esta manera bajo la regla chilena cualquiera puede emitir firmas electrónicas; sin embargo, para emitir firmas electrónicas avanzadas es necesario que, con anterioridad a la emisión, el Estado haya aprobado al prestador de servicios. En resumen, en Chile existe plena libertad de prestación de servicios de firma electrónica. Cuando se trata de firmas electrónicas avanzadas, sin embargo, son libres de emitirlas todos aquellos prestadores que hayan sido previamente autorizados por el Estado.

El segundo principio –la libre competencia- constituye un nuevo guiño al mercado y un complemento a la regla anterior. De lo que se trata es que el Estado y sus agencias no deberían intervenir en el mercado de los prestadores favoreciendo arbitrariamente a alguno de ellos.

El tercer principio –neutralidad tecnológica- aspira a evitar la obsolescencia que arriesga cualquier regulación que se comprometa con una determinada tecnología. De lo que se trata es de establecer instituciones permanentes que logren acoger adecuadamente los cambios tecnológicos. Por lo mismo, por ejemplo, al definir la firma electrónica avanzada, el legislador no hace mención a la tecnología que la soporta –actualmente la encriptación asimétrica- sino a los requisitos que debe satisfacer aquella tecnología, cualquiera que fuera.

El cuarto principio –la compatibilidad internacional- se relaciona con la estandarización de los sistemas de confianza a nivel global. La firma electrónica funciona con "externalidades de red", es decir su valor para cada usuario aumenta en la medida que se integren más usuarios al sistema. La idea entonces es que la tecnología que se utilice en Chile sea convergente con la utilizada en otros países de manera que permita el diálogo entre una y otra.

El quinto principio –la equivalencia del soporte electrónico al soporte papel- es, sin duda, el más relevante de esta ley. La norma disuade toda duda posible respecto del valor jurídico de los documentos electrónicos y, por lo mismo, de los actos jurídicos que consten en él. Con escasas excepciones, todos aquellos documentos en soporte papel a los que el legislador les concede algún valor jurídico pueden ser plasmados en soporte electrónico, manteniendo los efectos jurídicos que el ordenamiento les reconoce. El legislador explicita esta regla en los artículos tercero y séptimo utilizando los siguientes términos:

Art. 3º 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 de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito.

Art. 7º Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte papel.

Como se advierte, el legislador se preocupa de extender expresamente el principio consagrado en el artículo primero a las relaciones entre privados y a los actos del Estado.

3. Los modelos de firma electrónica.

La Ley regula dos modelos de firma electrónica. El primero de ellos, al que denominaré FE, se encuentra definido en la letra f) del artículo 2 como "cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar formalmente a su autor". El segundo refiere es lo que la Ley denomina firma electrónica avanzada –en adelante FEA. Definida en la letra g) del mismo artículo como "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".

Como no es difícil advertirlo, ambas firmas son diversas y a cada una se exigen requisitos diversos y reconocen distintos efectos. Conviene detenerse primero en los requisitos de cada una, a continuación en su equivalencia con la firma autógrafa y, en tercer lugar, en su valor probatorio.

- Requisitos.

FE.- La amplitud de la definición resulta inversamente proporcional a la exigibilidad de los requisitos. En verdad, lo único que requiere la FE es que el receptor de un documento electrónico sea capaz de identificar formalmente al emisor. Por lo mismo, dentro de este concepto quedarían comprendidas técnicas como la simple indicación del nombre al final de un mensaje electrónico o una firma manual digitalizada. Como se verá más adelante, esto determina que la equivalencia de la FE sea menor que la de la FEA, igual cosa sucede respecto del valor probatorio.

FEA.- La FEA debe satisfacer cuatro requisitos. En primer lugar debe haber sido certificada por un prestador acreditado; en segundo lugar debe haber sido creada usando medios que el titular mantiene bajo su exclusivo control; en tercer lugar debe permitir la detección de cualquier modificación al mensaje una vez que ha sido firmado; finalmente debe verificar la identidad del titular.

Prestador acreditado.- En Chile únicamente aquellos prestadores de firmas electrónicas acreditados por el Estado pueden emitir FEA. A diferencia, por ejemplo del caso europeo, los requisitos de la firma electrónica no son solo técnicos, se requiere además la autorización de un órgano público, la Subsecretaría de Economía. Dicho de otra manera aún cuando la firma electrónica que provea al mercado satisfaga todos los requisitos técnicos que se le exigen a nivel comparado y en el derecho chileno, el legislador no la reconoce como tal si no ha sido emitida por un prestador acreditado. Volveré sobre esto al momento de examinar los actores del sistema.

Creada usando medios que el titular mantiene bajo su exclusivo control.- Uno de los requisitos que se exigen a la FEA para que promueva la confianza en el comercio electrónico es que garantice la identidad de quien firma el mensaje. El requisito apunta en esta dirección. Si la firma únicamente puede ser creada a través de medios que se encuentran en poder de su titular, un documento firmado con firma electrónica avanzada garantiza –al menos legalmente- que el documento fue firmado por el titular de la firma electrónica avanzada.

Permitir la detección de cualquier modificación.- El segundo requisito que debe satisfacer la firma electrónica para promover confianza es la integridad del mensaje. La utilización de firma electrónica debe permitir la identificación de cualquier modificación que haya sufrido el documento con posterioridad a la firma.

Verifica la identidad del titular.- Hasta el momento la firma nos ha garantizado que quien envió el mensaje es el titular de la firma y que el documento no ha sufrido ninguna modificación con posterioridad a su firma. Lo tercero que se le exige a la FEA es que garantice que el titular de la firma sea quien dice ser. Un ejemplo ayudará a entender esto. Si recibo un mensaje de X firmado electrónicamente puedo tener certeza que solo pudo haber sido enviado por la persona que dice llamarse X y que el mensaje no ha sido modificado. Lo que me resta por saber es si la persona

que dice llamarse X es efectivamente X y no Y que se hizo pasar por X al momento de obtener su firma electrónica. Volveremos sobre esto al examinar los actores del sistema.

- Equivalencia.

Hace algunos minutos indiqué que el artículo primero de la Ley establecía como principio de la ley la equivalencia de soporte e indiqué como quedaba plasmada esa equivalencia en los artículos tercero y séptimo. Ahora es el momento de matizar esa afirmación.

Si bien la equivalencia es amplia, no es absoluta. El mismo artículo tercero se encarga de aclarar que existen excepciones. Entre estas excepciones hay algunas que alcanzan a la FE y a la FEA y otras que únicamente alcanzan a la FE. Las primeras –denominémoslas excepciones comunes- se presentan en los siguientes actos o contratos:

a) aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico;
b) aquellos en que la ley requiera la concurrencia personal de alguna de las partes
c) aquellos relativos al derecho de familia

Las segundas se aplican únicamente a la FE y a ellas se refiere el artículo quinto al establecer que "Los documentos electrónicos que tengan la calidad de instrumento público, deberán subscribirse mediante firma electrónica avanzada".

- Valor probatorio.

El legislador ha declarado expresamente que los documentos electrónicos pueden presentarse en juicio. Esto aligera, al menos en materia civil, la situación anterior del documento electrónico cuya aceptación –a diferencia de lo que sucede en el proceso penal- era posible únicamente a través de la utilización de un concepto amplio de documento, de la prueba pericial o de las presunciones.

Respecto al valor probatorio, la distinción entre FE y FEA cobra extraordinaria importancia. La regla –aunque expresada en forma ligeramente diversa en el artículo 5º- es que aquellos documentos firmados con FEA tienen el valor probatorio de un instrumento público. Si han sido suscritos con FE, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales. Su valor será generalmente el de un instrumento privado.

Conviene hacer dos precisiones respecto a la regla del artículo quinto. La primera de ellas es que la firma electrónica concede el valor probatorio de instrumento público a aquellos documentos firmados con FEA, esto, sin embargo, no los transforma en instrumentos públicos. Los documentos privados firmados con FEA conservan su calidad de tales, lo que se modifica es su valor probatorio.

La segunda precisión refiere a la equiparación probatoria entre instrumento público y documento firmado con FEA. Como resulta bien sabido, el artículo 1700 del Código Civil establece que el instrumento público hace plena prueba en cuanto al hecho de haberse otorgado y su fecha y,

respecto de los declarantes, acredita fehacientemente la verdad de las declaraciones de los comparecientes. Pues bien respecto de lo primero y lo tercero –haberse otorgado y verdad de las declaraciones- no existe mayor problema, los requisitos de la FEA permiten la equiparación sin fricciones. No sucede lo mismo respecto del segundo –la fecha. Como está definida la FEA en la ley ésta resulta incapaz de garantizar la fecha en que se emitió el documento. Es cierto que existen servicios asociados a la firma electrónica como el *time stamping* que permiten acreditar el momento, pero la definición de la ley chilena no los exige.

4. Los actores que vincula el sistema de confianza.

En el caso chileno la regulación de la firma electrónica vincula a tres actores: los prestadores de servicios de certificación, la entidad acreditadora y los usuarios. En la descripción más sintética posible la función de los primeros es poner a disposición de los usuarios la tecnología necesaria para emitir firmas electrónicas. La función de la segunda es la supervigilancia del mercado de prestadores de servicios de certificación con especial énfasis en aquellos que se acreditan. Finalmente los usuarios son quienes utilizan la firma electrónica para autenticar sus documentos electrónicos. Esta es, sin embargo, una descripción excesivamente breve, conviene detenerse por algunos minutos en cada uno de ellos.

4.1.Los prestadores de servicios de certificación (PSC).

Una mirada a la regulación de los PSC en la Ley –definidos en su artículo 2 letra c- permite definirlos como personas jurídicas, nacionales o extranjeras, públicas o privadas que entregan certificados de firma electrónica, sin perjuicio de los demás servicios que puedan realizar.

Guardando simetría con la regulación de dos modelos de firma electrónica, el título que trata sobre los PSC distingue según se trate de prestadores acreditados –aquellos que pueden emitir firma electrónica avanzada- y aquellos que no se han acreditado –y, por lo tanto, no pueden emitir esa especie de firmas. Me detendré primero en las funciones de los PSC, luego en sus obligaciones, En tercer lugar examinaré la responsabilidad de los PSC y, en cuarto lugar me referiré brevemente los certificados de firma electrónica.

- *Las funciones de los PSC.*

Como ya se ha advertido, el giro de los PSC puede ser amplio, con todo lo que interesa examinar aquí son sus funciones características son (1) la generación de los datos de creación de firma, (2) la certificación y (3) la homologación.

1) Generación de los datos de creación de firma.- Los datos de creación son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica. Según lo dispone el artículo 25 del Reglamento de la ley, son lo PSC quienes deben generan dichos datos.

2) Certificación.- la certificación es aquel proceso a través del cual el PSC da fe del vínculo existente entre la identidad del titular de la firma y los datos de creación de la misma. De lo que se trata es que el PSC compruebe la identidad de quien solicita la firma antes de

entregarle los datos de creación. De esta manera se garantiza que los datos de creación se encontrarán asociados a la persona del titular de la firma electrónica. Comprobada la identidad del titular de la firma electrónica, el PSC emite un certificado el cual se publica en un registro de acceso público disponible a través de medios electrónicos. Volveré sobre el certificado al examinar la tecnología que soporta la FEA actualmente.

3) Homologación.- Establecida en el artículo 15 de la Ley, la homologación opera respecto de la PSC de FEA. La idea es dotar a certificados emitidos por PSC domiciliados fuera de Chile, que satisfacen los requisitos establecidos por la Ley del valor de una FEA. Para que esto suceda, el artículo 29 del Reglamento exige al PSC que desea homologar que demuestre a la Entidad Acreditadora que el PSC que emitió los certificados satisface los requisitos técnicos que se le exigirían en Chile para emitir FEA. La homologación se hace bajo la responsabilidad del PSC chileno.

- *Las obligaciones de los PSC*

Ya he afirmado que la Ley distingue entre PSC acreditados y aquellos que no los son, fijando, en su artículo 12, obligaciones comunes para ambos y obligaciones exclusivas para los acreditados.

Obligaciones comunes a todos los PSC.

1. Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano.- Según lo dispuesto en el artículo seis del Reglamento, las prácticas de certificación constituyen una descripción detallada de las políticas, procedimientos y mecanismos que el certificador se obliga a cumplir en la prestación de servicios. En verdad, las prácticas de certificación constituyen una oferta indeterminada de contrato por adhesión en el que existe un cierto dirigismo estatal a través de las cláusulas que obligatoriamente deben incorporarse al contrato según lo dispuesto en el artículo seis.

2. Mantener un registro de acceso público de certificados, en el que quedará constancia de los emitidos y los que queden sin efecto, en los términos señalados en el reglamento.- Se trata de que el PSC disponga de un sitio electrónico accesible al público en el que se encuentren identificados los certificados que ha otorgado y el estado en que se encuentran (vigente, revocado, suspendido). Para mantener ese registro la Ley autoriza al titular a tratar los datos del titular para ese solo efecto y lo obliga a conservarlos por un plazo no inferior a seis años. En su artículo 11 el Reglamento dispone que si el PSC cesara en su actividad deberá transferir esos datos a otro PSC acreditado o a una empresa especializada en la custodia de datos electrónicos, por el plazo que excede para completar los seis años.

3. Comunicar a los titulares de firma electrónica certificadas por él, el cese voluntario de las actividades del PSC y, no existiendo oposición del titular de la firma electrónica, transferir los datos de certificación a otro PSC- El aviso de cese que debe dar el PSC a los titulares de firmas electrónicas debe ser con una antelación de, al menos, dos meses al término de sus actividades. La obligación de transferir los datos a otro PSC se relaciona con la necesidad de

generar continuidad respecto de las firmas electrónicas y certificados emitidos por el PSC que cesa en sus actividades.

4. Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las leyes nº 19.496, sobre Protección de los Derechos de los Consumidores, y nº 19.628, sobre Protección de la Vida Privada.

Obligaciones exclusivas de los PSC acreditados.

1. Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora las resoluciones que los afecten.- Como ya se ha advertido la supervigilancia de los PSC se encuentra a cargo de la Entidad Acreditadora la que monitorea la actividad de los PSC acreditados, la publicación de sus resoluciones en los sitios de los PSC hace accesible información sobre los PSC a los consumidores de firmas electrónicas.

2. Comprobar fehacientemente la identidad del solicitante de una FEA.- Como ya se ha advertido una de las funciones del PSC es certificar la coincidencia entre los datos de creación de la firma y su titular –esta es la función del certificado. Con este objeto la Ley exige al PSC acreditado que certifique la identidad a través de la concurrencia personal del titular de la FEA o de su representante legal si se trata de una persona jurídica. El solicitante podrá comparecer ante el PSC o ante notario u oficial del registro civil.

3. Pagar un arancel de supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá los costos del peritaje y del sistema de acreditación e inspección de los prestadores.- Sobre los costos del peritaje e inspección volveré al examinar la entidad acreditadora.

4. Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle 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.- Esta es otra manifestación de la supervigilancia que realiza la Entidad Acreditadora sobre las funciones de los PSC acreditados.

5. 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.- Una vez más lo que se encuentra en juego es la continuidad del servicio, esta vez la causa del problema es la cancelación de la inscripción. Sobre esto volveré más adelante.

6. 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 pagos.- Como se advertirá la Entidad Acreditadora certifica que en un determinado momento el PSC satisface todos los requisitos para emitir FEA, si existe algún cambio significativo en la

situación del PSC es posible que lesione el cumplimiento de sus requisitos y, por lo mismo, que arriesgue la acreditación del PSC.

- *La responsabilidad de los PSC.*

Respecto de la responsabilidad de los PSC existen tres puntos que conviene considerar. El primero de ellos es que el artículo 14 de la Ley establece que corresponderá al PSC demostrar que actuó con la debida diligencia. Como se sabe, respecto de la responsabilidad contractual esta es la regla en lo que refiere a la prueba de la culpa en el incumplimiento del contrato. En materia extracontractual no sucede lo mismo, allí quien alega el daño debe acreditar la culpa. Teniendo en cuenta que los daños generados por el PSC pueden generarse a raíz del incumplimiento del contrato que lo vincula con el titular de la firma o bien extracontractualmente respecto de terceros, la Ley modifica en este sentido la regla del artículo 1698 del Código Civil.

El segundo punto refiere a la obligación de los PSC acreditados de contratar un seguro que cubra su responsabilidad civil por un mínimo de 5.000 unidades de fomento y que cubre tanto los certificados emitidos por el PSC como aquellos que haya homologado. Según lo dispuesto en el artículo 12 del Reglamento, el seguro deberá contener las siguientes estipulaciones mínimas:

a) Una suma asegurada de al menos equivalente a cinco mil unidades de fomento;
b) La ausencia de deducibles o franquicias, en la parte de la indemnización que no exceda de cinco mil unidades de fomento
c) La responsabilidad civil asegurada, que comprenderá la originada en hechos acontecidos durante la vigencia de la póliza, no obstante sea reclamada con posterioridad a ella.

El tercer punto refiere a la responsabilidad del Estado. El inciso final del artículo 14 dispone que en ningún caso la responsabilidad que pueda emanar de una certificación efectuada por un PSC acreditado comprometerá la responsabilidad pecuniaria del Estado.

- *Los certificados de firma electrónica.*

El certificado es un documento electrónico cuya función principal es la comprobación de la identidad del titular de la firma electrónica. La Ley se refiere a las menciones que debe contener el certificado, sus límites funcionales y a su pérdida de efectos.

El artículo 15 de la Ley exige que los certificados, sean de FE o de FEA, contengan las siguientes menciones:

a) Un código de identificación único del certificado;
b) Identificación del prestador de servicio 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 deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y
d) Su plazo de vigencia.

En su inciso cuarto, el artículo 14 dispone que el PSC podrá establecer límites funcionales al certificado –por ejemplo monto o naturaleza de las transacciones en que puede ser utilizado. Dichos límites resultarán oponibles al titular o a terceros únicamente en la medida que estén incorporados al certificado en forma clara, de manera que sean reconocibles.

El artículo 16 indica las causas que privan de efecto a los certificados; ellas son las siguientes:

1) Por extinción del plazo de vigencia del certificado, el cual no podrá exceder de tres años contados desde la fecha de emisión;
2) Por revocación del prestador, la que tendrá lugar en las siguientes circunstancias:
a) A solicitud del titular del certificado;
b) Por fallecimiento del titular o disolución de la persona jurídica que represente, en su caso;
c) Por resolución judicial ejecutoriada, o
d) Por incumplimiento de las obligaciones del usuario establecidas en el artículo 24;
3) Por cancelación de la acreditación y de la inscripción
del prestador en el registro de prestadores acreditados que señala el artículo 18, en razón de lo dispuesto en el artículo 19 o del cese de la actividad del prestador, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad con lo dispuesto en las letras c) y h) del artículo 12, y
4) Por cese voluntario de la actividad del prestador no acreditado, a menos que se verifique el traspaso de los datos de los certificados a otro prestador, en conformidad a la letra c) del artículo 12.

4.2. La entidad acreditadora (EA).

En el caso chileno la EA es la Subsecretaría de Economía, Fomento y Reconstrucción y es ante ella que los PSC que deseen emitir FEA deben acreditarse. Según lo dispuesto en el artículo 13 del Reglamento, la EA podrá contratar expertos para que lleven a cabo el procedimiento de acreditación.

El procedimiento de acreditación tiene por objeto que el PSC demuestre a la EA que satisface los requisitos tecnológicos y humanos para otorgar los certificados según lo exigen la Ley y su Reglamento.

La Ley establece requisitos de acreditación, dispone el procedimiento para conseguirla, las causales que determinan la pérdida de la acreditación, el procedimiento que se encuentra a disposición de los PSC para reclamar la revocación de la acreditación, las consecuencias de la revocación y la facultad inspectora de la EA. En ese orden serán expuestos.

- Los requisitos

El artículo 17 establece que el PSC que desee acreditarse debe satisfacer los siguientes requisitos:

a) Demostrar la fiabilidad necesaria de sus servicios;
b) Garantizar la existencia de un servicio seguro de consulta del registro de certificados emitidos;

c) Emplear personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados;
d) Utilizar sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;
e) Haber contratado un seguro apropiado en los términos que señala el artículo 14, y
f) Contar con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación

- El procedimiento.

El procedimiento se encuentra regulado en el artículo 18 de la Ley y comienza a través de una solicitud que presenta el PSC ante la EA. Dicha solicitud debe acompañar aquellos antecedentes que permitan a la EA verificar que el PSC satisface los requisitos establecidos por la Ley. Se posterga, sin embargo, la póliza que da fe de la contratación del seguro requerido por el artículo 14 para el momento en que todos los demás requisitos hayan sido auditados. La solicitud deberá contener además una individualización del PSC incluyendo su nombre o razón social, su RUT, nombre y RUT del representante legal, domicilio y dirección de correo electrónico.

Recibida la solicitud la EA procederá a un examen formal de estos, en caso de reprobarlo la EA lo comunicará al PSC dentro del plazo de tres días hábiles con el objeto de que subsane las deficiencias detectadas. Aprobado este primer examen la EA procederá a examinar si el PSC satisface los requisitos establecidos por la Ley y las obligaciones que ésta le impone al PSC. En caso que no los satisfaga la EA determinará si pueden o no ser subsanadas las deficiencias. En caso de lo que sea la EA podrá acreditar al PSC, previa autorización de un plan de medidas correctivas. Si las deficiencias no pueden ser subsanadas la EA dictará una resolución rechazando la solicitud.

En el caso de que el PSC satisfaga los requisitos o bien en aquellos donde se le ha establecido un plan de medidas correctivas, la EA certificará dicha circunstancia y le notificará que dispone de un plazo de 20 días para contratar el seguro. Contratado, el PSC será incorporado a un registro público de PSC acreditados.

- La revocación de la acreditación.

El artículo 19 establece tres causas por las cuales el PSC acreditado puede perder su calidad de tal, a saber:

a) Solicitud del prestador acreditado;
b) Pérdida de las condiciones que sirvieron de fundamento a su acreditación, la que será calificada por los funcionarios o peritos que la Entidad Acreditadora ocupe en la inspección a que se refiere el artículo 20, y
c) Incumplimiento grave o reiterado de las obligaciones que establece esta ley y su reglamento.

La revocación deberá estar contenida en una resolución fundada de la EA.

- El procedimiento para impugnar la revocación.

El procedimiento para impugnar la resolución que revoca la certificación en los casos de las letras b) y C) del artículo 19 posee dos etapas. La primera es en sede administrativa, ante la EA, y la segunda en sede judicial, ante la Corte de Apelaciones del domicilio del interesado. En sede administrativa el interesado tiene un plazo de cinco días desde la notificación de la resolución para reclamar y la EA un plazo de 30 días para resolver. Desde la fecha en que la EA resuelva o bien desde aquella en que se certifique que ha transcurrido el plazo en que debía pronunciarse, el interesado dispone de diez días para acudir a la Corte de Apelaciones. Su recurso se rige por las reglas del recurso de protección y la resolución de la Corte no será susceptible de recurso alguno.

- Las consecuencias de la revocación.

De la revocación surgen efectos para el PSC, la EA y los titulares de FEA emitida por el PSC. Revocada la inscripción la EA cancelará la inscripción del PSC del Registro de PSC acreditados. El PSC deberá comunicar a sus titulares de firma electrónica esta situación. La EA publicará un aviso dando cuenta de esta situación. Respecto de los titulares, a partir de la fecha de esta publicación sus certificados quedarán sin efecto, a menos que sean transferidos a otros PSC acreditados según lo dispuesto en la letra h) del artículo 12 de la Ley.

- La facultad inspectora

Con el objetivo de realizar la supervigilancia de la actividad de los PSC, la Ley entrega en su artículo 20 a la EA la facultad inspectora sobre la actividad de estos. Esta facultad le permite requerirles información y ordenar visitas a sus instalaciones mediante funcionarios o peritos especialmente contratados en conformidad al Reglamento.

4.3. Los usuarios.

Usuarios son aquellos que obtienen su firma electrónica de un PSC. La Ley regula sus derechos y obligaciones en su Título VI. Teniendo en cuenta la extensión del artículo intentaré presentarlos resumidamente.

- *Los derechos.*

El artículo 23 de la Ley establece entre sus números 1 y 10 seis derechos para los titulares de firmas electrónicas la mayoría de ellos resultan exigibles al PSC, solo el contenido en el número 9 tiene como sujeto pasivo a la EA. El primero es el derecho a la información contenido en los numerales 1,3,4,5,6. El usuario tiene derecho a ser informado, entre otras cosas sobre: las características generales del procedimiento de creación y verificación de la firma electrónica y las prácticas de certificación; los usos del certificado y sus limitaciones, el domicilio del PSC en Chile, el cese de su actividad y la cancelación de la inscripción.

El segundo es el derecho a la confidencialidad respecto de la información que ha entregado al PSC (numeral 2). El cumplimiento de esta obligación por parte del PSC implica que disponga de la tecnología suficiente para proteger los datos personales que le entregado el titular de la firma.

El tercero es el traspaso de datos (numeral 7). Según se ha examinado, en aquellos casos en que el PSC cesa sus servicios voluntariamente o por cualquier otra causa el titular de la firma tiene derecho a que se traspase su certificado a otro PSC.

El cuarto es la calidad exacta y publicidad no deseada (numeral 8). La calidad exacta es una regla general del derecho de contratos, los contratantes tienen derecho a que se les proporcione exactamente lo convenido. La redacción de la Ley es curiosa, establece que el titular tendrá derecho "a que el prestador no proporcione más servicios y de otra calidad que los que haya pactado". Es una mención innecesaria, bastan las reglas generales en materia de contratos. Respecto a la publicidad no deseada, se establece un sistema de *opt-in* es decir el PSC no le puede enviar ningún tipo de publicidad al usuario, salvo que éste haya autorizado previamente el envío.

El quinto es el acceso al registro (numeral 9) se trata del registro de prestadores acreditados que mantiene la EA.

Finalmente, el sexto es el derecho a ser indemnizado y hacer valer los seguros comprometidos (numeral 10).

- *Obligaciones.*

Los usuarios poseen dos obligaciones. La primera de ellas refiere a la exactitud de los datos que le entregan al PSC al momento de la certificación. La segunda refiere a la custodia adecuada de los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador. Se trata aquí de que el usuario custodie diligentemente los mecanismos que le permiten firmar electrónicamente los documentos.

5. La tecnología de la firma electrónica.

La tecnología usada en forma mayoritaria en el mundo para las firmas electrónicas avanzadas es la criptografía asimétrica. A las firmas electrónicas que utilizan este sistema se les denomina firmas electrónicas digitales.

La criptografía es la ciencia que utiliza las matemáticas para encriptar y desencriptar información, esto es transformar la información en formas aparentemente ininteligible y devolverla a su forma original.

La criptografía utiliza un algoritmo matemático para cifrar información que solo puede ser descifrada por quien posea una clave. Tradicionalmente esta clave era secreta y compartida (criptografía simétrica). Actualmente se utiliza criptografía asimétrica esto es aquella que utiliza dos claves, una pública y una privada. La clave privada es conocida únicamente por su titular (puede que ni siquiera él la conozca y ésta se mantenga en una tarjeta inteligente). La clave pública es accesible para cualquiera y lo más frecuente será que conste en directorios públicos.

La encriptación asimétrica permite realizar firmas que garantizan autenticidad, integridad y no rechazo.

- *El procedimiento de las firmas digitales.*

El emisor del mensaje lo cifra parte del mensaje utilizando su clave privada y lo envía al receptor. Aún cuando es posible encriptar el mensaje completo esto resulta sumamente costoso. Una vez que reciba el mensaje, el receptor utilizará la clave pública para desencriptar aquella porción del mensaje encriptado. Si la llave pública logra desencriptar el mensaje entonces el emisor ya no tendrá dudas acerca del emisor. Esto garantiza la autenticidad del emisor, resta la integridad del mensaje; ella es garantizada por la función *hash.*

La función *hash* es un algoritmo que se utiliza para reducir la longitud del mensaje. Independientemente de la longitud del mensaje al aplicar la función ésta produce un resumen de 160 bits. Este resumen es irreversible y único. Cualquier modificación que se haga al mensaje original va a ser detectada al confrontar el mensaje con este resumen.

Al recibir el mensaje y luego de desencriptar la parte encriptada con la llave pública, el receptor aplicará la función *hash* al texto recibido, si el resumen es igual al que viajaba con el texto, entonces sabrá que el documento no ha sufrido alteraciones.

Sin perjuicio de lo complejo que resulte esto, para el usuario de la firma y para el receptor son procedimientos extraordinariamente sencillos. En el caso del primero bastará que utilice su clave privada para que parte del mensaje quede encriptada y se genere un resumen *hash.* En el caso del segundo bastará que utilice la llave pública para desencriptar la porción cifrada del mensaje y generar un resumen *hash* del documento recibido y compararlo con el resumen original.

La clave del sistema entonces se encuentra en las claves privada y pública, por lo mismo estas deben reunir algunos requisitos para garantizar la autoría e integridad del mensaje, a saber:

1) Debe tratarse de un par de claves seguras, es decir no ha de ser posible obtener la clave privada a partir de la clave pública.

2) El par de claves ha de ser único, es decir no deben existir dos o más personas con la misma clave.

3) Finalmente, el procedimiento de generación ha de ser adecuado, de forma que no se pueda obtener la clave privada reproduciendo el procedimiento de generación de claves.