IUS REVISTA DEL INSTITUTO DE CIENCIAS JURÍDICAS DE PUEBLA, MÉXICO. ISSN 1870-2147. NUEVA ÉPOCA VOL. 12, No. 41. ENERO - JUNIO DE 2018. PP 241-266

Entre la firma electrónica y la firma digital: aproximaciones sobre su regulación en el Perú*

Between Electronic Signature and Digital Signature: Approaches on its Regulation in Peru

José Francisco Espinoza Céspedes**

RESUMEN

El desarrollo de las operaciones electrónicas normalmente se efectúa en entornos inseguros, por lo que requieren ciertos mecanismos técnicos que permitan identificar al firmante y acreditar la voluntad manifestada en un medio seguro revestido de legalidad. En ese sentido, la presente investigación busca determinar cuáles son los aspectos normativos que permite el uso de las firmas electrónicas y las firmas digitales en el Perú; en ese ámbito también se busca conocer los entornos donde las tecnologías antes mencionadas pueden ser admitidas legalmente por el Derecho Informático.

PALABRAS CLAVE

Firma Electrónica, Firma Digital, Voluntad por Medios Electrónicos, Seguridad, Derecho Informático.

ABSTRACT

The development of electronic operations is normally carried out in unsafe environments, and therefore requires certain technical mechanisms to identify the signer and to be able to demonstrate the will manifested in a secure environment covered by legality. In this sense, the present research seeks to determine the regulatory aspects that allow the use of electronic signatures and digital signatures in Peru this field also seeks recognize the environments where the above mentioned technologies can be legally admitted by Computer Law.

KEYWORDS

Electronic Signature, Digital Signature, Disposition for Electronic Media, Security, Computer Law.

*Artículo recibido el 8 de junio de 2017 y aceptado el 24 de septiembre de 2017

**Universidad Tecnológica del Perú, Universidad Norbert Wiener. (jofraec@gmail.com) orcid 0000-0001-8436-5960

SUMARIO

1. Introducción

El mundo está realmente interconectado. Cada día se generan millones de operaciones electrónicas y éstas requieren niveles de seguridad que identifiquen adecuadamente a los firmantes, quienes interactúan en el ciberespacio[1] para comprar bienes o adquirir servicios de calidad.

En dicho contexto, Perú no puede ser ajeno a una realidad cuyos problemas legales se deben resolver desde el derecho informático,[2] con una visión iusinformática, donde derecho y tecnología se unen para facilitar las operaciones electrónicas en entornos globalizados e interconectados.

Es así que el sistema jurídico peruano se ha adaptado a las nuevas exigencias de los tiempos modernos. En concordancia con los avances del derecho informático, ha regulado en diversos cuerpos normativos tanto las firmas electrónicas como las firmas digitales.

El primer marco legal que dio origen a una revisión iusinformática para la generación de operaciones con firma electrónica fue la Ley 27269, Ley de Firmas y Certificados Digitales.[3] Posteriormente, en junio del año 2000, se aprobó

[1] Al respecto, debemos tener en cuenta que "quien desarrolla actividades en el ciberespacio, tiene acceso a información privada, confidencial y secretos de Estado por lo que está obligado a comportarse conforme a esta delicada y sensible situación". Stel, Enrique, *Seguridad y defensa del ciberespacio*, Buenos Aires, Dunken, 2014, p. 25. Lo anterior abona a la idea relativa a la importancia de generar un contexto de seguridad tanto técnico como jurídico.

[2] Sobre el particular, "El Derecho Informático nos plantea una serie de instituciones que [facilitan] el desarrollo de mecanismos de prevención de todas aquellas situaciones no deseadas para los usuarios de las Nuevas Tecnologías de la Información, de tal forma que cuando se presentan determinadas circunstancias de afectación existen nuevas instituciones jurídicas que generan confianza a las personas [como a las entidades públicas y privadas] que realizan operaciones por medios electrónicos, permitiendo la solución de problemas generados por el uso de los medios electrónicos en la sociedad". Espinoza Céspedes, José Francisco, *El derecho informático frente a la contratación electrónica*, México, unam. [Consulta: 25 de mayo, 2017]. Disponible en https://archivos.juridicas.unam.mx/www/bjv/libros/6/2940/19.pdf

[3] Publicada en el Diario Oficial El Peruano, el domingo 28 de mayo del 2000. La referida norma consta de dieciséis artículos y tres disposiciones complementarias, transitorias y finales. Posteriormente, 11 julio 2014, mediante la Segunda Disposición Complementaria Modificatoria de la Ley N° 30224, se incorporó el artículo 15-A, sobre el Régimen de Infracciones y Sanciones.

la Ley 27291, que trajo consigo una serie de modificaciones al Código Civil peruano de 1984. Esto permitió, entre otros aspectos, aquellos relativos a la utilización de los medios electrónicos para manifestar la voluntad y la correspondiente utilización de la firma electrónica.

2. Aproximaciones normativas en relación con la firma electrónica en el Perú

Por la evolución constante de las operaciones electrónicas en contextos nacionales y transfronterizos, se hizo necesario regular en el Perú los mecanismos técnicos que permiten una real identificación de las partes participantes en operaciones electrónicas y facilitan fehacientemente su manifestación de voluntad en el ciberespacio.

Una de las tecnologías más gravitantes para los efectos de interconexión de redes y operaciones electrónicas[4] es la firma electrónica, regulada en el Perú por el artículo 1 de la Ley 27269, la cual planteó la contextualización teórica de la referida tecnología. En ese sentido, la acotada norma expresamente señala que el objeto de la Ley 27269 es regular los mecanismos de utilización de la firma electrónica. Por otra parte, otorgó a dicha tecnología "la misma validez y eficacia jurídica que el uso de una firma manuscrita [o cualquier] otra análoga que conlleve manifestación de voluntad".[5]

La importancia de la Ley 27269 no sólo radica en que genera un entorno de seguridad y validez para las operaciones electrónicas, desde el Perú al mundo y viceversa, sino que permitió dar un paso más allá, al plantear una definición de firma electrónica,[6] con una redacción neutral. Señala expresamente que la citada tecnología se relaciona con el uso de "cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita".[7]

[4] Sobre el particular debe considerarse "la existencia de bases de datos sobre las operaciones electrónicas mediante el historial de navegación". Esteban Talaya, Agueda, *Principios de Marketing*, Madrid, esic Editorial, 2008. En dicho contexto, la firma electrónica busca dar un nivel de identificación electrónica, para generar de una u otra forma un entorno de seguridad, el mismo que estará en función de la tecnología utilizada.

[5] Conforme lo previsto en el artículo 1 de la Ley 27269, Ley de Firmas y Certificados Digitales.

[6] Al respecto, "La firma electrónica irrumpe de manera preponderante en la seguridad informática y en el derecho del comercio electrónico y se irradian sus efectos —en particular en cuanto a la equivalencia de funciones jurídicas— en el ordenamiento jurídico". Peña Valenzuela, Daniel, *De la firma manuscrita a las firmas electrónica y digital*, Bogotá, Universidad Externado de Colombia, 2015, p.16.

[7] De acuerdo con lo regulado por el artículo 1 de la Ley N° 27269.

En el contexto de la Ley 27269, son varios los aspectos relevantes en torno al uso de la firma electrónica en Perú. Entre éstos, destaca la generación de un elemento de vinculación con el propio mensaje de datos enviado por el firmante, a través del cual acredita su identidad en el mundo digital.[8] Así, se genera un entorno de plena identificación con el documento enviado y la exigencia de un mecanismo de autenticación con el mensaje de datos.[9]

Asimismo, la tecnología de firma electrónica que exige la ley peruana debe tener una potencia tal, que permita generar un conjunto de acciones en el mundo electrónico a modo de replicar las funciones características de la firma manuscrita, tales como:

- Crear una real vinculación entre el firmante y el documento firmado.
- Proponer mecanismos adecuados para una efectiva identificación del firmante, de tal forma que no exista duda sobre la identidad real de los intervinientes, en lo que se denomina la función de identificación o identificativa[10] de la firma. Además, esto permite la estrecha vinculación entre el firmante y lo firmado.
- Generar un espacio adecuado de seguridad a fin lograr una permanente preservación de todos aquellos aspectos relativos a la integridad del documento firmado, para que, una vez realizada dicha operación, surtan sus efectos. La consecuencia de estas funciones genera el no repudio del documento firmado.
- Otorgar obligatoriedad al acto de firmado, de tal forma que la declaración del firmante acredite su voluntad respecto del contenido obrante en el documento signado. En ese sentido, la firma actúa como seña o signo en relación con su actitud positiva y permite generar una expresión de voluntad válida para contratar u obligarse en general.
- Actuar como elemento verificador de la autoría del documento firmado, de tal modo que haya participado como firmante quien fue plenamente

[8] Debemos tener en cuenta que un "agente especialmente relevante son en sí los datos, es decir, el mundo digital, y el digitalizado. En los últimos años se ha capturado mucha información sobre el mundo real, por ejemplo datos sobre la localización, descripciones, imágenes, etc., tanto de lugares como de cosas y personas y toda esa información se ha ido almacenando en "el cloud" o en la "nube" [...] lo que ha ido configurando un mundo digital paralelo. Fundación Telefónica, *Realidad aumentada: una nueva lente para ver el mundo*, Barcelona, Ariel - Planeta, 2011, p. 23.

[9] Se entiende por el principio de autenticación a la operación técnica de vinculación del firmante con el contenido del documento, de tal forma que con posterioridad no se niegue ni se repudie la operación en un entorno electrónico, sea a nivel del mensaje de datos enviado, o en el contexto del documento firmado.

[10] Al respecto, "La regulación de la firma electrónica ha potenciado la función identificativa de la firma, que en el mundo presencial se ha llegado a suplir por otros mecanismos". Alonso Pérez, Mariano, *Estudios de derecho de obligaciones: homenaje al profesor Mariano Alonso Pérez*, *vol. 1*, Madrid, La Ley, 2006, p. 119.

identificado en relación con el documento y su contenido. Así, se generan tanto un acto pleno de identificación del firmante y su posterior participación en el acto de signado, como un medio de prueba idóneo, frente a posteriores eventualidades legales.

- Lograr un elemento diferenciador, como el grafismo generado por el ser humano firmante como elemento de individualidad, tal como ocurre en el caso de la firma manuscrita.
- Evidenciar un determinado resultado semejante al identificador personal que se genera en un contexto de firma manuscrita, como signatura particular y personal. De este modo, se determina un alto grado de intencionalidad, todo ello como resultado del *animus signandi*, que vincula al firmante con el contenido firmado.
- Implementar determinado mecanismo de autenticación que genere certeza y fiabilidad respecto al contenido de lo firmado, para deducir la existencia de un consentimiento válido.
- Conocer fehacientemente al autor del documento firmado, sea por los trazos, marcas, signos o símbolos dejados sobre la superficie firmada.
- Determinar su validez al momento de la firma, aunque ocurriera su modificación posterior, por el paso del tiempo o por su uso constante.

Sobre el particular, podemos apreciar que toda firma electrónica debe cumplir una serie de requisitos vinculados con la firma manuscrita. La tecnología utilizada puede ser de cualquier tipo, lo importante es dar cumplimiento a los mínimos tecnológicos que exige la norma.

Por otro lado, debemos tener presente lo previsto por el artículo 2 de la Ley 27269, respecto a su ámbito de aplicación, cuando señala: "se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a los mismos, puedan *vincular e identificar* al firmante, así como *garantizar la autenticación e integridad* de los documentos electrónicos" (las cursivas son nuestras).

En ese orden de ideas, la norma acota puntualmente el concepto de firma electrónica para efectos de la ley de firmas digitales, al elemento de vinculación e identificación, a un contexto técnico. Además, indica que se debe garantizar la autenticación e integridad de todos los documentos electrónicos trabajados con dicha tecnología.

Se aprecia la existencia de un contexto genérico para el uso de cualquier tipo de firma electrónica, debiendo asegurarse en dicho proceso la aplicación

del principio de autenticación. Éste es el proceso técnico de verificación de la autoría del firmante y el principio de integridad, para que el documento no pueda ser modificado durante su envío. Pero, en caso de que ocurra cualquier tipo de afectación, se deberá contar con un mecanismo de alerta temprana que permita eliminar cualquier efecto perjudicial en el documento firmado. De este modo, se procederá a su nulidad y al firmado de un nuevo documento, a fin de no afectar las operaciones electrónicas, ni las manifestaciones de voluntad generadas por medios electrónicos.

Posteriormente, en el artículo 3 de la ley de firmas y certificados digitales, Ley27269, se define la firma digital, como un tipo de firma electrónica "que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada". La norma prosigue con el desarrollo de todos los demás aspectos aplicables a la firma digital.

3. La firma electrónica y la manifestación de voluntad por medios electrónicos

Otro ámbito no menos importante de la legislación peruana es el desarrollo, en el marco de la Ley N27291,[11] de otros aspectos vinculados con la firma electrónica. La acotada norma modificó el Código Civil de 1984, para permitir la utilización de diversos medios electrónicos, con la finalidad de comunicar toda manifestación de voluntad utilizando diversas tecnologías que faciliten el firmado electrónico.

En dicho contexto, en el artículo 1 de la Ley 27291, se modifica, entre otros, el artículo 141 del Código Civil. Respecto a la manifestación de voluntad se plantea que ésta "puede ser expresa o tácita. Es expresa cuando se realiza en forma oral o escrita, a través de cualquier medio directo, manual, mecánico, *electrónico u otro análogo*" (las cursivas son nuestras).

Por otro lado, mediante el artículo 2 de la Ley 27291, se adicionaron al Código Civil elementos directamente vinculados con la formalidad que debe tenerse en cuenta al manifestar la voluntad. En ese sentido, el artículo 141 a, con la adición antes referida, expresamente señala que: "En los casos en que la Ley establezca que la *manifestación de voluntad* deba hacerse a través de alguna formalidad expresa o *requiera de firma*, ésta podrá ser *generada* o

[11] Publicada en el Diario Oficial El Peruano el Sábado, 24 de junio de 2000. La norma consta de tres artículos.

comunicada a *través de medios electrónicos*, ópticos o cualquier otro análogo" (las cursivas son nuestras).

Podemos apreciar que, para efectos de la manifestación de voluntad por medios electrónicos, se puede utilizar la firma electrónica, es decir aquella generada en entornos electrónicos. Pero se debe tener presente que la norma va más allá, pues se permite la utilización de tecnología óptica generada a partir del rayo láser. Además, se deja en libertad a las partes para que decidan el uso de cualquier otro medio análogo derivado de la tecnología electrónica. Con ello, podemos apreciar la existencia de una redacción normativa neutral, pues se deja al albedrío del interesado la decisión de optar por la tecnología que requiera, de acuerdo a sus necesidades en el mundo electrónico.

En dicho contexto surge una nueva especialidad iusinformática para los abogados y demás operadores jurídicos, pues están en condiciones de brindar asesoría especializada, con apoyo del derecho informático, a las partes intervinientes en ámbitos electrónicos. Esto para evitarles cualquier tipo de afectación por desconocimiento o por la falta de seguridad derivada de las operaciones electrónicas.

Desde un punto de vista sistémico, tanto en la Ley 27269 como en la Ley 27291, se puede deducir que la firma electrónica, bajo la ley peruana, representa un conjunto universal, tecnológicamente hablando. En dicho conjunto, destacan las tecnologías electrónicas que permiten generar firmas digitalizadas, firmas con lapiceros electrónicos, lectoras de rasgos biométricos, entre otras.

Por otro lado, en el conjunto universal antes referido se encuentran las tecnologías digitales. Entre éstas, destacan los sistemas simétricos,[12] los cuales resultan poco seguros al tener que compartirse la clave privada. No obstante, también encontramos los sistemas asimétricos,[13] con el uso de un par de claves en un contexto de infraestructura de clave pública[14] (PKI).

---

[12] Es importante señalar que "los sistemas simétricos permiten el cifrado eficiente de mensajes extensos, requieren un acuerdo previo en las claves y poseen capacidad de autenticación limitada". España Boquera, María Carmen, *Servicios avanzados de telecomunicación*, Madrid, Díaz de Santos, 2003, p. 61.

[13] En dicho contexto, debemos resaltar que "Los sistemas asimétricos tienen como ventaja que la clave pública y el algoritmo de cifrado pueden ser conocidos y no se necesita mandar la clave privada. Frente a esto, los sistemas asimétricos son más lentos y más difíciles de implementar que los sistemas simétricos". Quero Catalinas, Enrique, *Mantenimiento de portales de la información: explotación de sistemas informáticos*, Madrid, Thomson Editores - Paraninfo, 2007, p. 102.

[14] "El uso de una infraestructura de clave pública jerárquica implica que existen determinadas entidades, denominadas autoridades de certificación, que garantizan la autenticidad del certificado". Sivianes Castillo, Francisco, *Servicios en red*, Madrid, Paraninfo, 2010, p. 138. Sobre el particular debemos tener en cuenta que en la legislación peruana se denominan entidades de certificación. En todo caso, se cuenta con una autoridad administrativa competente para el ámbito privado, representada por Indecopi y la autoridad para el ámbito público es Reniec.

En tal sentido, podemos apreciar que la normatividad peruana genera un proceso regulatorio, de la firma electrónica a la firma digital. En un marco de diversas tecnologías que pueden ser utilizadas por los interesados en sus operaciones electrónicas, se genera una situación de desarrollo para la asesoría jurídica en contextos iusinformáticos. Así, a partir de una base jurídica en el derecho informático, se puede determinar el cumplimiento de las exigencias legales.

4. La firma electrónica en la normatividad peruana

A continuación presentamos el resultado una profunda investigación la cual nos ha permitido sistematizar las diversas normas que recoge la institución de la firma electrónica en el sistema jurídico peruano.

Resalta, en el ámbito bancario, la Resolución SBS 373-2000, mediante la cual se modificó el Reglamento de Tarjetas de Crédito, conforme al artículo primero de la citada norma. Se sustituyó el numeral 3) del artículo 8 del Reglamento de Tarjetas de Crédito, aprobado por Resolución SBS 271-2000.

En dicho contexto la referida modificación es la siguiente: "3. Nombre del usuario de la tarjeta de crédito y su firma. En caso el usuario sea una persona diferente del titular de la tarjeta podrá constar también el nombre de éste. Las firmas podrán ser sustituidas o complementadas por una clave secreta, firma electrónica u otros mecanismos que permitan identificar al usuario".

Por otra parte, es notable la Resolución SBS 1121-2017, a través de la cual se aprobó el Reglamento de Comercialización de Productos de Seguros, disponiendo en literal b) del artículo 3, respecto al consentimiento del contratante para el envío de pólizas de seguro electrónicas, como se detalla a continuación:

> Artículo 3.- Consentimiento del contratante para el envío de pólizas de seguro electrónicas
> Las empresas podrán enviar pólizas de seguro electrónicas a los contratantes, previo consentimiento expreso de estos últimos. Dicho consentimiento podrá manifestarse de forma escrita, telefónica, electrónica, o a través de cualquier otro medio que permita dejar constancia de ello.

El consentimiento del contratante deberá incluir lo siguiente:

> d) La forma en que se acreditará la autenticidad e integridad de la póliza de seguro electrónica, mediante la firma electrónica u otro medio que asegure igual o mayor seguridad.

En el contexto del Registro Público de Minería, la Resolución Jefatural 04200-2000-RPM se dispuso precisar las coordenadas UTM definitivas, nombre, padrón, extensión y área libre exclusiva, en resoluciones jefaturales de título de derechos mineros formulados bajo el sistema de cuadrículas.

En el ámbito de la norma antes indicada se reguló lo siguiente: "artículo 5. Autorizar de conformidad a lo establecido en la Ley 27269, Ley de Firmas y Certificados Digitales, el empleo de la firma electrónica, la misma que tendrá la validez y eficacia jurídica de la firma manuscrita".

A nivel de los registros públicos, la Resolución del Superintendente Nacional de los Registros Públicos 096-2001-SUNARP-SN, autoriza la utilización de nueva técnica de inscripción en las oficinas registrales del país, a través del software denominado Sistema de Información Registral. Para tal efecto, es importante analizar el tercer considerando de la citada resolución, el cual señala:

> Esta Superintendencia ha decidido adoptar como *software* registral estándar el Sistema de Información Registral (SIR), que fuera desarrollado bajo la supervisión del PNUD y que actualmente se encuentra operando en la Oficina Registral de Lima y Callao, a través del cual se utiliza una nueva técnica de inscripción, consistente en la generación de asientos electrónicos, grabados en medios que aseguran la inalterabilidad e integridad de la información, apoyada por un *dispositivo de captura de huella digital* en calidad de *firma electrónica*, con el objeto de identificar indubitablemente al registrador público responsable de la generación del asiento (las cursivas son nuestras).

Sobresale también la Resolución del Superintendente Nacional de los Registros Públicos 094-2013-SUNARP-SN, mediante la cual se aprobó la Directiva que establece los Lineamientos para la Proyección de una Imagen Institucional y Corporativa Homogénea de los Registros Públicos en el Ámbito Nacional a través de la Aplicación adecuada del Logotipo Institucional. La referida norma, en su artículo 6.12, dispone lo siguiente:

> 6.12 De la firma electrónica y las presentaciones de Power Point (a nivel interno como externo)
> con la finalidad de guardar coherencia con la identidad visual y la imagen que se desea transmitir a través de todas las herramientas de comunicación, la GIIRRPP será la encargada de diseñar la firma electrónica y la plantilla para las presentaciones de Power Point (PPT), las cuales serán

> de uso obligatorio por todos los funcionarios que tengan una cuenta de correo electrónico autorizada y tengan que realizar presentaciones de PPT a nivel interno como externo.

Resalta el Decreto Supremo 070-2011-PCM, mediante el cual se modificó el Reglamento de la Ley 27269, Ley de Firmas y Certificados Digitales, con la finalidad de establecer normas aplicables al procedimiento registral en virtud del Decreto Legislativo 681 y ampliatorias, en dicho sentido, se planteó que:

> dada la importancia de la información registral, contenida en asientos electrónicos suscritos con firma electrónica, resulta necesario disponer que la Superintendencia Nacional de los Registros Públicos adopte las acciones pertinentes a efectos que, a partir de una determinada fecha, los mismos empiecen a ser micrograbados y microarchivados, conforme a lo establecido en el Decreto Legislativo 681, Decreto Legislativo 827 y demás normas modificatorias ampliatorias y reglamentarias, así como de acuerdo a las regulaciones específicas que dicte para el efecto el Ministerio de Justicia, de acuerdo a lo previsto en el artículo 4 del Decreto Legislativo 827.

En ese orden de ideas, se aprobó el artículo 4, sobre los asientos de inscripción y los correspondientes mecanismos para su almacenamiento en bóveda certificada y acredita por las supervisoras acreditadas ante el Instituto Nacional de Calidad (Inacal).

La bóveda antes referida es un concepto técnico que jurídicamente, en el marco de la micrograbación con valor legal dispuesta por el Decreto Legislativo 681, es conocida como microarchivo. Es el lugar de almacenamiento de las microformas, como documentos con pleno valor legal en un marco de fe pública, debido a la presencia de un fedatario juramentado, denominado en el ámbito societario y mercantil como fedatario informático. El referido artículo fue regulado de la siguiente manera:

> Artículo 4.- Asientos de inscripción y su almacenamiento en microarchivos
>
> La Superintendencia Nacional de los Registros Públicos (Sunarp) deberá adoptar, de manera progresiva, las acciones que permitan obtener microformas a partir de los asientos de inscripción suscritos con firma electrónica, conforme a lo establecido en el Decreto Legislativo 681, así como a las regulaciones específicas que dicte para el efecto el Ministerio de Justicia, de acuerdo a lo previsto en el artículo 4 del

> Decreto Legislativo 827; para lo cual, deberá expedirse una resolución del titular de dicha entidad, en la que se precise la fecha a partir de la cual los asientos de inscripción empezarán a ser micrograbados para su ulterior almacenamiento en microarchivos.
>
> Lo antes señalado será también de aplicación a la micrograbación y ulterior almacenamiento en microarchivos de los documentos que sustenten la inscripción.

En el contexto de la Dirección Nacional de Turismo del Mitinci, ahora Mincetur (Ministerio de Comercio Exterior y Turismo), se encuentra la Resolución Directoral 425-2001-MITINCI-VMT-DNT, mediante la cual se aprobó la Directiva Supervisión de Obligaciones de Entidades Autorizadas.

La referida norma hace alusión a la firma electrónica en el artículo 4, en el contexto de los instrumentos de control, señalando en su tercer párrafo lo siguiente: "Los instrumentos de control deben proporcionar una huella o firma electrónica individualizada e irrepetible, que garantice la identificación particular de cada memoria de sólo lectura de los programas de juego de las máquinas tragamonedas".

Asimismo, la norma antes referida plantea en la literal b) de la primera disposición complementaria y final, respecto a la aprobación de los métodos de control lo siguiente:

> b.- Dataman S4 del fabricante Dataman Programmers Ltd. Este instrumento utilizará el Library ROM Dataman S4 para proporcionar la huella o firma electrónica.
>
> La DEJCMT en un plazo máximo de 90 días calendario deberá registrar en una base de datos, el signature o firma electrónica proporcionada por el Memory Tester 2000 y el Dataman S4 para todas las memorias de sólo lectura que por su naturaleza puedan ser verificadas por dichos instrumentos y que cuenten con número de registro otorgado por la DNT.

El Decreto Supremo 010-2010-MINCETUR es la norma mediante la cual se establecieron las disposiciones reglamentarias referidas a la Ventanilla Única de Comercio Exterior, en su glosario de términos se define a la clave SOL como la firma electrónica de la Superintendencia de Administración Tributaria (Sunat), en los términos siguientes: "Clave SOL: Firma electrónica regulada por la Resolución de Superintendencia 109-2000/SUNAT, la misma que será utilizada para la autenticación de los administrados que realizan trámites ante la VUCE".

Por su parte, el Decreto Supremo 003-2017-MINCETUR dispuso la ejecución de la Decisión número 1 de la Comisión de Libre Comercio del Protocolo Adicional relativo al Acuerdo Marco de la Alianza del Pacífico en el marco del Reconocimiento de los Documentos Firmados Electrónicamente en el contexto de la Interoperabilidad de las Ventanillas Únicas de Comercio Exterior en la Alianza del Pacífico, en los términos siguientes:

1. Las partes reconocen la validez de los documentos firmados electrónicamente susceptibles de ser intercambiados entre las VUCE de cada parte a través de una plataforma de interoperabilidad.
2. Las partes reconocen como válida la firma electrónica de los documentos que se transmitan entre las VUCE a través de la plataforma de interoperabilidad.
3. Cada parte garantiza que las firmas electrónicas utilizadas en los documentos electrónicos transmitidos a través de la plataforma de interoperabilidad de las VUCE aseguren la identificación del firmante, así como la autenticidad e integridad de los documentos.

En el ámbito de la Superintendencia el Mercado de Valores, se encuentra la Resolución SMV 010-2013-SMV-01, mediante la cual se aprobó el Reglamento del Sistema MVNet y SMV Virtual, en su tercer considerando refiere: "Que, el Sistema MVNet se caracteriza por requerir de certificado y firma digital provistos por empresas especializadas, los cuales deben ser adquiridos por las entidades obligadas al uso de dicho sistema; a diferencia del Sistema SMV Virtual, en el cual se utiliza firma electrónica, sin generar, en este caso, gasto alguno para los usuarios correspondientes".

Posteriormente, en su artículo 30, al desarrollar la definición de SMV Virtual, señala que:

> El SMV Virtual es el sistema WEB de intercambio de información que permite el almacenamiento de información, garantiza la confidencialidad, integridad y no repudio de las transacciones a través del uso de componentes de firma electrónica, autenticación y canales seguros.

Los usuarios del SMV Virtual deberán remitir, por este medio, a la SMV toda información y documentación firmada electrónicamente. La SMV utilizará este mismo medio para remitir a tales usuarios cualquier información o documentación firmada digitalmente.

Finalmente, la norma acotada indica en su artículo 31 que:

En el SMV Virtual se encuentran integradas las siguientes aplicaciones jurídico-informáticas y funcionales:

a) De control de acceso;
b) De firma electrónica de los documentos a ser enviados por los usuarios del SMV Virtual y SMV;
c) De transmisión telemática segura de la información y documentos;
d) De formularios web;
e) De generación y entrega de cargos electrónicos con sello electrónico de tiempo;
f) Del domicilio electrónico de los usuarios del Sistema SMV Virtual y de la SMV;
g) De auditabilidad y disponibilidad de la bitácora en el SMV Virtual.

A nivel portuario, mediante la Ley 27943, Ley del Sistema Portuario Nacional, se aprobó el uso de la firma electrónica en la Décimo Primera Disposición Transitoria y Final, señalándose que para tal efecto:

> Todo acto jurídico, administrativo o contractual, que se exija o se derive de esta ley, reglamento o normas complementarias, puede ser realizado por medios electrónicos. En ese sentido los mensajes electrónicos de datos, los documentos electrónicos, así como la firma electrónica gozan de total validez jurídica en el ámbito portuario. Decláranse válidas las comunicaciones electrónicas para autorizar en la libre plática, recepción y despacho de naves. A más tardar, al 31 de diciembre de 2004, el Sistema Nacional Portuario deberá interconectarse digitalmente.

La Ley General de Aduanas, aprobada por Decreto Legislativo 1053, en su artículo 134, al regular la Declaración Aduanera, plantea el uso de la firma electrónica en los términos siguientes:

> Artículo 134.- Declaración aduanera
>
> La destinación aduanera se solicita mediante declaración aduanera presentada o transmitida a través de medios electrónicos y es aceptada con la numeración de la declaración aduanera. La Administración Aduanera determinará cuando se presentará por escrito.
>
> Los documentos justificativos exigidos para la aplicación de las disposiciones que regulen el régimen aduanero para el que se declaren las

> mercancías podrán ser presentados en físico o puestos a disposición por medios electrónicos, en la forma, condiciones y plazos que establezca la Administración Aduanera.
>
> Los datos transmitidos por medios electrónicos para la formulación de las declaraciones gozan de plena validez legal. En caso se produzca discrepancia en los datos contenidos en los documentos y archivos de los operadores de comercio exterior con los de la Sunat, se presumen correctos estos últimos.
>
> La declaración efectuada utilizando una técnica de procesamiento de datos incluirá una firma electrónica u otros medios de autenticación.
>
> La clave electrónica asignada a los despachadores de aduana equivale y sustituye a su firma manuscrita o a la del representante legal, según se trate de persona natural o jurídica, para todos los efectos legales.

Sobresale, también, la Resolución de Acuerdo de Directorio 049-2014-APN-DIR, por la cual se dispuso la prepublicación del proyecto de lineamientos para el registro, aprobación y certificación de la capacitación en protección y seguridad portuaria, trabajo portuario y gestión portuaria, en el portal electrónico de la Autoridad Portuaria Nacional, en los términos siguientes:

La Undécima Disposición Transitoria y Final de la Ley del Sistema Portuario Nacional establece que todo acto jurídico, administrativo o contractual, que se exija o se derive de esta ley, reglamento o normas complementarias, puede ser realizado por medios electrónicos y, en ese sentido, los mensajes electrónicos de datos, los documentos electrónicos, así como la firma electrónica gozan de total validez jurídica en el ámbito portuario.

La Resolución de Acuerdo de Directorio 022-2015-APN-DIR aprobó la Directiva para el registro, aprobación y certificación de la capacitación en protección y seguridad portuaria, trabajo portuario y gestión portuaria, en los términos siguientes:

> Que, la Undécima Disposición Transitoria y Final de la Ley del Sistema Portuario Nacional establece que todo acto jurídico, administrativo o contractual, que se exija o se derive de esta ley, reglamento o normas complementarias, puede ser realizado por medios electrónicos y, en ese sentido, los mensajes electrónicos de datos, los documentos electrónicos, así como la firma electrónica gozan de total validez jurídica en el ámbito portuario.

Por la Resolución Directoral 0129-2016-MGP-DGCG, se estableció como modalidad válida de notificación para los actos administrativos y servicios prestados en exclusividad a cargo de la Autoridad Marítima Nacional el correo electrónico, manifestando en su primera Disposición complementaria final, lo siguiente:

> La Primera Disposición Complementaria Final del Decreto Legislativo 1147 establece que todo acto jurídico, administrativo o contractual, que se exija o se derive del referido Decreto Legislativo, reglamento o normas complementarias, puede ser realizado y notificado por medios electrónicos. En ese sentido, los mensajes electrónicos de datos, los documentos electrónicos, así como la firma electrónica gozan de total validez jurídica en el ámbito de competencia de la Autoridad Marítima Nacional.

En el contexto de economía y finanzas, la Resolución Directoral 087-2003-EF-77.15, aprobó la Directiva de Tesorería para el Año Fiscal 2004. En su artículo 37, aprobó la facultad y responsabilidad para el pago a proveedores con abono en sus cuentas:

> Artículo 37.- Facultad y responsabilidad para el pago a proveedores con abono en sus cuentas
>
> El pago a proveedores mediante el abono en sus cuentas será efectuado únicamente por dos de las personas acreditadas ante el Banco de la Nación por la DNTP como responsables titulares y/o suplentes del manejo de las cuentas bancarias de la UE, es decir, aquellos cuyas firmas se encuentran debidamente registradas ante la indicada entidad bancaria.
>
> A efectos de lo establecido en el presente artículo, el Ministerio de Economía y Finanzas asigna un código de usuario y una clave o password para cada una de las personas acreditadas y que, dadas sus características de uso como firma electrónica, es personal e intransferible, bajo responsabilidad civil y/o penal que se derive del uso indebido de dicha clave o password.

Destaca la Resolución Directoral 023-2004-EF-76.01, por la cual se aprobó Directiva para el Registro de las Altas y Bajas del personal activo y pensionista, así como de los servicios no personales: Módulo de Control del Pago de Planillas y de los Servicios No Personales. Dicha norma disponía en su Artículo 7, el uso de la firma electrónica en el sentido siguiente:

> Dentro de los cinco (5) días hábiles de publicada la presente Directiva, el director de administración o el que haga sus veces en la Unidad Ejecutora, remitirá a la Oficina General de Informática y Estadística (Ofine) del Ministerio de Economía y Finanzas, un oficio que contenga el o los nombres, documento de identidad y cargo de los servidores acreditados para efectuar el ingreso de información en el Módulo de Control del Pago de Planillas y de los Servicios No Personales (MCPP-SNP), a fin de que se asigne un código de usuario y una clave o password para cada una de las personas acreditadas y que, dadas sus características de uso como firma electrónica, es personal e intransferible, bajo responsabilidad civil y/o penal que se derive del uso indebido de dicha clave o password. Copia de dicho oficio se remitirá a la Oficina de Administración o la que haga sus veces en el Pliego.

En el ámbito de la Defensoría del Pueblo, mediante la Resolución Defensorial Nº 0050-2006-DP, se aprobó el Informe Defensorial 109 sobre propuestas básicas de la Defensoría del Pueblo para la reforma de la justicia en el Perú. En el numeral 10 del referido informe se señala lo siguiente:

> Recomendar la elaboración, ejecución, monitoreo y publicación de un plan integral de lucha contra las dilaciones indebidas, en coordinación con las Presidencias y/o Consejos Ejecutivos Distritales, que tenga en cuenta los siguientes aspectos:
>
> a) La identificación periódica de las causas de la dilación en los procesos judiciales, teniendo en cuenta lo indicado en el Capítulo Séptimo del Informe Defensorial 109.
> b) La implementación, a la brevedad, de la notificación vía correo electrónico prevista hace trece años en el artículo 164 del Código Procesal Civil, así como la evaluación de otras medidas tecnológicas como la firma electrónica y la consulta del "expediente virtual".

En el contexto del Fondo de Garantía Empresarial (Fogem), resalta el Decreto Legislativo 1282, mediante el cual se modificó la Ley 29623, Ley de promoción del financiamiento a través de la factura comercial y que amplía el plazo de acogimiento al Fondo de Garantía Empresarial. Dicha norma, en su artículo 3 a), regula lo siguiente:

Contenido de la factura negociable originada en un comprobante de pago electrónico

La factura negociable que se origine en una factura comercial electrónica o en un recibo por honorarios electrónico, además de la información requerida por la Sunat para dicho comprobante de pago, debe contener, cuando menos, la información señalada en los literales b), c), d), e) y f) del artículo 3.

En este caso y para efectos de lo señalado en el literal b) del artículo 3, la firma del proveedor puede ser:

a) Aquella que obre en la factura comercial y/o en el recibo por honorarios electrónico, a partir de los cuales se origine la factura negociable; o
b) La clave SOL, cuando en su función de firma electrónica vincula al proveedor con la factura comercial o el recibo por honorarios emitidos de manera electrónica a través de Sunat Virtual, a partir de los cuales se origine la factura negociable; o,
c) La firma electrónica u otra forma de manifestación de voluntad válida que permita que se autentique y vincule al proveedor con la factura negociable, de acuerdo a lo que señalen las disposiciones pertinentes de la SMV.

En el ámbito de la Autoridad Marítima Nacional, Dirección General de Capitanías y Guardacostas, se encuentra el Decreto Legislativo 1147, mediante el cual se reguló el fortalecimiento de las Fuerzas Armadas en las competencias de la Autoridad Marítima Nacional a nivel de la Dirección General de Capitanías y Guardacostas, en la primera Disposición Complementaria Final. Regula aspectos sobre la firma electrónica al establecer criterios sobre la simplificación administrativa, tal como se presenta a continuación:

La Autoridad Marítima Nacional promueve la eliminación de cualquier regulación, trámite, costo o requisito de tipo administrativo, económico, técnico, operativo o de cualquier naturaleza, así como de los obstáculos burocráticos o criterios de calificación que no resulten razonables para la autorización del ejercicio de las actividades dentro del ámbito de su competencia.

Todo acto jurídico, administrativo o contractual, que se exija o se derive de este Decreto Legislativo, reglamento o normas complementarias, puede ser realizado y notificado por medios electrónicos. En ese

> sentido, los mensajes electrónicos de datos, los documentos electrónicos, así como la firma electrónica gozan de total validez jurídica en el ámbito de competencia de la Autoridad Marítima Nacional.

En el contexto de Protección de Datos, el Decreto Supremo Nº 003-2013-JUS, aprobó el Reglamento de la Ley 29733, Ley de Protección de Datos Personales. Ésta regula en el numeral 3, del artículo 12, los siguientes términos:

> Expreso e inequívoco: Cuando el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento.
>
> La condición de expreso no se limita a la manifestación verbal o escrita [...] Tratándose del entorno digital, también se considera expresa la manifestación consistente en "hacer clic", "cliquear" o "pinchar", "dar un toque", "touch" o "pad" u otros similares.
>
> En este contexto el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, de forma tal que pueda ser leída e impresa, o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito. También podrá otorgarse mediante texto preestablecido, fácilmente visible, legible y en lenguaje sencillo, que el titular pueda hacer suyo, o no, mediante una respuesta escrita, gráfica o mediante clic o pinchado.

A nivel de salud virtual, el Decreto Supremo 034-2015-SA aprobó el Reglamento de Supervisión de Superintendencia Nacional de Salud aplicable a las instituciones administradoras de fondos de aseguramiento en salud, instituciones prestadoras de servicios de salud y unidades de gestión de instituciones prestadoras de servicios de salud.

Resalta en su artículo 41 la Creación de Susalud Virtual: "Susalud desarrolla una extranet denominada Susalud Virtual, basada en una aplicación Web de intercambio de información que permita su almacenamiento, considerando la confidencialidad, integridad y no rechazo de las transacciones a través del uso de componentes de firma electrónica, autenticación y canales seguros".

En el entorno de la simplificación administrativa, el Decreto Legislativo 1310 fue el medio por el cual se aprobaron diversas medidas adicionales de simplificación administrativa, en los siguientes términos:

> Artículo 3.- Simplificación para la emisión, remisión y conservación de documentos en materia laboral.
>
> En la emisión, remisión y conservación de documentos en materia laboral, se autoriza el uso de tecnologías de la digitalización, información y comunicación para la sustitución de documentos físicos y firmas ológrafas, de acuerdo a las siguientes disposiciones:
>
> 3.1 En todo tipo de documentos laborales, el empleador puede sustituir su firma ológrafa y el sellado manual por su firma digital, conforme a lo regulado por el artículo 141-A del Código Civil; o, su firma electrónica, emitida conforme a lo regulado por la Ley 27269, Ley de Firmas y Certificados Digitales; así como hacer uso de microformas, conforme a lo regulado por el Decreto Legislativo 681.

En el ámbito del Ministerio de la Mujer e Inclusión Social, el Decreto Supremo 005-2017-MIDIS, fue el medio por el cual se establecieron las acciones que debe realizar el Reniec en cumplimiento de la Vigésima Novena Disposición Complementaria Final de la Ley 30518, Ley de Presupuesto del Sector Público para el Año Fiscal 2017. En ese sentido, el numeral 5 del Anexo, sobre las acciones a cargo del Registro Nacional de Identificación y Estado Civil (Reniec). Se reguló dicho contexto de la siguiente forma:

> Acciones necesarias para la implementación de la Fase de Recojo de Información de Empadronamiento en cuarenta y cinco (45) ULE, las cuales comprenden lo siguiente:
>
> (i) Reniec, como parte del Sistema Nacional de Focalización (Sinafo), acompañará al personal del MIDIS destinado en cada ULE y entregará cuarenta y cinco (45) dispositivos biométricos, los mismos que serán cedidos en uso al MIDIS.
>
> (ii) El usuario de la ULE (responsable y/o funcionario) deberá digitar la información en la ficha S-100, validando con la huella dactilar biométrica y/o firma electrónica usando el DNI electrónico.

A nivel del Ministerio de la Producción, se encuentra el Decreto Supremo 006-2017-PRODUCE. Por éste se aprobó el Reglamento del Decreto Legislativo 1332, mediante el cual se facilita la constitución de empresas a través de los Centros de Desarrollo Empresarial (CDE), en los términos siguientes:

Artículo 5.- Funciones del CDE para la constitución de empresas

5.1. Mediante el CDE es posible obtener la reserva de preferencia registral y la inscripción de la constitución de empresa, bajo cualquier forma de organización o gestión empresarial. Para tal efecto, el CDE tiene una infraestructura física y tecnológica mínima para cumplir, entre otras, las siguientes funciones:

1. Asesorar y brindar asistencia técnica en la constitución de empresas a fin de promover la formalización empresarial.
2. Atender de manera presencial a los ciudadanos con interés en la creación de una persona jurídica para la actividad empresarial.
3. Identificar a los intervinientes (socios o titular) mediante el sistema para la identificación biométrica.
4. Obtener la grabación o filmación de los intervinientes en la generación del formato de estatuto de la constitución de empresa.
5. Usar la firma electrónica para los intervinientes en el formato de estatuto de la constitución de empresa de acuerdo a lo establecido en la Ley 27269 y su reglamento.

5. De la firma electrónica a la firma digital en el marco de la Ley 27269

A través de la presente investigación, se ha podido determinar que la firma electrónica, en la regulación peruana, tiene sus primeros elementos de configuración en lo previsto por la Ley 27269, Ley de Firmas y Certificados Digitales. Asimismo, tiene base en la Ley 27291, ley que modificó el Código Civil con la finalidad de permitir la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica. Ello exige mayor especialización por parte de los operadores jurídicos para dar adecuados servicios legales en medios electrónicos.

Sobre el particular, debemos tener en cuenta que, en el ámbito de la Ley 27291, se amplió el concepto de firma manuscrita aplicable al mundo físico hacia el ámbito electrónico; óptico, mediante el uso del rayo láser, u otro análogo. Con ello, se aprecia que en la normatividad peruana se tiene una configuración de firma electrónica bastante amplia.

En dicho contexto, debemos resaltar que la Ley 27269, Ley de Firmas y Certificados Digitales, en su artículo 3, nos plantea el concepto de firma digital como “aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que

las personas que conocen la clave pública no puedan derivar de ella la clave privada".

De la definición de firma digital regulada en el Perú, podemos apreciar que ésta es configurada como un tipo de firma electrónica. A nuestro entender, la firma digital en el marco de la infraestructura de clave pública es la más segura, debido a que utiliza criptografía asimétrica. Por ello, debemos estar muy atentos al tipo de tecnología que puedan adquirir nuestros clientes, porque en el mundo de las firmas digitales existe la tecnología simétrica. Ésta, por su estructura técnica, utiliza una sola clave (la clave privada) que debe ser compartida por los firmantes, razón por la cual es inadmisible en el sistema jurídico peruano.

La exigencia de la regulación peruana de dar un par de claves, en el ámbito de la criptografía asimétrica,[15] nos lleva a la aplicación de la infraestructura de clave pública, conocida por sus siglas en inglés como PKI. En ésta se requiere la participación de una tercera parte confiable, denominada entidad de certificación, la cual se encarga de emitir los certificados digitales, así como las entidades de registro para la acreditación plena de la identidad personal de quienes ingresan al mundo de la PKI.

A la hora de analizar la tecnología exigida por la regulación peruana, lo importante son las funciones matemáticas que permitan relacionar las claves[16](pública y privada), sin que nadie pueda conocer el elemento inmaterial que permite el firmado. El mismo viene representado por la clave privada que, de ser necesario, permite cifrar los mensajes, los cuales serán descifrados con su correspondiente clave pública.

Por otro, lado respecto a la titularidad de la firma digital, el artículo 4 de la acotada ley señala que es de "la persona a la que se le atribuye de manera exclusiva un certificado digital que contiene una firma digital, identificándolo objetivamente en relación con el mensaje de datos". Esto nos lleva a la exigencia de una identificación plena del titular, para su posterior interacción en el ciberespacio, mundo digital o ámbito electrónico, que se encuentra en la capacidad de generar un mercado electrónico dinámico.

[15] Sobre el particular, debemos tener en cuenta que "la criptografía asimétrica funciona bien para la autenticación, ya que cada usuario protege su clave secreta, pero es lenta para el cifrado [...] la criptografía simétrica es rápida en el cifrado y mala en la gestión de claves". Mifsuf Talón, Elvira, *Curso Mentor Apache*, Madrid, Ministerio de Educación Cultura y Deporte, 2012, p. 3.

[16] Para tal efecto, se utilizan mecanismos que permitan generar adecuada trazabilidad entendida como "la capacidad de rastrear la estructura de relaciones entre los requisitos, a modo de poder comprender los impactos que el cambio en un requisito específico puede provocar en el desarrollo de un sistema. Para gestionar la trazabilidad, en general, se utiliza la matriz de Trazabilidad". Arias, Ángel, *Aprende sobre la Ingeniería de Software*, e-book, IT Campus Academy, 2015, p. 108.

De ahí la importancia de la exigencia legal prevista en el artículo 5 de la Ley 27269, en el sentido de exigir al titular de la firma digital "la obligación de brindar a las entidades de certificación y a los terceros con quienes se relacione [...] declaraciones o manifestaciones materiales exactas y completas".

De tal forma, el certificado digital[17] que se emita posteriormente podrá generar certeza sobre la identidad del titular del par de claves, a fin de lograr una total interacción en el mundo electrónico con plena identificación de las partes intervinientes. Todo ello facilita el desarrollo de las operaciones electrónicas, tanto en el ámbito público como privado.

En ese sentido, se genera confianza en la web y en el mercado electrónico en general. Dicha confianza está centrada en el actuar de las entidades de certificación y las entidades de registro, quienes tienen la obligación de recabar los datos personales de los titulares que deseen interactuar en el mundo electrónico. Además, les deben mantener a buen recaudo, implementando para tal efecto medidas de seguridad adecuadas, de acuerdo a estándares técnicos idóneos.

Por otro lado, la norma peruana admite tanto la figura de la cancelación, como la revocación del certificado digital, conforme lo previsto por los artículos 9 y 10 de la Ley 27269. Para el caso de la primera, el titular puede mediar solicitud, existir revocación por parte de la entidad de certificación, o por el paso del tiempo. Pero, con ello, surge el problema de la expiración del certificado digital —para evitar problemas de probanza sobre la validez del documentos firmado luego del vencimiento del plazo del certificado digital se viene utilizando la firma digital longeva—, y finalmente, por la existencia del cese de operaciones que afecte directamente a la entidad de certificación.[18]

Para efectos del segundo caso, es decir, la revocación del certificado digital, es competencia de la entidad de certificación generar las acciones correspondientes para dar cumplimiento al mandato de revocación cuando se logre determinar algún tipo de afección a la información incorporada al certificado digital, sea por inexactitud o modificación de la misma.[19]

[17] Sobre el particular, el artículo 6 de la Ley N° 27269, Ley de Firmas y Certificados Digitales, define al certificado digital como "el documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad". Asimismo, los datos que debe contener el certificado digital son señalados por el artículo 7 de la acotada norma: "1. Datos que identifiquen indubitablemente al suscriptor, 2. Datos que identifiquen a la Entidad de Certificación, 3. La clave pública, 4. La metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos, 5. Número de serie del certificado, 6. Vigencia del certificado, 7. Firma digital de la Entidad de Certificación".

[18] Cfr. Artículo 9 de la Ley de Firmas y Certificados Digitales, Ley N° 27269.

[19] Cfr. Artículo 10 de la Ley de Firmas y Certificados Digitales, Ley N° 27269.

El otro supuesto de revocación del certificado digital se presenta por fallecimiento del titular del par de claves y, finalmente, se presenta por la existencia del algún tipo de incumplimiento contractual que pueda afectar a la entidad de certificación.[20]

Para efectos de regulación de los certificados generados o emitidos por entidades de certificación extranjeras, conforme al artículo único de la Ley 27310 —el cual modificó en ese sentido a la Ley 27269— plantea que tales certificados "tendrán la misma validez y eficacia jurídica reconocidas en la presente ley, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente".[21]

Al respecto, podemos afirmar que la autoridad competente para dar cumplimiento a lo previsto por la ley de firmas digitales, en el ámbito privado, es el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi) y, en el público, el Registro Nacional de Identificación y Estado Civil (Reniec).

Posteriormente, por efectos de la Segunda Disposición Complementaria Modificatoria de la Ley 30224 —ley que creó el Sistema Nacional para la Calidad y el Instituto Nacional de la Calidad— se incorpora el artículo 15-A,[22] referido al Régimen de Infracciones y Sanciones, que van desde la aplicación de una multa a la suspensión temporal y la cancelación de la acreditación.

6. El soporte legal para el estudio de las firmas electrónicas y las firmas digitales

Realizar una investigación sobre las firmas electrónicas y las firmas digitales en el Perú implica un estudio de elementos técnicos, jurídicos y organizacionales. Para ello, se requiere presupuesto, que muchas veces es escaso y difícil de conseguir. En dicho contexto, es necesario determinar el soporte legal que estos nuevos elementos inmateriales deben tener para permitir la identificación de los seres humanos en la web y en el mundo electrónico en general.

Desde esa perspectiva, el derecho informático se perfila como la rama del derecho que permite realizar un estudio calificado del aspecto tecnológico en íntima relación con el mundo jurídico. Esto para solucionar los constantes problemas legales que se generan en ambientes electrónicos y digitales.

[20] Cfr. Artículo 10 de la Ley de Firmas y Certificados Digitales, Ley N° 27269.
[21] Cfr. Artículo 11 de la Ley de Firmas y Certificados Digitales, Ley N° 27269.
[22] Cfr. Artículo 15°-A de la Ley N° 30224.

El derecho informático, como nueva rama del derecho, ha ido evolucionando, desde el estudio del hardware para efectos de las transferencias de propiedad requeridas por las partes, pasando por el análisis del software con la finalidad de licenciar a los usuarios respecto al uso de los elementos intangibles.

Posteriormente, con la evolución de las computadoras y su interconexión a redes de comunicaciones, el derecho informático pasa además a analizar la problemática de la contratación electrónica, los negocios electrónicos, los nombres de dominio, los contratos informáticos, hasta llegar a las firmas electrónicas y las firmas digitales. Tal entorno, que se puede llamar iusinformático, necesita respuestas legales a los diversos problemas netamente tecnológicos con alta incidencia en el derecho.

Sobre el particular, consideramos que el derecho informático, con sus instituciones, como el principio del equivalente funcional[23] y el principio de neutralidad tecnológica,[24] permite generar un contexto adecuado para su desarrollo. Sobre todo para el estudio, análisis y configuración de soluciones legales a los problemas jurídicos que se irán presentando durante la aplicación de las firmas electrónicas y las firmas digitales en el Perú, en pleno siglo XXI y, sobre todo, a futuro.

Por lo tanto, el derecho informático[25] tiene mucho que aportar en estos tiempos dominados por el acceso a las redes de telecomunicaciones, internet y redes sociales. Frente a toda nueva tecnología que vaya apareciendo, el derecho informático se presenta como el soporte legal para el estudio, entre otros grandes temas de interés, en íntima interacción con las firmas electrónicas y las firmas digitales.

---

[23] Sobre el particular, se precisa que existe "equivalente funcional de escrito —principio importantísimo de la regulación en materia de comercio electrónico— se ve complementado con los equivalentes funcionales de firma, original y archivo". Rincón Cárdenas, Erick, *Manual de derecho de comercio electrónico y de internet*, Bogotá, Centro Editorial Universidad de Rosario, 2006, p. 33. Abundando en el tema, Rincón Cárdenas afirma que "Si un mensaje de datos cumple con los mismos requisitos objetivos y tiene las mismas funciones que un medio tradicional o físico de transmisión de información, dicho mensaje tendrá las mismas consecuencias jurídicas que el medio tradicional al que reemplaza. Este principio se conoce en doctrina como el principio del equivalente funcional, y existen cuatro manifestaciones expresas del mismo en la ley, escrito, original, firma y archivo. Se reconoce expresamente la posibilidad de que los documentos se firmen digitalmente". Hernández Villareal, Gabriel, *Actualidad y futuro del derecho procesal: principios, reglas y pruebas*, Bogotá, Editorial Universidad del Rosario, 2010, p.228.

[24] Al respecto, "Por el principio de neutralidad tecnológica, las normas ordenadoras del comercio electrónico no podrán excluir ninguna técnica de comunicación, deberán abarcar no sólo la tecnología existente en el momento en que sean formuladas sino también las tecnologías futuras. Este principio responde a la necesidad de que los usuarios del comercio electrónico puedan contar con un régimen coherente que sea aplicable a las diversas técnicas de comunicación". Camacho Clavijo, Sandra, *Partes intervinientes, formación y prueba del contrato electrónico*, Madrid, Reus, 2005, p. 52.

[25] Debe tenerse en cuenta que "A través del Derecho Informático se buscan los mecanismos pertinentes que regulen las relaciones de los seres humanos frente al avance de la tecnología, evitando las consecuencias funestas que sucederían de no existir una política legislativa pertinente". Espinoza Céspedes, José Francisco, *Contratación electrónica, medidas de seguridad y derecho informático*, Lima, RAO, 2000, p. 71.

7. Conclusiones

En primer lugar, a mayo de 2017, en la presente investigación se ha logrado determinar la normatividad vinculada con las firmas electrónicas en la legislación peruana. Queda pendiente el arduo trabajo para investigar y estudiar la normatividad relativa a las firmas digitales en los diversos ámbitos del quehacer social en nuestro país.

En segundo lugar, la firma electrónica en la legislación peruana se configura como el conjunto universal que contiene una serie de firmas, entre las cuales destacan, por su seguridad y robustez, las firmas digitales asimétricas en el marco de la infraestructura de clave pública (PKI).

En tercer lugar, se aprecia la existencia de un marco normativo abundante para efectos de la aplicación de la firma electrónica, en los diversos ámbitos de la sociedad peruana.

En cuarto lugar, el derecho informático, es la rama del derecho llamada a estudiar, analizar y buscar soluciones a los problemas generados por las firmas digitales y las firmas electrónicas en general, siendo el soporte legal necesario para su incidencia en el mundo tecnológico.

Finalmente, en su conjunto, el uso de las firmas electrónicas y las firmas digitales generan un nuevo reto para el trabajo multidisciplinario en entornos colaborativos. En éstos, los componentes iusinformáticos son de vital importancia para una solución concreta a los problemas que se vayan presentando en real incidencia social.

Bibliografía

Alonso Pérez, Mariano, *Estudios de derecho de obligaciones: homenaje al profesor Mariano Alonso Pérez, vol. 1*, Madrid, La Ley, 2006.

Arias, Ángel, *Aprende sobre la Ingeniería de Software*, e-book, IT Campus Academy, 2015.

Camacho Clavijo, Sandra, *Partes intervinientes, formación y prueba del contrato electrónico*, Madrid, Reus, 2005.

España Boquera, María Carmen, *Servicios avanzados de telecomunicación*, Madrid, Díaz de Santos, 2003.

Espinoza Céspedes, José Francisco, *Contratación electrónica, medidas de seguridad y derecho informático*, Lima, rao, 2000.

Espinoza Céspedes, José Francisco, *El derecho informático frente a la contratación electrónica*, México, unam. [Consulta: 25 de mayo, 2017]. Disponible en https://archivos.juridicas.unam.mx/www/bjv/libros/6/2940/19.pdf

Esteban Talaya, Agueda, *Principios de Marketing*, Madrid, esic Editorial, 2008.

"Firmador Digital de Documentos", *Tconversa*. [Consulta: 30 de mayo, 2017]. Disponible en: tconversa.com/wp-content/uploads/2014/09/Catalogo-Productos-005.pdf

Fundación Telefónica, *Realidad aumentada: una nueva lente para ver el mundo*, Barcelona, Ariel - Planeta, 2011.

Hernández Villareal, Gabriel, *Actualidad y futuro del derecho procesal: principios, reglas y pruebas*, Bogotá, Editorial Universidad del Rosario, 2010.

Mifsuf Talón, Elvira, *Curso Mentor Apache*, Madrid, Ministerio de Educación Cultura y Deporte, 2012.

Peña Valenzuela, Daniel, *De la firma manuscrita a las firmas electrónica y digital*, Bogotá, Universidad Externado de Colombia, 2015.

Quero Catalinas, Enrique, *Mantenimiento de portales de la Información: explotación de sistemas informáticos*, Madrid, Thomson Editores - Paraninfo, 2007.

Rincón Cárdenas, Erick, *Manual de derecho de comercio electrónico y de internet*, Bogotá, Centro Editorial Universidad de Rosario, 2006.

Sivianes Castillo, Francisco, *Servicios en red*, Madrid, Paraninfo, 2010.

Stel, Enrique, *Seguridad y defensa del ciberespacio*, Buenos Aires, Dunken, 2014.