LA IDENTIDAD DIGITAL Y LA IDENTIFICACIÓN EN EL DERECHO INFORMÁTICO EMPRESARIAL Y EN EL GOBIERNO ELECTRÓNICO.

Julio Núñez Ponce.[1]

Sumario: 1. Introducción. 2. Aspectos jurídicos relacionados con la gestión de la identidad y los servicios de confianza en el derecho comparado. 3. La identidad digital y la identificación en el derecho informático empresarial peruano. 4. La identidad digital y la identificación en el gobierno electrónico peruano. 5. Lineamientos de aplicación en el contexto de la alianza del pacifico. 6. Conclusiones.

Palabras Clave: Identidad Digital. Identificación. Derecho Empresarial Informático. Gobierno Electrónico. Alianza Del Pacifico.

1. Introducción

Esencialmente, la gestión de identidad representa un conjunto de procesos para gestionar la determinación, autenticación y autorización de las personas físicas, entidades jurídicas, dispositivos u otros sujetos en un contexto de línea. Tiene por objeto responder a dos preguntas sencillas que cada una de las partes en una operación en línea se formula acerca de la otra parte, a saber, "¿quién es usted?" y "como puede demostrarlo?" apoyándose en una comprobación fiable de la identidad, una parte en una operación en línea puede decidir,

[1] Doctor en Derecho. Magister en Derecho Empresarial. Profesor de Derecho de las Nuevas Tecnologías y de Derecho Informático en la Universidad ESAN. Experto en Derecho Informático. (Lima, Perú). Email: jnunezp@esan.edu.pe y julionunezponce@gmail.com

> por ejemplo, si celebrar un contrato con la otra parte, si permite a la otra parte el acceso a una base de datos confidencial o si otorga a la otra parte algún otro privilegio o derecho de acceso.[2]

La identidad digital y la identificación permiten en un entorno digital dar seguridad jurídica y técnica tanto a las empresas como al gobierno en temas tales como teletrabajo, sesiones no presenciales de junta de accionistas, contratos empresariales, tributación empresarial, historias clínicas electrónicas, notificación judicial electrónica, expediente electrónico judicial, boleta de pago electrónica, procedimientos administrativos electrónicos, el uso de las firmas y certificados digitales, entre otros temas. Tal es así que las empresas y gobiernos están prestando cada vez más atención e importancia a los sistemas de gestión de identidades y de servicios de confianza.

En este orden de ideas, hay que tener en cuenta que:

> Las Tecnologías de la información y las comunicaciones (TICs) están presentes en todas las actividades humanas e inciden en el ejercicio de los derechos y el cumplimiento de las obligaciones de las personas en la sociedad. La visión sistémica del Derecho Informático permite darle una solución eficaz a los problemas jurídicos que la sociedad de la información plantea. El tema de la identificación de las personas en el "mundo digital" es un tema recurrente y transversal que se interrelaciona con los diversos campos de aplicación del derecho informático.[3]

El objetivo de la presente ponencia es interrelacionar la identidad digital y la identificación con los principales temas del derecho informático empresarial y del gobierno electrónico, teniendo en cuenta los avances en el derecho comparado y exponiendo con una visión jurídica la realidad del ordenamiento jurídico peruano. Además se busca, en base a la realidad peruana concordada con el derecho comparado, dar lineamientos de aplicación de los criterios predominantes en la gestión de identidades y los servicios de confianza, en el Contexto de la Alianza del Pacifico que integran Chile, Colombia, México y Perú.

---

[2] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI): "Posible Labor futura en materia de comercio electrónico: cuestiones jurídicas relacionadas con la gestión de identidad y los servicios de Confianza". Documento A/CN.9/854. Fecha: 05 de Mayo de 2015. Numeral 6. En http://www.uncitral.org/uncitral/es/commission/colloquia/identity-management-2016.html p. 3.

[3] Nuñez Ponce, Julio: "El Derecho Informático y la Identificación". En Revista de Jurisprudencia Institucional del RENIEC "Gaceta Registral". Año VIII. Número 7, 2014. Ed. Registro Nacional de Identificación y Estado Civil (RENIEC). Lima, Perú. p. 30.

2. Aspectos jurídicos relacionados con la gestión de la identidad y los servicios de confianza en el derecho comparado.

En el contexto del Derecho Comparado, hay que tener presente el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (Reglamento eIDAS) establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro, así como las normas para los servicios de confianza y un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.[4]

Otra legislación reciente respecto a la gestión de identidades y servicios de confianza se ha dado en el derecho comparado, entre esta legislación podemos mencionar la siguiente: la ley belga sobre el documento de identidad electrónico[5] , la legislación francesa sobre las firmas electrónicas y también la del correo electrónico certificado[6] y la Electronic Identity Management Act de Virginia (Estados Unidos de América) que entro en vigor el 1 de julio de 2015[7]

Asimismo, cabe mencionar en Italia, el Decreto Legislativo 179 del 26 de agosto de 2016, publicado el 13 de Setiembre de 2016 que modifica el Código de Administración Digital Italiano, estableciendo entre otros temas los siguientes:

a) El Hogar Digital, definido como la dirección de correo electrónico u otro certificado electrónico reconocido relativa a los servicios electrónicos de confianza conforme el Reglamento eIDAS.

[4] También conocido como Reglamento eIDAS desde su dación ha incidido en distintas modificaciones legislativas en el ámbito europeo y global con respecto a la gestión de identidades y los servicios de confianza.
[5] http://www.lachambre.be/FLWB/PDF/53/2745/53K2745006.pdf
[6] http://www.legifrance.gouv.fr
[7] https://leg1.state.va.us/cgi-bin/legp504.exe?151+ful+CHAP0483

b) El uso de la identidad digital que permite la representación informática.
c) El sistema público de conectividad, dirigido a la interacción entre los sistemas informáticos de las entidades participantes, para asegurar la integración de los metadatos, información, procesos y procedimientos administrativos.
d) Que todos los ciudadanos y las empresas tienen derecho a que se le asigne una identidad digital a través del cual acceder y utilizar los servicios públicos seguros.
e) Que todos tienen el derecho a ser identificados por las autoridades públicas a través de la identidad digital, así como enviar mensajes a las administraciones públicas y recibir documentos a través de un hogar digital.
f) El gobierno ofrece, a través de la conectividad del sistema público, una plataforma tecnológica para la interconexión e interoperabilidad entre los servicios públicos y financieros a fin de garantizar la autenticación de las partes involucradas.
g) La promoción de iniciativas para fomentar la difusión de la cultura digital entre los ciudadanos, con especial atención a los niños y personas en riesgo de exclusión, también con el fin de promover el desarrollo de habilidades informáticas legales y el uso de los servicios digitales de las administraciones públicas con acciones específicas y concretas.
h) La promoción de la innovación digital en el país y el uso de las tecnologías digitales en la organización de la administración pública y en la relación entre esta, ciudadanos y empresas, respetando al mismo tiempo los principios de legalidad, equidad, transparencia y criterios de eficiencia, economía y eficacia.
i) La validez y eficacia probatoria del documento informático y el uso de los certificados de firma electrónica cualificada.
j) Disposiciones sobre el sistema público para la gestión de la identidad digital en la modalidad de acceso a los servicios prestados en la red de la Administración Pública.

3. La identidad digital y la identificación en el derecho informático empresarial peruano

a) El Teletrabajo, la Identidad Digital y la Identificación.

La Ley peruana 30036, tiene por objeto "regular el teletrabajo, como una modalidad especial de prestación de servicios caracterizada por la utilización de las tecnologías de la Información y las Comunicaciones (TIC) en las instituciones privadas y públicas, y promover políticas públicas para promover su desarrollo".

El teletrabajo se caracteriza por el desempeño subordinado de labores sin la presencia física del trabajador, denominado "teletrabajador" en la empresa con la que mantiene vínculo laboral, a través de medios informáticos, de telecomunicaciones y análogos, mediante los cuales se ejercen a su vez el control y la supervisión de labores. Son elementos que coadyuvan a tipificar el carácter subordinado de esta modalidad de trabajo la provisión por el empleador de los medios físicos y métodos informáticos, la dependencia tecnológica y la propiedad de los resultados.

Conforme el Reglamento de la Ley peruana de Teletrabajo, D.S. 017-2015-TR, son principios que orientan la aplicación de la modalidad de teletrabajo, los siguientes:

i) Voluntariedad: el empleador por razones debidamente sustentadas, puede efectuar la variación de la prestación de servicios a la modalidad de teletrabajo, contando para ello con el consentimiento del trabajador.

ii) Reversibilidad: el empleador puede reponer al teletrabajador a la modalidad de prestación de servicios anterior al teletrabajo, si se acredita que no se alcanzan los objetivos bajo la modalidad de teletrabajo.

iii) Igualdad de trato: el empleador o entidad pública debe promover la igualdad de trato en cuanto a las condiciones de trabajo de los teletrabajadores, en relación a quienes laboran presencialmente.

iv) Conciliación entre la vida personal, familiar y laboral: promover un equilibrio ente las actividades realizadas en los ámbitos personal, familiar y laboral de los trabajadores, a través de la modalidad de teletrabajo. En tal sentido, deberá

existir una adecuada correspondencia entre la carga de trabajo y la jornada de labores asignada.

La modalidad del teletrabajo puede desarrollarse bajo las siguientes formas:

- Forma completa: el teletrabajador presta servicios fuera del centro de trabajo; pudiendo acudir ocasionalmente a estos para las coordinaciones que sean necesarias.

- Forma mixta: el teletrabajador presta servicios de forma alternada dentro y fuera del centro de trabajo.

El teletrabajador tiene los mismos derechos y beneficios que los trabajadores que prestan servicios bajo la modalidad convencional, de acuerdo al régimen que pertenezca cada teletrabajador, salvo aquellos vinculados a la asistencia al centro de trabajo. Entre los derechos que serán garantizados se encuentran las vacaciones, compensación por tiempo de servicios, gratificaciones, capacitación, intimidad e inviolabilidad de las comunicaciones y documentos privados del teletrabajador, protección de la maternidad, seguridad y salud en el trabajo, libertad sindical.

b) Sesiones No Presenciales de Junta General de Accionistas

Por Decreto Legislativo 1061, publicado el sábado 28 de Junio de 2008 se ha adicionado el artículo 21-A sobre voto electrónico, en la Ley General de Sociedades, Ley 26887. El artículo 21-A está ubicado en el Libro 1 de reglas aplicables a todas las sociedades.

Se ha adicionado a la Ley General de Sociedades el artículo 21-A, de la siguiente forma:

> "Artículo 21ºA.- Voto por medio electrónico o postal.
> Los accionistas o socios podrán para efectos de la determinación del quórum, así como la respectiva votación y adopción de acuerdos, ejercer el derecho a voto por medio electrónico siempre que éste cuente con firma digital o por medio postal a cuyo efecto se requiere contar con firmas legalizadas.
> Cuando se utilice firma digital, para ejercer el voto electrónico en la adopción de acuerdos, el acta electrónica resultante deberá ser almacenada mediante microforma digital (documento electrónico con valor legal), conforme a ley.
> Cuando la sociedad aplique estas formas de voto deberá garantizar el respeto al derecho de intervención de cada accionista o socio, siendo responsabilidad del presidente de la junta el cumplimiento de la presente disposición.

> La instalación de una junta o asamblea universal, así como la voluntad social formada a través del voto electrónico o postal tiene los mismos efectos que una junta o asamblea realizada de manera presencial.

En las sesiones no presenciales por medios electrónicos, la identidad digital es fundamental para el ejercicio de los derechos de los accionistas con seguridad jurídica y técnica. El uso de la firma digital, los certificados digitales y la microforma digital[8] coadyuvan con esta finalidad.

c) Ley que crea el registro de Historias Clínicas Electrónicas

La Ley peruana 30024, regula en forma específica la autenticación de la identidad de las personas para acceder al Registro Nacional de Historias Clínicas Electrónicas. Se define al Registro Nacional de Historias como la "infraestructura tecnológica especializada en salud que permite al paciente o su representante legal y a los profesionales de salud que son previamente autorizados por aquellos, el acceso a la información clínica contenida en las historias clínicas electrónicas, dentro de los términos estrictamente necesarios para garantizar la calidad de la atención en los establecimientos de salud y en los servicios médicos de apoyo públicos, privados o mixtos, en el ámbito de la Ley General de Salud".

La autenticación de la identidad utilizando las firmas y certificados digitales, es una característica de este sistema que permite la utilización de la identidad digital en el campo empresarial de las clínicas y de los establecimientos de salud tanto privados como públicos. En este sentido, se aplica al sistema de historias clínicas electrónicas, los siguientes conceptos:

> La gestión de identidad se ha convertido en un requisito fundamental de las actividades del comercio electrónico (y de historias clínicas electrónicas), en particular a medida que aumenta la importancia y la confidencialidad de esas operaciones. De hecho, en un informe

[8] La microforma digital es la imagen digital de un documento con valor probatorio y efecto legal, que cumplen requisitos técnicos y formales que garantizan su seguridad técnica y jurídica. Los requisitos técnicos garantizan la absoluta fidelidad e integridad de las imágenes digitalizadas, garantizando la durabilidad, inalterabilidad y fijeza iguales o superiores al documento original. Los requisitos formales garantizan que el depositario de la fe pública (fedatario juramentado) autentique el proceso de micrograbación ya sea de papel a papel o de papel a digital, garantizando la fidelidad entre la imagen digitalizada y el documento digital, dando certeza y seguridad jurídica. En el Perú, el sistema legal de microforma digital está regulado por el Decreto Legislativo Nº 681 y por la Ley 26612.

de orientación de la OCDE relativo a la gestión de identidad se señalaba que la gestión de identidad es fundamental para el desarrollo ulterior de la economía de internet.[9]

El sistema de historias clínicas electrónicas es un servicio electrónico prestado habitualmente que consiste en: a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios. b) la creación, verificación y validación de certificados para la autenticación de sitios web. c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios. d) La consulta de la información médica por medios electrónicos, previa autenticación y comprobación de la identidad digital.

4. La identidad digital y la identificación en el gobierno electrónico peruano.

"Aquellos que se enfrentan con el problema de cómo verificar la identidad de las personas harían bien hacerse la siguiente pregunta: ¿Identidad con qué? Una vez que se tiene la respuesta a esta pregunta. Hay que adoptar una posición para hacer frente, sobre una base racional, la tarea de decidir qué pruebas será de utilidad para el proceso"[10] .

El Gobierno electrónico es el uso de las Tecnologías de Información y Comunicaciones (TICs) para mejorar la gestión y los servicios, garantizar la transparencia y la participación y facilitar el acceso seguro a la información pública. Las características del Gobierno electrónico son: a) El centro de atención es el ciudadano. b) Mejora constante de procesos (*work flow*). c) Ubicuidad del Estado. El Estado está donde el ciudadano más lo necesita.

[9] OECD "Digital Identity Management for Natural Persons. Enabling Innovation and Trust in the Internet Economy- Guidance for Government Policy Makers", OECD Digital Economy Papers, núm.196, 17 April 2012. OECD Publishing. Page 3. En: http://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826

[10] Bohm, Nicholas and Mason Stephen: "Identity and its verification". In Computer Law & Security Review, Volume 26, Numer 1, Jannuary 2010. Pages 43-51.

Estos servicios deben ser prestados en un marco de seguridad jurídica y técnica. Al respecto, hay que tener presente:

> Una alternativa planteada para afrontar las amenazas en Internet es la identidad digital basada en certificados digitales…Lo que posibilita hacer realidad esta aspiración de tramitar y transaccionar de manera segura y confiable en el mundo del ciberespacio no es otra cosa que la identidad digital basada en certificados digitales. La identidad digital es la posibilidad de verificar que soy la persona que digo ser en internet, de manera indubitable. Para eso es necesaria la autenticación a partir de lo que tengo, lo que se y lo que soy.[11]

La identidad digital formal requiere de un documento credencial electrónico que con seguridad autentique a la persona en Internet. En este orden de ideas, debemos definir a este documento en el marco de la legislación peruana:

> "El DNI electrónico es una tarjeta inteligente (*Smart Card*) con chip de contactos, capacidades criptográficas y certificaciones internacionales de seguridad FIPS y Common Criteria, para cuya lectura se requiere el dispositivo correspondiente… En el marco de las buenas prácticas en documentos de identidad electrónicos de otros países y los estándares internacionales, se conceptualizó el DNIe como documento de identidad de usos múltiples. Acorde con ello, se contempló implementar en su chip las siguientes funcionalidades: a) El DNIe ofrece la funcionalidad de identificación a través de una primera aplicación de identidad basada en la definida por OACI para los documentos de viaje de lectura mecánica (eMRTDs). Esta aplicación posibilita la autenticación del titular de manera presencial y con la certeza de que el documento y sus contenidos son originales y no han sido cambiados. b) Las funcionalidades de firma digital y autenticación de la identidad en entornos electrónicos mediante certificados digitales se hace posible con la aplicación PKI, ello incluso de forma remota o por Internet. c) Bajo la funcionalidad de autenticación biométrica de la identidad Match-On-Card, el chip lleva almacenadas en una zona segura de su memoria las plantillas biométricas correspondientes a las huellas dactilares de los dedos índice derecho e izquierdo del titular del documento, posibilitándose así el contrastarlas con las de la persona que porta el documento de manera que se produzca su validación.[12]

En el Perú, en octubre de 2014, RENIEC presentó al Congreso de la República, el Proyecto de Ley de Identidad digital[13]. Este proyecto, tiene entre otros el siguiente contenido:

---

[11] Yrivarren, Jorge: "Identidad, Identificación y persona humana; por la institucionalidad de lo diverso". En Identidad Digital: La Identificación desde los registros parroquiales al DNI electrónico. Ed. Registro Nacional de Identificación y Estado Civil (RENIEC). Lima, Perú. Primera edición. Diciembre de 2015. Página 36.

[12] Cueva, Eddie et al: "El Documento Nacional de Identidad Electrónico". En identidad digital: La Identificación desde los registros parroquiales al DNI electrónico. Ed. Registro Nacional de Identificación y Estado Civil (RENIEC). Lima, Perú. Primera edición. Diciembre de 2015. Páginas 205-206.

[13] Proyecto de Ley Nº 3900-2014-RENIEC, del mes de Octubre de 2014. Presentado en el Congreso de la República del Perú, en el periodo 2011-2016.

a) Objeto.- La presente Ley tiene por objeto reconocer el derecho de todas las personas a la inclusión digital y regular el derecho a la identidad digital para el uso de servicios de gobierno electrónico seguro, prestados por las entidades de la Administración Pública.
b) Concepto de identidad digital: Entiéndase por identidad digital de las personas naturales y jurídicas a aquella basada en un documento credencial electrónico, emitido en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), y conforme a las disposiciones legales vigentes.
c) Servicios Seguros: La identidad digital permite la identificación y autenticación de modo fehaciente en medios electrónicos, para el uso de los servicios de gobierno y comercio electrónico seguros, prestados dentro de la Infraestructura Oficial de Firma Electrónica (IOFE).
d) Identidad digital nacional: Entiéndase por identidad digital nacional a aquella identidad digital que es atribuida a las personas naturales nacionales a través de su Documento Nacional de Identidad electrónico (DNIe), emitido por el Registro Nacional de Identificación y Estado Civil (RENIEC).
e) Registro para la obtención de la identidad digital: El registro para la obtención de la identidad digital es el proceso mediante el cual una Entidad de Registro o Verificación, debidamente acreditada ante la Autoridad Administrativa Competente (INDECOPI), identifica presencialmente a la persona, gestionando ante una Entidad de Certificación acreditada la correspondiente emisión del documento credencial electrónico que contiene su identidad digital.

   En el caso de las personas naturales nacionales se verificará su identidad a través de las bases de datos del Registro Nacional de Identificación y Estado Civil (RENIEC) y tratándose de las personas jurídicas se verificará la existencia de la misma mediante los instrumentos públicos pertinentes, observándose según el caso el nivel de seguridad que corresponda según lo previsto en la normatividad vigente.
f) Responsabilidad: Es responsabilidad de la Entidad de Registro o Verificación, debidamente acreditada ante la Autoridad Administrativa Competente (INDECOPI)

y operando dentro de la Infraestructura Oficial de Firma Electrónica (IOFE), llevar el registro respectivo para la obtención de la referida identidad digital.

g) Identificación digital: La identificación digital es el proceso a través del cual una persona ejerce su identidad digital en medios electrónicos seguros.

h) Autenticación digital: La autenticación digital es el proceso por el cual se confirma la identidad digital de una persona, permitiéndosele el uso de servicios de gobierno y comercio electrónico seguros.

   Para verificar la identidad digital de una persona en servicios ofrecidos por canales electrónicos, el proceso de autenticación digital utilizara como mínimo dos (2) de los factores de autenticación siguientes:

   i) Algo que el usuario posee, ya sean tarjetas o dispositivos criptográficos, tabletas, teléfonos móviles, u otros, los cuales deberán cumplir con las especificaciones técnicas para el almacenamiento de las claves privadas de entidad final- usuarios- establecidas por la Autoridad Administrativa competente.

   ii) Algo que el usuario conoce, a través de la contraseña de acceso a la clave privada de los Certificados Digitales.

   iii) Algo que el usuario es, a través de sus características biométricas.

Tratándose de servicios prestados vía canales electrónicos no presenciales, uno de los factores de autenticación será necesariamente el indicado en el inciso ii). Entiéndase por no presenciales aquellas comunicaciones y/o transacciones efectuadas en línea en que las personas no se hayan una en presencia de la otra.

Cuando el proceso de autenticación digital incluya características biométricas conforme el inciso ii) del presente artículo, pueden utilizarse sistemas biométricos como, entre otros, la verificación de huellas digitales, del iris del ojo, del perfil genético, de la voz, del rostro, en la medida que estén respaldados por plataformas tecnológicas seguras basados en estándares internacionalmente aceptados.

5. Lineamientos de aplicación en el contexto de la alianza del pacifico.

> "La Alianza del Pacífico constituye un área de integración profunda para avanzar hacia la libre circulación de bienes, servicios, capitales y personas e impulsar un mayor crecimiento, desarrollo y competitividad de las economías de las Partes. Nació como iniciativa del Perú, a raíz de la invitación realizada por su Presidente en el 2010 a sus contrapartes de Colombia y Chile para conformar un "área de integración profunda", en la que se asegure plena libertad para la circulación de bienes, servicios, capitales y personas, con miras a convertir este espacio en un modelo de integración para la región, consolidando además una plataforma económica común con proyección a otras partes del mundo, especialmente, el Asia. Posteriormente, México se sumó a la iniciativa conformada por Colombia, Chile y Perú"[14]

La identidad digital va a permitir aplicar el enfoque de gobierno digital, conectividad y "minería de datos", de forma tal de personalizar la atención del Gobierno a cada ciudadano según sus necesidades y especiales características, facilitando la circulación de bienes, servicios y capitales, lo cual está acorde con su finalidad.

En este orden de ideas, la Alianza del Pacifico tiene como objetivos los siguientes:

> a) construir de manera participativa y consensuada, un área de integración profunda para avanzar progresivamente hacia la libre circulación de bienes, servicios, capitales y personas; b) impulsar un mayor crecimiento, desarrollo y competitividad de las economías de las Partes, con miras a lograr un mayor bienestar, la superación de la desigualdad socio económica y la inclusión social de sus habitantes y c) convertirse en una plataforma de articulación política, de integración política y comercial, y de proyección al mundo, con especial énfasis al Asia Pacifico. [15]

En el cumplimiento de los objetivos de la APEC, la identidad digital tiene un papel preponderante porque coadyuvará a consolidar la integración profunda y la inclusión digital de sus habitantes.

En los documentos jurídicos de la Alianza del Pacifico, es necesario mencionar los siguientes artículos del Acuerdo Marco:

a) ARTÍCULO 13.8: Protección de la Información Personal 1. Las Partes deberán adoptar o mantener leyes, regulaciones o medidas administrativas para la protección de la información personal de los usuarios que participen en el comercio electrónico. Las Partes tomaran en consideración los estándares internacionales que existen en esta

[14] Acuerdos Comerciales del Perú. Ministerio de Comercio Exterior y Turismo del Perú. Alianza del Pacifico. http://www.acuerdoscomerciales.gob.pe/index.php?option=com_content&view=category&layout=blog&id=166&Itemid=185

[15] Acuerdo Marco de la Alianza del Pacifico. Art. 3. Suscrito en Paranal, Antofagasta. República de Chile, el 06 de Julio de 2012. En http://www.sice.oas.org/Trade/PAC_ALL/Framework_Agreement_Pacific_Alliance_s.pdf

materia. 2. Las Partes deberán intercambiar información y experiencias en cuanto a su legislación de protección de la información personal.

b) ARTÍCULO 13.9: Mensajes Comerciales Electrónicos no Solicitados Las Partes adoptarán o mantendrán medidas para proteger a los usuarios, de los mensajes comerciales electrónicos no solicitados.

c) ARTÍCULO 13.10: Autenticación y Certificados Digitales
1. Ninguna Parte podrá adoptar o mantener legislación sobre autenticación electrónica, que impida a las partes de una transacción realizada por medios electrónicos, tener la oportunidad de probar ante las instancias judiciales o administrativas correspondientes, que dicha transacción electrónica cumple los requerimientos de autenticación establecidos por su legislación.
2. Las Partes establecerán mecanismos y criterios de homologación que fomenten la interoperabilidad de la autenticación electrónica entre ellas de acuerdo a estándares internacionales. Con este propósito, podrán considerar el reconocimiento de certificados de firma electrónica avanzada o digital según corresponda, emitidos por prestadores de servicios de certificación, que operen en el territorio de cualquier Parte de acuerdo con el procedimiento que determine su legislación, con el fin de resguardar los estándares de seguridad e integridad.

d) ARTÍCULO 13.11: Flujo Transfronterizo de Información Con el objetivo de profundizar las relaciones en materia de comercio electrónico, las Partes considerarán a futuro la negociación de compromisos relacionados con flujo transfronterizo de información.

e) ARTÍCULO 13.12: Cooperación Reconociendo la naturaleza global del comercio electrónico, las Partes afirman la importancia de:
(i) Trabajar conjuntamente para facilitar el uso del comercio electrónico por las micro, pequeñas y medianas empresas;
(ii) Compartir información y experiencias sobre leyes, regulaciones, y programas en la esfera del comercio electrónico, incluyendo aquellos relacionados con protección de la información personal, protección del consumidor, seguridad en las comunicaciones electrónicas, autenticación, derechos de propiedad intelectual, y gobierno electrónico;
(iii) Trabajar para mantener los flujos transfronterizos de información como un elemento esencial en el fomento de un entorno dinámico para el comercio electrónico;
(iv) Fomentar el comercio electrónico promoviendo la adopción de códigos de conducta, modelos de contratos, sellos de confianza, directrices y mecanismos de aplicación en el sector privado, y
(v) Participar activamente en foros regionales y multilaterales, para promover el desarrollo del comercio electrónico. [16]

Estas disposiciones nos muestran el grado de avance del marco legal vigente, que consolida la oportunidad de encontrar los medios adecuados para fortalecer y promover la

[16] Protocolo Adicional al Acuerdo Marco de la Alianza del Pacifico. Suscrito en Cartagena de Indias, el 10 de Febrero de 2014. Capítulo 13: Comercio Electrónico. En http://www.acuerdoscomerciales.gob.pe/index.php?option=com_content&view=category&layout=blog&id=168&Itemid=187

identidad digital y consolidar la legislación en torno al derecho informático empresarial y al gobierno electrónico seguro.

6. Conclusiones

La identidad digital permite la identificación y autenticación de modo fehaciente en medios electrónicos en el Derecho Informático Empresarial y en el uso de los servicios de gobierno electrónico seguro, prestados dentro de la Infraestructura Oficial de Firma Electrónica (IOFE). El Derecho Informático con un enfoque digital, tiene en la identidad digital el factor de cohesión para la seguridad jurídica y técnica en Internet.

Para un adecuado ejercicio de la identidad digital, los mecanismos de identificación deben estar adecuadamente regulados, por cuánto la identificación digital es el proceso a través del cual una persona ejerce su identidad digital en medios electrónicos seguros.

La Alianza del Pacifico, es un marco de integración adecuado para el fortalecimiento de la identidad digital para su uso en el derecho informático empresarial y en el gobierno electrónico seguro. En la Alianza del Pacifico los países miembros: Colombia, Chile, México y Perú deben armonizar su legislación en torno al fortalecimiento de la identidad digital como un medio de lograr en un entorno electrónico seguro la libre circulación de bienes, personas y capitales con seguridad que disminuya los riesgos de suplantación de identidad y el uso fraudulento de identidades múltiples.

Consideramos, que el tema tratado es propicio para un tratamiento académico conjunto de las universidades y expertos de los países miembros, sobre la regulación y estrategias más adecuadas para fortalecer y promover el uso de la identidad digital en los países miembros de la Alianza del Pacifico.

Bibliografía

- BOHM, Nicholas and MASON Stephen: “Identity and its verification”. In Computer Law & Security Review, Volume 26, Numer 1, Jannuary 2010.
- COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (CNUDMI): “Posible Labor futura en materia de comercio

electrónico: cuestiones jurídicas relacionadas con la gestión de identidad y los servicios de Confianza". Documento A/CN.9/854. Fecha: 05 de Mayo de 2015. Numerales 22. En http://www.uncitral.org/uncitral/es/commission/colloquia/identity-management-2016.html

- CUEVA, Eddie et al: "El Documento Nacional de Identidad Electrónico". En IDENTIDAD DIGITAL: La Identificación desde los registros parroquiales al DNI electrónico. Ed. Registro Nacional de Identificación y Estado Civil (RENIEC). Lima, Perú. Primera edición. Diciembre de 2015.
- NUÑEZ PONCE, Julio: "El Derecho Informático y la Identificación". En Revista de Jurisprudencia Institucional del RENIEC "Gaceta Registral". Año VIII. Número 7, 2014. Ed. Registro Nacional de Identificación y Estado Civil (RENIEC). Lima, Perú.
- OECD. "Digital Identity Management for Natural Persons. Enabling Innovation and Trust in the Internet Economy- Guidance for Government Policy Makers", OECD Digital Economy Papers, núm.196, 17 April 2012. OECD Publishing. Pages 34. En http://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-papers_20716826
- YRIVARREN, Jorge: "Identidad, Identificación y persona humana; por la institucionalidad de lo diverso". En IDENTIDAD DIGITAL: La Identificación desde los registros parroquiales al DNI electrónico. Ed. Registro Nacional de Identificación y Estado Civil (RENIEC). Lima, Perú. Primera edición. Diciembre de 2015.
- Acuerdos Comerciales del Perú. Ministerio de Comercio Exterior y Turismo del Perú. Alianza del Pacifico.
- Proyecto de Ley Nº 3900-2014-RENIEC, presentado al Congreso de la Republica del Perú en Octubre del 2014; en el periodo legislativo 2011-2016. http://www.acuerdoscomerciales.gob.pe/index.php?option=com_content&view=category&layout=blog&id=166&Itemid=185

- http://www.lachambre.be/FLWB/PDF/53/2745/53K2745006.pdf
- http://www.legifrance.gouv.fr
- https://leg1.state.va.us/cgi-bin/legp504.exe?151+ful+CHAP0483