Las Leyes que regulan los Sistemas de Identidad (v2)

Thomas J. Smedinghoff

Tabla de contenidos

Resumen

Los sistemas de identidad y sus participantes están regulados por un conjunto de leyes, normas, regulaciones y requisitos contractuales, complejos e innumerables. Este artículo ofrece un panorama general del entorno legal que regula los sistemas de identidad, enfocándose en tres niveles diferentes de normativa jurídica: Ley General, Ley General de Sistemas de Identidad y Ley Específica de Sistemas de Identidad.

Introducción

¿Cuáles son las normas jurídicas que regulan los sistemas de identidad? ¿Qué obligaciones imponen estas normas a los involucrados?

La realidad es que los sistemas de identidad y sus participantes están regulados por un conjunto de leyes, normativas, regulaciones y requisitos contractuales, complejos e innumerables, y las obligaciones que imponen no siempre están claras. Para entender todo esto, lo mejor es enfocarse primero en el entorno legal que regula los sistemas de identidad.

Terminología

- Ley de protección del consumidor - Leyes y regulaciones que están diseñadas para proteger los derechos de los consumidores individuales y para impedir prácticas de negocio desleales, engañosas y fraudulentas.

- Derecho contractual – Leyes relativas a la creación y ejecución de acuerdos entre partes distintas.

- Ley antifraude – Leyes que protegen contra la representación falsa e intencional de información hecha por una persona hacia otra que confía en ella, con conocimiento de su falsedad y con el propósito de inducir a la otra persona a actuar de forma que resulte en daños y perjuicios para sí misma.

- Leyes de robo de identidad – Leyes que rigen los crímenes en los que un perpetrador accede a información personal sensible perteneciente a la víctima (como fecha de nacimiento, contraseñas, direcciones de correo electrónico, números de seguridad social, registros financieros, etc.) y luego la utiliza para hacerse pasar por la víctima para beneficio personal, como por ejemplo cometer fraude, sacar préstamos en nombre de la víctima o acceder a las cuentas de la víctima.

- Ley de privacidad - Es el conjunto de leyes que regula la recopilación, uso, almacenamiento y transferencia de datos personales asociados a individuos identificados o identificables.

- *Tort Law* (responsabilidad civil extracontractual) - Es el cuerpo de jurisprudencia de situaciones en las que el comportamiento de una persona causa daños, perjuicios, sufrimiento o pérdida injusta a otra persona, otorgando a la persona damnificada el derecho de iniciar una demanda civil con el fin de ser compensada por la persona que causó el daño. Algunos ejemplos de esto son: agresión, fraude, difamación, negligencia y responsabilidad objetiva.

El entorno legal de los sistemas de identidad

A grandes rasgos, el entorno legal que regula las operaciones de cualquier sistema de identidad se conforma de tres niveles diferentes de normas jurídicas que se clasifican de la siguiente manera:

- Nivel 1: Ley general: El primer nivel abarca la ley que se aplica de forma general a todas las actividades de negocio y personales. Esta ley abarca una amplia variedad de temas y, aunque con frecuencia y en la medida que corresponda se la aplica a las actividades de los sistemas de identidad, no fue redactada pensando en ellos. Algunas de las leyes generales que pueden interferir en el funcionamiento de un sistema de identidad son: el derecho contractual, *Tort*, las leyes de privacidad, las leyes de garantía y las leyes de protección del consumidor.

- Nivel 2: Ley general de sistemas de identidad: El segundo nivel abarca las leyes generales dictadas específicamente para regular los sistemas de identidad. Normalmente, las leyes de administración de identidades de nivel 2 aplican a todos los sistemas de identidad dentro de una jurisdicción y son, por naturaleza, generales. Actualmente existen muy pocas leyes de nivel 2. Algunos ejemplos de leyes generales de sistemas de identidad son la legislación sobre la administración electrónica de identidades de Virginia[1] y el borrador de cláusulas sobre el reconocimiento transfronterizo de la IdM y de los servicios de confianza[2] que está siendo desarrollado por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). En muchas jurisdicciones aún no existen leyes de nivel 2 para los sistemas de identidad.

- Nivel 3: Leyes específicas de los sistemas de identidad: El tercer nivel de normas jurídicas consiste en un conjunto de reglas de sistema específicas para regular el funcionamiento de un sistema de identidad determinado. Estas reglas proveen las especificaciones y regulaciones técnicas, de negocio y operativas para el sistema de identidad, especifica los derechos y las responsabilidades de los participantes y regula las relaciones entre las diversas partes. Pueden ser muy detalladas, pero aplican únicamente dentro de los límites del sistema de identidad para el cual fueron escritas.

---

[1] Código de Virginia - Capítulo 50. "Ley de Gestión de la Identidad Electrónica. 2015". https://law.lis.virginia.gov/vacode/title59.1/chapter50/.

[2] "Proyecto de Disposiciones sobre el Reconocimiento Transfronterizo de IdM y Servicios de Confianza," revisión A/CN.9/WG.IV/WP.160, Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, revisado por última vez el 16 de septiembre de 2019, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/wp-160-e.pdf.

En los sistemas de identidad del sector privado, estas normas suelen basarse en contratos y con frecuencia se las llama marco de confianza o reglas de sistema, y aplican únicamente a los participantes del sistema que las hayan aceptado por contrato. Algunos ejemplos de esto son el Marco de confianza de identidad SAFE (anteriormente llamado Marco de confianza SAFE-BioPharma),[3] el Marco de gobernanza Sovrin,[4] y el Marco de confianza concierge de SecureKey.[5]

En el caso de los sistemas de identidad gubernamentales, estas leyes de nivel 3 suelen estar incorporadas dentro de una ley o regulación promulgada por el gobierno y por lo tanto aplica a todos quienes participen en el sistema de identidad. Algunos ejemplos son el Reglamento EIDAS de la Unión Europea,[6] la Ley de documentos de identidad de Estonia,[7] y la Ley *Aadhaar Act* de India.[8] Sin embargo, a veces los sistemas de identidad gubernamentales también utilizan marcos de confianza basados en contratos como el Marco de Identidad Digital Confiable (TDIF, por sus siglas en inglés)[9] usado en el sistema nacional de identidad federada de Australia.

La parte del entorno legal correspondiente al nivel 3 de cualquier sistema de identidad está bajo supervisión de los desarrolladores de ese sistema de identidad (ya sea gubernamental o del sector privado). Esto significa que los operadores de un sistema de identidad del sector privado tienen la libertad de crear y diseñar las reglas de sistema de nivel 3 según les parezca mejor para cumplir con los objetivos de ese sistema de identidad específico. Dicho esto, en el caso de reglas basadas en contratos estas solo aplicarán a los participantes que las hayan aceptado y pueden ser complementadas (y en algunos casos

---

[3] "Mayor seguridad a través del marco de confianza de identidad SAFE," consultado el 18 de mayo de 2021, *SAFE Identity*, https://makeidentitysafe.com/trust-framework/.

[4] "Marco de gobernanza de Sovrin," consultado el 18 de mayo de 2021, Sovrin, https://sovrin.org/library/sovrin-governance-framework/.

[5] "Marco de confianza concierge de SecureKey," consultado el 10 de octubre de 2019, SecureKey, https://securekey.com/resources/trust-framework-securekey-concierge-in-canada/.

[6] Reglamento eIDAS[UE]: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32014R0910

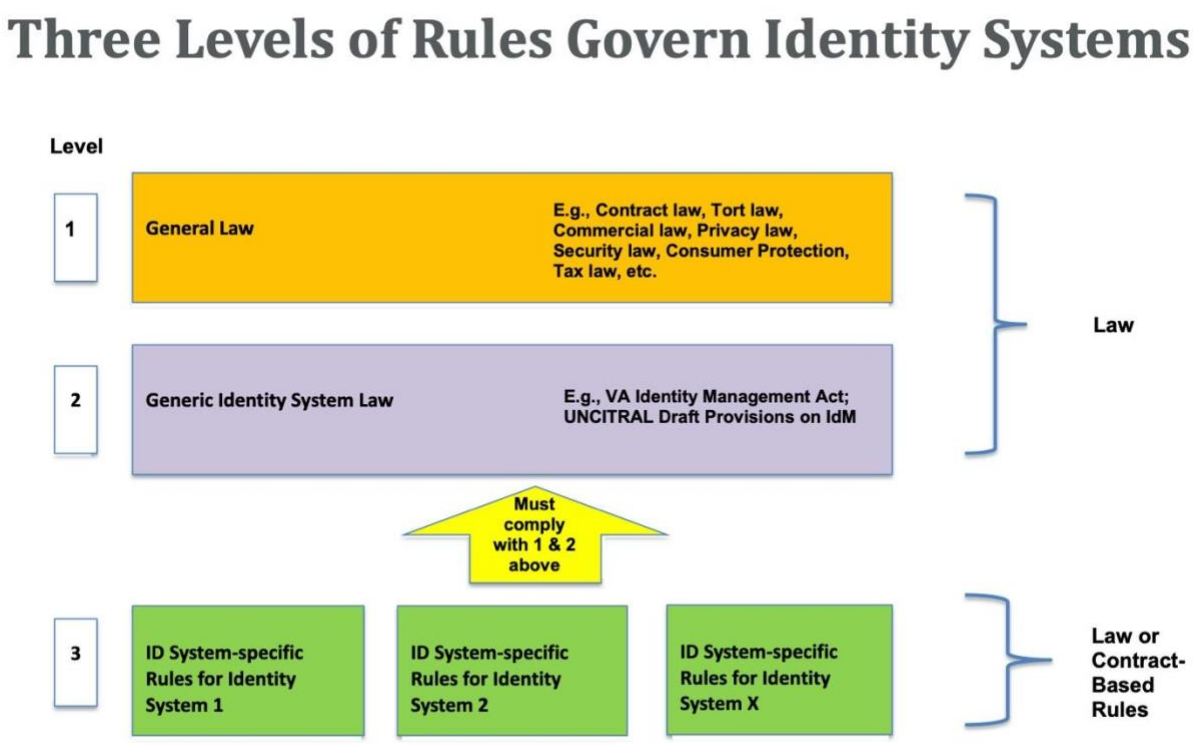
[7] Ley de documentos de identidad [Estonia]: http://www.unhcr.org/refworld/docid/4728ab1b2.html

[8] Ley Aadhaar https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

[9] "Marco de identidad digital confiable," consultado el 18 de mayo de 2021, Agencia de Transformación Digital del Gobierno australiano, https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework

incluso anuladas) por leyes y regulaciones de nivel 1 y 2. En otras palabras, las normas de nivel 3 diseñadas para cualquier sistema de identidad específico deben cumplir con las leyes existentes - desafío que se profundiza por las dificultades que presentan los sistemas de identidad que atraviesan los límites jurisdiccionales.

El siguiente diagrama resume la estructura del entorno legal de este sistema de identidad:



Esta estructura del entorno legal de un sistema de identidad es muy similar a la que regula un sistema de tarjetas de crédito (como Amex®, Discover®, MasterCard®, o Visa®). Cada sistema de tarjetas de crédito está regulado por reglas de sistema de nivel 3 que fueron desarrolladas por el operador de ese sistema (por ej., las reglas de MasterCard[10], las reglas centrales de Visa y las reglas de producto y servicio de Visa[11]). Estas reglas proveen especificaciones técnicas, de negocio y operativas para el sistema de tarjeta de crédito específico y regula las relaciones entre las diversas partes. Son vinculantes por contrato a

[10] "Reglas de MasterCard," consultado el 18 de mayo de 2021, MasterCard, https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html.
[11] "Reglas principales de Visa y reglas de productos y servicios de Visa," 15 de octubre de 2013, consultado el 18 de mayo de 2021, Visa,https://usa.visa.com/dam/VCOM/download/merchants/visa-international-operating-regulations-main.pdf.

las partes participantes del sistema (por ej., titulares de tarjetas de crédito, comerciantes, bancos emisores, procesadores, etc.).

Estas reglas de sistema de tarjeta de crédito de nivel 3 y los contratos asociados también están regulados por: (1) la ley general de nivel 1 (por ej., el derecho contractual, la ley de negligencia, etc.), y la ley general del sistema de tarjeta de crédito dictada para regular todos los sistemas de tarjetas de crédito (por ej., la Regulación Z[12] en los Estados Unidos). Al igual que en los entornos legales de sistemas de identidad, las reglas de sistema y contratos de nivel 3 junto con las normativas de nivel 1 y 2, conforman el entorno legal en el cual opera cada sistema de tarjetas de crédito.

Las Normas jurídicas que regulan los sistemas de identidad

Nivel 1 – Ley General

Actualmente, la mayor parte de la ley que se aplica a los sistemas de identidad es ley general (Nivel 1). Generalmente, esta ley fue redactada con un propósito no relacionado a la administración de identidades (por ej., *Tort*, el derecho contractual, la ley de garantía, ley de privacidad, etc.) y sin considerar cómo podría aplicar a los sistemas de identidad. De hecho, en muchos casos fue redactada antes que el concepto de sistemas de identidad existiese. Algunas leyes generales fueron desarrolladas a lo largo de cientos de años ya sea mediante derecho anglosajón o decisiones de tribunales y sin embargo aplican a las actividades de sistemas de identidad de formas insospechadas para la época en la que fueron adoptadas.

Esencialmente, los sistemas de identidad manejan información. Por lo tanto, las leyes de nivel 1 que aplican a los sistemas de identidad suelen ser aquellas que abordan diversos aspectos de las transacciones que involucran información. Principalmente, esto incluye la normativa que regula los siguientes aspectos de la información:

-- Recopilación, uso y transferencia de la información de identidad

La información de identidad de un individuo es información personal y los procesos de los sistemas de identidad suelen implicar la recopilación y procesamiento (por parte de un proveedor de identidad, proveedor de atributos, o sus respectivos agentes) y la divulgación (a un tercero confiable) de dicha información personal sobre un sujeto. Por lo tanto, las leyes de ***privacidad*** van a regular la recopilación, almacenamiento, uso y transferencia de la información de identidad y tendrán un impacto importante en todos los participantes de

[12] "§ 1026.1 Autoridad, propósito, cobertura, organización, ejecución y responsabilidad," 12 CFR Prt 1026 (Regulación Z), Oficina de protección financiera del consumidor, consultado el 18 de mayo de 2021 https://www.consumerfinance.gov/rules-policy/regulations/1026/.

sistemas de identidad y en todas las transacciones de sistemas de identidad. Esto incluye, por ejemplo, la imposición de límites sobre qué información puede ser recopilada, requisitos de notificación de las prácticas de recopilación, límites en el uso que puede hacerse de dicha información y restricciones en la transferencia de dicha información a terceras partes y/o por fuera de las fronteras del país.

-- Exactitud de la información de identidad

La exactitud y veracidad de la información de identidad que están comunicando o en la cual están confiando, es una preocupación fundamental de todos los participantes de un sistema de identidad. La información de identidad inexacta puede causar una variedad de problemas para las personas que confían en esa información y acarrear responsabilidades a quienes la provean.

Las leyes que regulan la provisión de información falsa o incorrecta, sea intencionalmente o por negligencia, son relevantes para la evaluación de los derechos, obligaciones y responsabilidades de los participantes de sistemas de identidad, incluyendo a los proveedores de identidad, proveedores de atributos y sujetos de datos.

Las más notorias son las leyes ***antifraude*** y las leyes de ***robo de identidad***. El fraude es la representación de un hecho (u omisión de hechos) con el objetivo de engañar a otro, perjudicándolo materialmente. El robo de identidad ocurre cuando un tercero adquiere, transfiere, toma posesión o usa la información personal de alguien de forma no autorizada, con la intención de cometer un fraude u otros crímenes.

Aún en la ausencia de fraude, el *Tort* de ***falsa representación por negligencia*** puede generar responsabilidades por la comunicación de información falsa. Esto ocurre cuando la información está destinada a guiar a otros en sus transacciones de negocio, pero el proveedor de información no tuvo suficiente cuidado al determinar la exactitud de la información antes de comunicarla. Por eso, en determinadas circunstancias, una aserción incorrecta de uno o más atributos de identidad puede calificar como falsa representación por negligencia.

Este *Tort* de falsa representación por negligencia genera el deber de ejercer un cuidado razonable o de tener la capacidad de verificar hechos, y adjudica responsabilidades por hacer falsas representaciones por no tener un cuidado razonable de la exactitud de los hechos afirmados. No obstante, no convierte al proveedor de información (por ej., el proveedor de identidad) en un garante de la exactitud de la aserción de identidad. En general, el proveedor de información no tiene responsabilidad por información “falsa” o inexacta salvo que el proveedor haya fallado en ejercer un cuidado razonable en la obtención o comunicación de la información.

En la medida que la información de identidad erróneamente comunicada dañe la reputación del sujeto de datos, el *Tort* de ***difamación*** también es relevante. La difamación es la declaración falsa o maliciosa de hechos sobre una persona que se divulga a terceras partes, causando daños a la persona. En determinadas situaciones, las aserciones incorrectas de identidad o de atributos pueden ser consideradas difamatorias. Por ejemplo, la aserción de un atributo inexacto - por ej., la edad, información médica, orientación sexual, afiliación política o información laboral -- puede ser considerado como difamatorio en determinados casos en los que resulte en daños a la persona mencionada.

La exactitud o fiabilidad de los atributos de información de identidad comunicados por un proveedor de identidad o por un proveedor de atributos a un tercero confiable también pueden estar regulados por leyes de ***garantía***. Una garantía es una certeza, promesa o aseveración que hace una parte a otra de que los hechos o condiciones son veraces y confiables para la otra parte.

Una garantía puede ser expresa o implícita. Una *garantía expresa* surge de declaraciones específicas hechas de una parte a la otra. Estas declaraciones pueden hacerse por escrito, como en un contrato o anuncio, o verbalmente, como a través de un representante de ventas. Por ejemplo, los procesos que divulga un proveedor de identidad incluyen una garantía respecto a la calidad de la información que está proveyendo a los terceros confiables.

Una *garantía implícita* es una promesa no dicha ni escrita que surge de la naturaleza misma de la transacción y del entendimiento inherente del recipiente, más que de representaciones expresas del proveedor. Las garantías implícitas se basan en el principio de derecho común de “calidad acorde al precio”. Por eso, una corte podría concluir que los proveedores de identidad hacen garantías implícitas en cuanto a la sensatez de los procesos que utilizan para recopilar y verificar los atributos de información de identidad.

Por último, es importante destacar que algunas leyes de privacidad también regulan la exactitud de la información personal. Por ejemplo, el Artículo 5(1)(d) del Reglamento General de Protección de Datos (RGPD) de la Unión Europea requiere que la información personal mantenida por controladores de datos (como los proveedores de identidad) debe ser “exacta y estar actualizada en caso de que sea necesario” y que “cada paso razonable debe ser tomado para garantizar que toda la información personal inexacta sea eliminada o rectificada sin demora”. Y agrega en el Artículo 16 que “los sujetos de datos deben tener derecho a una rectificación inmediata por parte del controlador de la información personal incorrecta que le incumbe”.

-- Disponibilidad, conservación y eliminación de información de identidad

En el caso de los sistemas de identidad en los que un proveedor de identidad, tercero confiable u otro participante del sistema de identidad conserva información sobre un sujeto de datos, la disponibilidad, conservación y eliminación de dichos datos personales puede estar regulada mediante una variedad de leyes de nivel 1.

La ***ley de privacidad*** (por ej. el RGPD y la Ley de privacidad del consumidor de California (CCPA, por sus siglas en inglés)[13] regula la disponibilidad de los datos personales (y por lo tanto de información de identidad) para el sujeto de datos. Concretamente, estas leyes suelen imponer a los proveedores de identidad el deber de proveer el acceso de los sujetos de datos individuales a los datos que hayan recopilado sobre su persona, así como información sobre el propósito por el cual recopila y procesa dicha información y sobre quién la recibe o las categorías de los recipientes de dicha información.

Asimismo, varias leyes imponen obligaciones a las empresas sobre la ***conservación de datos*** en sus registros corporativos. Estas leyes pueden requerir que tanto los proveedores de identidad como los terceros confiables conserven cierta información de identidad por un tiempo determinado.

Sin embargo, algunas leyes de ***privacidad*** (como el RGPD) pueden imponer límites en la conservación de información personal. Y más aún, las leyes de privacidad (como el RGPD y la CCPA) otorgan el derecho a los sujetos de datos a solicitar que sus datos sean eliminados o borrados.

-- Seguridad de la información de identidad y procesos

Existen muchas ***leyes de seguridad de datos*** y regulaciones que imponen obligaciones a las empresas sobre la seguridad de información personal u otro tipo de información que posean o controlen. Estas leyes de seguridad de datos pueden tener un impacto significativo en las obligaciones y responsabilidades de un participante de un sistema de identidad que esté recopilando, usando, almacenando o transfiriendo información personal. Esto es así sobre todo para los proveedores de identidad y terceros confiables.

Las leyes de seguridad de datos suelen estar incorporadas dentro de leyes de privacidad, pero más allá de la forma, en general imponen dos obligaciones fundamentales: (1) el deber de *proveer una seguridad razonable* para los datos personales y (2) el deber de *notificar las violaciones de la seguridad* de información personal a las personas afectadas y a los reguladores. Aunque no hayan sido promulgadas para abordar específicamente las

[13] "Ley de Privacidad del Consumidor de California de 2018," Título 1.81.5, Artículo 1798.100, Parte 4 del Inciso 3, Estado de California, consultado el 18 de mayo de 2021, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

actividades de los sistemas de identidad, estas leyes se aplican a la información personal utilizada por los sistemas de identidad.

Nivel 2 – Ley general de sistemas de identidad

La aplicación de la ley general existente a los sistemas de identidad no suele funcionar bien, a menudo es ambigua y en muchos casos conduce a resultados inapropiados que son discutibles. Las cosas se complican aún más por el hecho de que las leyes de Nivel 1 que se aplican a los sistemas de seguridad varían a lo largo de las jurisdicciones. Así es que ha habido numerosos intentos por resolver estos problemas.

Algunas jurisdicciones han propuesto y promulgado legislación o regulaciones para regular expresamente todos los sistemas de identidad dentro de su jurisdicción. Sin embargo, aún no hay un consenso sobre la conveniencia o los objetivos de esta legislación genérica y menos aún sobre cómo alcanzarla. Todavía quedan por resolver aspectos clave en cuanto a si esta legislación debe estar diseñada para: (1) simplemente eliminar las trabas legales (reales y percibidas) de los sistemas de identidad, (2) promover y asistir el desarrollo de sistemas de identidad o ayudar a crear la "confianza" y "predictibilidad" necesarias para las partes involucradas en transacciones de identidad en línea, o (3) regular y controlar los sistemas de identidad por ejemplo protegiendo la privacidad de la información personal, garantizando la seguridad y fiabilidad de las transacciones de identidad o imponiendo o limitando la responsabilidad de los proveedores de identidad.

Actualmente existen muy pocas leyes de Nivel 2. Sin embargo, algunos esfuerzos por desarrollar leyes de Nivel 2 que regulen los sistemas de identidad se han llevado a cabo, como, por ejemplo:

Virginia. Con la promulgación de la Legislación sobre la Administración Electrónica de Identidades de Virginia en el año 2015, el estado de Virginia se convirtió en el primer estado de los Estados Unidos en adoptar legislación de identidad de Nivel 2. Esta legislación se enfoca principalmente en la responsabilidad. Para ello, estipula la creación de un Consejo Consultor de Estándares de Administración de Identidades de Virginia cuya tarea consiste en desarrollar estándares de administración de identidades. Los proveedores de identidad y operadores de marcos de confianza que cumplan con los requisitos establecidos en los Estándares de Administración de Identidades están exentos de responsabilidades civiles. En otras palabras, la legislación de Virginia ofrece protección legal en lo que refiere a la responsabilidad de los proveedores de identidad y operadores de marcos de confianza.

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). En la primavera de 2015, el Equipo Especial Legal de Administración de Identidades del Colegio de Abogados de los Estados Unidos junto a un grupo de países de la UE (Austria, Bélgica,

Francia, Italia y Polonia, con el apoyo de la Comisión de la UE), presentaron propuestas de legislación sobre la administración de identidades a la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). Estas propuestas recomendaban que la CNUDMI llevase adelante un proyecto para desarrollar "un marco legal básico que abarque las transacciones de administración de identidades y que incluya las cláusulas apropiadas para facilitar la interoperabilidad internacional transfronteriza." CNUDMI acordó avanzar con ese proyecto.[14]

CNUDMI proporciona un foro internacional capaz de desarrollar un conjunto armonioso de leyes que regulen la administración de identidades y que sea globalmente aceptado. Para promover un abordaje universal a las leyes de administración de identidades, las mismas podrían ser adaptadas a nivel doméstico por cada país individual y extenderse globalmente (para facilitar las transacciones de identidad transfronterizas) mediante un tratado o convención internacional.

En septiembre de 2019, CNUDMI realizó la segunda versión de su borrador de cláusulas sobre el reconocimiento transfronterizo de la IdM y de los servicios de confianza. Los aspectos que tiene en consideración actualmente son:

- Derechos y responsabilidades de los variados roles de un sistema de identidad
- Determinación de las responsabilidades de los sistemas de identidad
- Responsabilidad de los proveedores de identidad
- Reconocimiento legal de credenciales de identidad
- Reconocimiento transfronterizo de credenciales de identidad.

Nivel 3 – Ley específica de sistemas de identidad

Tanto las leyes de Nivel 1 como las de Nivel 2 proveen normas generales aplicables a todos los sistemas de identidad. Sin embargo y como cada sistema de identidad es único, tener un conjunto de reglas detalladas y hechas a medida para regular sus operaciones es necesario.

De hecho, tener reglas predecibles y ejecutables que hayan sido diseñadas para garantizar su correcto funcionamiento y fiabilidad, es clave para cualquier sistema de identidad. Idealmente, las reglas de sistema únicas (por ej., un marco de confianza) proveen la estructura necesaria para regular las operaciones de un sistema de identidad, de la misma forma que las reglas de Visa o MasterCard regulan los sistemas de tarjetas de crédito. Estas reglas incluyen las especificaciones técnicas, las reglas y requisitos operativos necesarios

[14] CNUDMI, "Coloquio sobre gestión de identidad y servicios de confianza," 21-22 de abril de 2016, consultado el 18 de mayo de 2021, https://uncitral.un.org/en/colloquia/electronic_commerce/2016.

para que el sistema sea funcional y confiable, así como las normas jurídicas que definen los derechos y obligaciones legales de las partes y facilitan su ejecución en la medida que sea necesario.

Estas reglas de sistema específicas a cada sistema de identidad son las leyes de Nivel 3 que regulan un sistema de identidad. En el caso de sistemas de identidad del sector privado, estas reglas suelen tomar la forma del llamado "marco de confianza" y son ejecutables a todos los diversos participantes del sistema mediante contrato. Tal y como corresponde, estas reglas deben acatar cualquier restricción existente en las leyes de Nivel 1 y 2.

En el caso de sistemas de identidad del sector público (como un sistema nacional de identificación), estas reglas suelen tomar la forma de legislación o regulaciones adoptadas por el gobierno para regular el sistema. Muchos países, notoriamente Estonia e India, han adoptado leyes para regular sus sistemas nacionales de identificación específicos. A veces, un país establece un sistema de identidad basado en un conjunto de reglas que los participantes voluntariamente aceptan por contrato. El Marco de Identidad Digital Confiable (TDIF, por sus siglas en inglés) de Australia y el programa gubernamental de Reino Unido, *UK Verify*, toman ese camino.

Más allá de si un sistema de identidad es público o privado, los aspectos generales abordados por las reglas de sistema de Nivel 3/marco de confianza suelen ser:

- las especificaciones técnicas que van a regular el sistema
- los derechos y obligaciones de los participantes de cada rol de sistema
- los procesos de registro e inscripción de sujetos de datos
- los requisitos de los procesos de verificación de la identidad
- los requisitos para la emisión de credenciales
- los requisitos de los procesos de autenticación
- las reglas que regulan la confianza de terceros confiables
- los requisitos de seguridad de la información (además de los requisitos de la ley vigente)
- los requisitos de privacidad (además de los requisitos de la ley vigente)
- los requisitos de auditoría, evaluación y certificación
- la adjudicación de riesgo de responsabilidad a cada rol
- los derechos y obligaciones de rescisión
- la resolución de disputas
- la ejecución/cumplimiento de los derechos y obligaciones

Cuando están contempladas en leyes o regulaciones emitidas por un gobierno, estas reglas son vinculantes a todos los participantes del sistema con fuerza de ley. Pero en el caso de un marco de confianza (generalmente usado en sistemas del sector privado), las reglas de

sistema son vinculantes únicamente si los participantes aceptan cumplirlas por contrato. En todos los casos, las leyes de Nivel 3 son reglas de sistema redactadas para un sistema de identidad específico y por lo tanto su aplicación está limitada a ese sistema.

Biografía del autor

Thomas J. Smedinghoff es asesor jurídico en Locke Lord, LLP, y presidente del Equipo Especial Legal de Administración de Identidades del Colegio de Abogados de los Estados Unidos. Puede ser contactado en Tom.Smedinghoff@lockelord.com.

Registro de cambios

Fecha	Cambio
30-06-2021	Actualizaciones editoriales