LA SEGURIDAD DE LA INFORMACIÓN: ALGUNAS CONSIDERACIONES LEGALES

Rodolfo Herrera Bravo
Abogado, Profesor de Derecho Informático, Universidad Central
Master en Informática y Derecho, Universidad Complutense de Madrid
Secretario General, Asociación de Derecho e Informática de Chile

Es un hecho que para algunos los beneficios que se derivan de la utilización de las tecnologías de información les son indiferentes y que otros, incluso, sienten temor y desconfían, todo lo cual ralentiza el aprovechamiento de estos medios y su asunción natural en nuestro quehacer cotidiano. Pero como las confianzas no se obtienen gratuitamente, sino que se ganan, es necesario contribuir a mejorar la percepción individual y colectiva del fenómeno tecnológico, siendo uno de los puntos influyentes para ello aquel que dice relación con la seguridad de la información y de su entorno.

La seguridad de la información descansa sobre cuatro condiciones que deben coexistir: primero, una organización estructurada en pro de la seguridad; segundo, un factor cultural a partir del cual se realicen compromisos serios para garantizar un correcto y prudente comportamiento en el tratamiento de la información; tercero, la adopción y aplicación de medidas tecnológicas de resguardo de los sistemas; y cuarto, un marco jurídico claro y específico sobre materias vinculadas con las tecnologías de información, ámbito sobre el cual están centradas las siguientes consideraciones.

Como punto de partida, es dable mencionar que dentro del ordenamiento jurídico chileno existen algunas leyes específicas sobre materias tecnológicas que deben tenerse en cuenta al momento de analizar el aporte legal a la seguridad de la información, a saber: la ley Nº 19.223, sobre delitos informáticos; la ley Nº 19.628, sobre protección de datos personales; o la ley Nº 19.799, sobre firma electrónica, entre otras. No obstante, cabe advertir que dichos cuerpos legales no contienen regulaciones detalladas sobre seguridad, sino sólo algunas disposiciones muy generales, como el artículo 11, de la ley Nº 19.628 ("El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños"). Por lo tanto, para lograr un cabal conocimiento de la regulación de la seguridad de sistemas no bastan estas normas sino que se requiere buscar los complementos de cada caso en el resto del ordenamiento jurídico.

Una segunda idea fundamental apunta a la perspectiva adoptada para este análisis. Nos parece que el enfoque más apropiado no es el acudir al articulado de una ley puntual, sino más bien obedecer a la finalidad de las medidas jurídicas de seguridad, es decir, a las características de la información que pretenden garantizar, para que a partir de ellas se proceda a buscar normas específicas en el ordenamiento jurídico. Dicho de otro modo, lo que interesa saber es si el legislador resguarda la autenticidad, la integridad, la disponibilidad y la confidencialidad de la información y de qué forma.

En tal sentido, y en lo que se refiere a la autenticidad de la información, ésta implica garantizar el carácter fidedigno tanto de la persona que la proporciona como de su

contenido, característica que hoy enfrenta permanentes amenazas en entornos en línea, como Internet por ejemplo. La razón es simple: a diferencia del mundo tangible en donde estamos condicionados a realizar conductas previas para disfrazar nuestra identidad, en el ciberespacio el anonimato es la situación predeterminada, por lo que se requieren dispositivos adicionales para conocer cuál es el sexo de la persona con quien me comunico por Internet, cuál es la edad de la contraparte con quien celebro un contrato electrónico, o incluso, si se trata de una persona o de una máquina. A ello se suman los riesgos a la autenticidad del contenido de la información, puesto que la facilidad para comunicar datos no impide que, por ejemplo, circulen libremente ofertas fraudulentas que inundan nuestras casillas de correo electrónico, a través de la práctica conocida como *spam* o envío de correos comerciales no solicitados.

Por su parte, la integridad de la información obedece a la cualidad de que sea alterada o eliminada sólo por los usuarios autorizados. Al respecto, la documentación electrónica ofrece una vulnerabilidad evidente en cuanto a su inestabilidad, porque al ser posible modificar estos documentos fácilmente y, sobre todo, por la dificultad para advertir este hecho, se vuelven potenciales objetos de falsificaciones o fraudes, sin que puedan constituirse *per se*, en plenas pruebas de los hechos que dan cuenta, requiriendo entonces de la adopción previa de medidas concretas de seguridad.

A su turno, la disponibilidad consiste en que los usuarios autorizados puedan acceder a la información oportunamente, atendido que su conocimiento extemporáneo equivale, desde el punto de vista de los eventuales perjuicios sufridos, a carecer de ella. Además, los riesgos a que se ve expuesta esta característica pueden ser diversos, aunque por mencionar sólo un ejemplo, destacan los ataques informáticos que tienen por objeto provocar la denegación de servicio de un sistema determinado, generalmente ocasionado por la acción de programas virus que infectan miles de computadores para que efectúen una petición determinada a un mismo servidor en un mismo instante, haciéndolo colapsar.

Por último, la confidencialidad se traduce en que el conocimiento de los datos le corresponda sólo a los usuarios autorizados para ello. Esto no significa que la información sea secreta, sino que el número de personas que tienen derecho a conocerla es variable, en atención al tipo de contenido de que se trata. En tal sentido, la información que encierra decisiones de los órganos de la Administración del Estado es, por regla general, de carácter público, en cambio el *know how* de una empresa cuenta con restricciones al conocimiento de terceros, sobre todo, ante acciones de espionaje.

Ahora bien, ¿qué aportes ha hecho la ley a favor de estas características de la información? Sólo por mencionar algunos ejemplos, merece la pena destacar que, en cuanto a la autenticidad de la información se ha reconocido en la ley Nº 19.799 la equivalencia funcional de dispositivos técnicos creados con el objeto de identificarnos en nuestras comunicaciones electrónicas. Así, la ley ha homologado las firmas electrónicas, esto es, cualquier sonido, símbolo o proceso electrónico creado para identificar a lo menos formalmente al autor de un documento electrónico, con los efectos de una firma manuscrita.

Con relación a la integridad, la ley Nº 19.223 ha tipificado como delito la alteración maliciosa de los datos contenidos en un sistema de tratamiento de información, sancionándolo con una pena de hasta 3 años de presidio, ilícito que se configura, por ejemplo, a través de distintas técnicas de manipulación de la entrada de datos, el borrado de datos verdaderos, transformaciones o desfiguraciones de éstos, y en general mediante toda conducta que implique cambiar la información sin destruirla, careciendo de autorización para ello.

En cuanto a la disponibilidad, la ley Nº 19.628 establece dos vías para garantizarla cuando se trata de datos de carácter personal: por un lado, el reconocimiento del derecho de los titulares de datos personales a exigir información sobre sus datos contenidos en registros de otros, a que sean corregidos cuando no corresponden a la realidad, a que se les actualice o, incluso, a que sean eliminados cuando el tratamiento ha perdido fundamento legal; y por el otro, la correlativa obligación impuesta a los responsables de los bancos de datos de velar por lo anterior, de oficio, es decir, sin necesidad de esperar una petición expresa del titular de datos.

Por último, esta misma ley ha querido proteger la privacidad de las personas al disponer indirectamente la confidencialidad de los datos personales sensibles, atendido que su tratamiento exige la concurrencia de alguno de los dos presupuestos legales que indica para ser legítimo: que el titular haya consentido por escrito el tratamiento o que la ley autorice expresamente al responsable del banco de datos para efectuarlo, no obstante que los datos estén referidos a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad. Sin embargo, cabe precisar que la ley no ha dado un carácter secreto a los datos nominativos *per se*, incluso si son de naturaleza sensible, sino que ha impuesto restricciones adicionales a su tratamiento.

En consecuencia, de conformidad con lo expuesto precedentemente se aprecia que la ley ha sentado algunas bases a partir de las cuales el entorno tecnológico puede ofrecer un nivel de confianza mayor para los usuarios. Sin embargo, el marco jurídico requiere ampliaciones y mejoras, sobre todo en relación con la protección de la privacidad en el tratamiento de datos personales y respecto del vacío existente en materia de contratación electrónica. Igualmente, es necesario dictar disposiciones que permitan instrumentalizar los principios generales de seguridad contenidos en ciertas disposiciones legales y que establezcan sanciones por el sólo hecho de no disponer medidas de seguridad, y no únicamente acudir al régimen general de indemnización de perjuicios por los daños causados, como ocurre en la actualidad. Tal vez con estas medidas básicas sea posible incrementar la percepción de seguridad en las personas, en lo que se refiere al entorno en el cual se desarrollan las relaciones interpersonales en línea.