La ley y la seguridad de la información: una perspectiva regional

Carlos S. Álvarez C.

Cuando en 2003 abordé por primera vez la relación entre la seguridad de la información y la ley y escribí sobre ella intentando analizar desde una perspectiva práctica las implicaciones y las necesidades legales y contractuales generadas por la adopción de una política estandarizada de seguridad, planteé algunas premisas que vale la pena volver a analizar, vistas varios años después y desde la realidad en la que hoy nos encontramos. *"La seguridad de la información ha sido asumida como un tema primordialmente tecnológico"*, *"los servicios contratados en relación con la seguridad de la información suelen limitarse a la realización de pruebas de penetración"*, *"la legislación penal es realmente pobre y en la práctica del derecho no siempre es fácil encuadrar, o convencer al fiscal o al juez, de que un incidente de seguridad ha sido debidamente encuadrado en un delito"*, *"existe una constante apatía legislativa en la materia"*, expresiones todas que en su momento estaban para mí llenas de verdad pero que hoy pueden o no ser acertadas.

Corriendo el riesgo de la imprecisión me atrevo a presentar una breve radiografía de la situación actual a nivel latinoamericano, teniendo en mente la percepción que de ella tenía hace cuatro años:

- De una rápida observación al mercado de seguridad de la información

encuentro que existe una creciente cantidad de proveedores de productos y servicios que surten una igualmente creciente demanda.

- Parecería que hoy quienes demandan estos productos y servicios son conscientes de la importancia de implementarlos solamente en la medida en la que hayan sido definidos como contramedidas costo efectivas, capaces de disminuir al nivel de riesgo residual aquellas amenazas cuya concreción se prevé puede afectar los bienes que deben ser protegidos, de acuerdo a la priorización resultante de la definición de la política de seguridad de la información.

- Tanto a nivel académico como profesional percibo un interés creciente por incrementar los niveles de conocimiento y experiencia en seguridad de la información, en prevención y respuesta a incidentes y en recaudación, administración y presentación de evidencia digital en entornos judiciales. Interés este, valga aclarar, demostrado solamente por algunos expertos en sistemas y uno que otro abogado, no por los sectores público y privado en general.

- Percibo también un creciente interés, por parte de algunos organismos estatales de la región, por elevar los niveles de seguridad de la información en nuestros países; sobra decir que esta percepción es solamente relativa a algunas dependencias en el Ejecutivo y a algunas fuerzas de seguridad estatal, tanto militares como policiales, y sólo en algunos países.

“Corriendo el riesgo de la imprecisión me atrevo a presentar una breve radiografía de la situación actual a nivel latinoamericano, teniendo en mente la percepción que de ella tenía hace cuatro años”.

- Los congresos en determinados países latinoamericanos han promulgado leyes en la materia.

Algunas de estas impresiones mías pueden parecer muy positivas para quien las lea en forma desprevenida; sin embargo, puedo también plantearlas desde la perspectiva que en realidad me interesa, para efectos del presente artículo, así:

- Sí, es cierto que hoy existen numerosas empresas que ofrecen produc-

tos y servicios en seguridad de la información; sin embargo, es imposible afirmar que todas ellas (i) cuentan en sus nóminas con expertos realmente expertos en los servicios que ofrecen – ingenieros que además de haber sido certificados por un par de cursos tengan conocimientos profundos a nivel teórico en sus áreas – y (ii) están en capacidad real de responder tanto patrimonial como legalmente ante un incumplimiento suyo de una obligación adquirida frente a un cliente.

- Sí, es cierto que hoy muchas empresas quieren adquirir herramientas de seguridad de la información e incluso contratar servicios de seguridad, pero es imposible afirmar siquiera que (i) al comprar programas de software de seguridad o elementos de hardware, por ejemplo, los configuren adecuadamente, (ii) entiendan el tan frecuentemente inentendible lenguaje en el que les es presentado el extenso reporte final del consultor y (iii) estén dispuestas a invertir las sumas usualmente astronómicas, para sus bolsillos, correspondientes a las contramedidas definidas en su reciente política de seguridad.

- Sí, es cierto que hoy muchos ingenieros y abogados se interesan por este tema; pero es imposible afirmar (i) que su nivel de preparación y experiencia sea acorde con el interés que el tema despierta en ellos, (ii) lamentablemente, que nuestras universidades en América Latina les den el nivel de preparación que requieren para, v. g., responder a un incidente de la mayor gravedad en tiempo real, o casi real, evitando se consume el daño o se pierda la validez judicial de la prueba y (iii) que en cantidad suficiente lleguen a ocupar posiciones influyentes en las ramas judiciales o en un gobierno, desde las que contribuyan efectivamente a uniformizar leyes y procedimientos, tan necesarios en esta área.

- Sí, es cierto que cada día hay más agencias estatales interesadas en la seguridad de la información; sin embargo, es imposible afirmar que (i) ese interés corresponda a políticas estatales realmente fundadas y de proyección a largo plazo – más que a intereses particulares de los funcionarios de turno – , (ii) ese interés implique la disponibilidad de los recursos necesarios para la toma de decisiones acertadas y a tiempo y (iii) los países de la región hayan entendido que el delito informático es por esencia transfronterizo y, como tal, trabajen todos juntos en la implementación y aplicación de leyes y procedimientos legales estandarizados o uniformizados.

Sobra decir que los esfuerzos y adelantos alcanzados, en todas las áreas que tocan con la seguridad de la información, son plausibles; sin embargo es necesario llamar la atención de la comunidad de expertos sobre algunos puntos estructurales que me atrevo a proponer como puntos mínimos de acuerdo regional, sobre los que en todos los países tanto el sector privado como el estatal deben trabajar. Estos puntos mínimos parten necesariamente desde la definición de leyes y reglamentaciones estandarizadas, es decir, similares en todos los países, que nos den a todos la misma base jurídica sobre la que podamos trabajar.

No tiene sentido que en un país de la región se defina que una conducta es delito, mientras que en otro país tal conducta es ignorada por el legislativo; no tiene sentido que en un país se regule sobre procedimientos forenses digitales mientras que en otro no se haga. Y, lógicamente, no tiene sentido que las legislaciones latinoamericanas desatiendan los adelantos alcanzados en otras latitudes, que frente a nosotros son bastante más adelantadas en estos temas.

La estandarización de las leyes lógicamente no tiene que ver con los estándares internacionales bien conocidos en el medio, v. g. las normas ISO o los estándares británicos, que pueden o no ser adoptados por las entidades, públicas o privadas. Está relacionada con definir, tal y como propone el Convenio de Cíber Seguridad del Consejo de Europa, y según ya mencioné, puntos mínimos:

- Las definiciones incorporadas en las leyes; es decir, si en un país se define legalmente que un dato es "X" mientras que en otro se define que en realidad es "Y", la definición de acuerdos bilaterales de cooperación judicial e investigativa va a ser particularmente difícil. Todos los países deben definir legalmente en forma similar los términos usados en la jerga de las tecnologías de la información y las comunicaciones (en el escenario ideal debería proponer la no definición legal de conceptos, pero a veces es una necesidad tanto de política legislativa como de coherencia dentro del marco general de la ley nacional).

- La definición de bienes jurídicos y la tipificación penal de las conductas: los países que han suscrito el Convenio europeo se han obligado a legislar, en cuanto al derecho penal material se refiere, definiendo la imposición de sanciones para quienes incurran en conductas que (i) atenten contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos, (ii) constituyan en sí mismas infracciones informáti-

cas, (iii) sean relativas a su contenido o (iv) atenten contra los derechos de propiedad intelectual o sus derechos afines. Ojalá nuestros países, al legislar en materia penal informática, lo hagan teniendo en cuenta que casi la mitad del mundo, y justamente la correspondiente a los países desarrollados, ha ya definido los bienes que deben ser protegidos y las conductas que deben ser sancionadas; sin demeritar el trabajo de los legisladores de nuestros países, a veces los intereses que defienden, de sectores particulares o simplemente locales, los llevan a promulgar leyes realmente inconvenientes y técnicamente mal redactadas que nos trasladan de un escenario de ausencia de leyes a uno en el que existen leyes inaplicables o cuya existencia no se puede aceptar.

- Frente a la responsabilidad civil es fundamental, igualmente, que los países definan en forma similar los eventos en los que sea aplicable; v. g., si en un país se define legalmente que la víctima "A" puede cobrar a "B" los perjuicios económicos que le fueron causados con motivo de un ataque que recibió su red, siendo "B" el dueño del servidor desde el que el ataque fue dirigido, que era controlado remotamente por el verdadero atacante gracias a una mala configuración de seguridad, no tiene sentido alguno que en otro país no se legisle sobre este aspecto, si es necesario, o que, no siéndolo, la jurisprudencia vaya en sentido opuesto eximiendo a "B" de la obligación de indemnizar los daños causados por su negligencia en la administración de sus bienes informáticos. Los ataques en línea suelen cruzar fronteras y, lógicamente, es deseable que los responsables, por falta de diligencia o por evidente negligencia, paguen los daños que su acción o su omisión haya podido generar, sin importar el país en el que se encuentren la víctima del perjuicio y quien sea civilmente responsable de su causación.

- En cuanto a la evidencia digital, es decir, en relación con su recaudación, administración y presentación, buscando que nunca pierda fuerza probatoria y sea siempre aceptable en un proceso judicial, nuestros países deben necesariamente prestar atención al menos a dos aspectos y regularlos de manera que las pruebas digitales recaudadas en un país sean judicialmente aceptables en cualquiera otro: (i) el procedimiento forense digital como tal, es decir, el paso a paso que debe seguir el investigador desde el momento en el que llega a la máquina comprometida hasta que presenta la evidencia al funcionario competente; y, (ii) los requerimientos que deben cumplir las herramientas de cómputo forense que use el investigador al

recaudar las pruebas. Así siempre los investigadores forenses digitales, privados o estatales, trabajarán sobre la base de mínimos regulados comunes en todos los países y su trabajo no será perdido al aportar sus descubrimientos en una jurisdicción distinta de la suya.

- En cuanto a la cooperación judicial internacional, los países deben definir herramientas que permitan, por ejemplo y trayendo a colación algunas previsiones del Convenio europeo, obligar internacionalmente a una empresa a guardar datos de tráfico; obligar a esa misma empresa a comunicar tales datos, en forma automática una vez hayan sido almacenados, a una autoridad extranjera; y, permitir a una autoridad policial extranjera el acceso directo en tiempo real, o casi real, a datos de tráfico. Las velocidades de comisión de estos delitos, siendo tan apabullantes como suelen ser, no permiten a las autoridades seguir los causes procesales tradicionales, es decir, sería absolutamente torpe pretender que en una investigación internacional de hacking, el investigador judicial deba oficiar a la Oficina de Relaciones Internacionales de su entidad, para que ella a su vez oficie a la Cancillería de su país, para que ella oficie a la embajada o al consulado correspondiente, para que a su vez oficie a la autoridad policial o judicial internacional, aclarando que de vuelta debe seguirse la misma ruta.

Lo que he podido encontrar hasta la fecha es que los gobiernos de la región, junto con los congresos de nuestros países, han sido completamente indiferentes frente a estos asuntos. Definitivamente no he podido descubrir la decisión política que es razonablemente esperable en la materia.

Soy consciente de que este artículo es particularmente dirigido a ingenieros de sistemas, si bien podrá ser leído por algún abogado, investigador o funcionario público; y, tal vez por esa misma razón quiero resaltar la idea que está detrás de este texto: mientras que no existan leyes sólidas y estandarizadas en la región, que definan los puntos a los que me he referido ya, los esfuerzos en seguridad de la información pueden ser casi simples saludos a la bandera. Y afirmo esto por cuanto tengo la convicción de que, puesto que el riesgo cero no existe, siempre podrá tener lugar un incidente serio que comprometa los bienes o la responsabilidad de cualquier persona, sea natural o jurídica (sobra mencionar (i) las limitaciones de recursos de los usuarios de bienes informáticos, que les impiden implementar políticas y arquitecturas de seguridad tan

sólidas como deberían ser y (ii) las *0day vulns* que, siendo de tan frecuente aparición, abren espacios de tiempo más o menos largos en los que lo único que respecto de ellas conoce el público en todo el mundo es la forma de explotarlas y sacar provecho de miles de potenciales inermes víctimas).

Si hoy una empresa que haya definido e implementado una política de seguridad es atacada y decide proceder judicialmente contra el causante de sus perjuicios, tendrá que enfrentar la falta de las herramientas más elementales que le permitan en realidad obtener la reparación de los daños correspondientes. Es decir, no podrán por ahora, ni ella ni la sociedad en general, mandar a los delincuentes informáticos el mensaje de que las conductas en línea que consideramos inapropiadas son realmente perseguidas y sancionadas; debemos lamentablemente reconocer que hoy, en nuestra materia, enfrentamos una impunidad que tiende al 100% de los casos.

Esperemos, como ya tantas veces he escrito y expresado ante algunos auditorios, que no sea necesario esperar a la concreción de un ataque serio contra la infraestructura crítica de nuestros países que comprometa la vida y la integridad de miles de ciudadanos, o el orden y la estabilidad del Estado, o la administración de justicia, para que nuestros gobernantes y legisladores tomen conciencia acerca de la importancia de legislar y lo hagan, además, de manera uniforme. No basta con crear grupos de trabajo en la materia, nacionales o internacionales e incluso con la participación de unidades policiales y de algunos geeks del sector privado; si esos grupos no cuentan con el decidido apoyo de los niveles políticos del Estado y directivo de sus entidades, y con el respaldo legal necesario para actuar, terminarán dedicándose solamente a dictar capacitaciones y publicar bonitos y coloridos folletos sobre la materia.

Carlos Álvarez C. *Gerente de Asuntos Legales para la Región Andina en Sony BMG Music Entertainment - Day One Entertainment; sus artículos se han publicado en Colombia, Venezuela, Argentina y España. Ha sido instructor, y ha dictado charlas en el país y el exterior, por invitación de fuerzas de seguridad nacionales e internacionales, universidades y otras organizaciones. Miembro observador del WHOIS Working Group, establecido por la GNSO de ICANN, miembro de la Subcomisión de Comercio Electrónico del Comité Nacional Colombiano de la Cámara Internacional de Comercio, y miembro del Consejo Asesor de Alfa Redi.*