Ley de Delitos informáticos y su relación con la Ley 20.393, en específico la responsabilidad que tienen las empresas (u organizaciones) en el cumplimiento y resguardo de la información que obtengan por su actividad o giro comercial.

Hassen Kamal Becerra[1]

La ley 21.459 ha incorporado a la ley 20.393 (sobre responsabilidad penal de las personas jurídicas) ciertos delitos informáticos al catálogo (cada vez más amplio) en que pueden estar involucradas las organizaciones, sus directores, gerentes, socios o accionistas. Lo anterior obliga o por lo menos incentiva a estas mismas personas jurídicas a dar un gran paso en tecnología y estrategia, pero sobre todo modernizar sus modelos de prevención de delitos, alertas, controles y revisión de políticas internas a raíz de las nuevas tecnologías que existen hoy en el mundo, porque sabemos que los avances en la ciencia nos han ayudado a progresar en varios ámbitos, sin embargo, también han ayudado a generar mayores porcentajes de fraude.

Ahora bien, en razón del presente artículo nos abocaremos a la responsabilidad que puedan tener las empresas (personas jurídicas en general) en el cumplimiento y resguardo de la información que puedan obtener a raíz de su actividad o giro comercial. En específico los delitos de Receptación[2] y Falsificación informática[3] contemplados en los artículos 6 y 5 de la ley 21.459.

¿Por qué este tipo de delitos?

Las empresas que trabajan con datos pueden ser fácilmente responsables de información que obtengan a raíz de bancos de datos que no tengan una fuente licita y/o desconozcan el origen del mismo. El mejor ejemplo de cómo una empresa podría verse involucrada en este tipo de delito son las que se dedican al giro de cobranza. El principal giro de una empresa de cobranza o recaudación es el cobro de deudas sobre carteras de clientes de otras empresas, la principal vía que tienen este tipo de empresas para lograr el pago de sus mandantes es a través de correos

---

[1] Hassen Kamal Becerra, Abogado de la Universidad Andrés Bello; Magíster en Tributación de la Universidad de Chile. Socio y Director Legal de Grupo de Estudios Tributarios.

[2] Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos. (Art.6).

3 Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos. (Art.5),.

electrónicos o llamadas a los teléfonos personales de los deudores. Claramente la información de los deudores en primera instancia es entregada por los acreedores o clientes de estas empresas, sin perjuicio de aquello, es común que de alguna u otra manera este tipo de empresas consiguen otros correos electrónicos o números de teléfono fuera del alcance del acreedor o de otras personas (familiares, amigos, trabajo entre otros). Aquí es el punto importante para destacar: las empresas podrían verse expuestas a responsabilidades según la fuente u origen de este tipo de información que obtienen para cumplir con su objetivo que es el cobro.

Otro delito al que las empresas podrían verse expuestas es la falsificación informática, en este punto es importante el trato y control que tengan las empresas sobre la información que obtengan de sus clientes, proveedores o terceros, porque la constitución del delito podrá originarse en la manipulación que realice uno o más colaboradores de la misma organización para adulterar, dañar, o suprimir información que puedan tener alojada. Esto puede ocurrir en la manipulación de datos que obtengan los colaboradores de una organización con el fin de beneficiar y/o perjudicar a otras personas en procesos de licitación, contratación, conflictos de interés entre otros aspectos.

¿Cuál es la responsabilidad y qué sanciones existen aparejadas a estos delitos?

Los delitos descritos anteriormente tienen sanciones particulares y especificas respecto de las personas naturales que puedan cometerlos y tienen una base de pena de presidio menor en su grado menor hasta máximo.

La misma ley indica en su artículo 21 que se incorporarán estos delitos al catálogo contemplado en la ley 20.393, por tanto, los Gobiernos Corporativos podrán verse involucrados de manera indirecta en la comisión de estos delitos. Lo anterior resulta del todo relevante, teniendo en consideración que las sanciones que contempla la ley 20.393 van desde multas, inhabilidades de poder celebrar contratos con organismos del Estado hasta la disolución de la Persona Jurídica o penas de presidio efectivo para directores de empresas según la ley 21.595 recientemente promulgada.

El deber de control y supervisión del almacenamiento de datos internos como externos

La responsabilidad de las empresas en el uso de la información hoy en día será de vital importancia para cumplir con sus fines económicos, esto porque, la información que recopilan y

reciben a través de terceras personas son la fuente de su negocio, ya sea para atraer nuevos clientes, ampliar áreas de negocio y/o reforzar sus propias carteras de clientes. Sin embargo, ahora las empresas deberán revisar y controlar el origen de la información que reciban, ya sea a través de sus propios canales de comunicación como también a través de proveedores de información que adquieran.

La receptación de información que pueda resultar ilícita o falsa ahora conlleva un delito donde una empresa podrá verse responsable. Lo cual hace necesario elevar los grados de control y responsabilidad que antiguamente no tenían las empresas al momento de adquirir o recopilar información de terceras personas. La forma en que las empresas tendrán que realizar sus matrices de riesgo, determinar el grado de importancia de cada delito (sobre todo los descritos en el presente artículo) invitarán a desarrollar o implementar medidas de mitigación, control y resguardo para reducir este tipo de conductas en concordancia con lo indicado en el artículo 4 de la ley 20.393. Esto básicamente se traduce en capacitación en las áreas de tecnologías de la información.

A nuestro criterio esto resulta un importante grado de diligencia y cuidado con derechos que antiguamente no eran relevantes, pero hoy resultan ser muy valiosos, como lo son los datos personales que tienen relación con la vida privada de las personas. Lo anterior será crucial con la promulgación de la ley 21.595 (Ley de Delitos Económicos) que contempla una categorización de los delitos y eleva los delitos y responsabilidad de cada empresa a un deber de supervigilancia y control que anteriormente no existía. Sin perjuicio de aquello, será muy importante analizar que se deberá entender como información privada o dato informático para determinar si existe o no la comisión de los delitos hoy tipificados en nuestra legislación.

Por último, la ley 21.459 ya se encuentra en vigencia, por tanto, los Modelos de Prevención de Delitos ya deben contar con este tipo de herramientas, controles y supervisión sobre estas áreas.