EU: Millonaria multa a AT&T por no proteger datos personales

Un sucursal de AT&T en Nueva York.
Foto: AP

MÉXICO, D.F. (apro).- El manejo de perfiles personales por parte de empresas subcontratadas empieza a estar en el radar de las autoridades de protección de esa información, a partir de una reciente resolución de la Comisión Federal de Comunicaciones de Estados Unidos (FCC, por sus siglas en inglés).

Ese órgano aplicó el 8 de abril una multa de 25 millones de dólares a la telefónica AT&T por no garantizar la protección de datos personales de sus clientes administrados en México, Colombia y Filipinas.

Además, le impuso varias medidas para cuidar de manera más adecuada la información de los consumidores frente a vulneraciones de la privacidad de datos personales (*data breaches*).

Se trata del primer caso relacionado con la privacidad que pide concretamente el nombramiento de profesionales certificados en el campo, señal de los futuros requerimientos para quienes recolecten y gestionen datos.

En México “ninguna empresa ha avisado de vulneraciones a usuarios, lo cual es una violación a la ley. Los responsables de tratar datos, por cuenta de empresas, tienen que cumplir con la ley mexicana”, señala a **Apro** Cédric Laurant, fundador de Son Tus Datos, organización dedicada a promover la privacidad.

AT&T incumplió en proteger adecuadamente la confidencialidad de la información de unos 280 mil usuarios, incluyendo nombres, al menos los últimos cuatro dígitos de sus números de Seguridad Social y datos relacionados con las cuentas conocidos como información de la red de clientes (CPNI, por sus siglas inglesas). Dicha protección fue vulnerada en *call centers* que la telefónica contrató en México, Colombia y Filipinas.

El acceso ilegal a los registros del *call center* de la transnacional francesa Teleperformance en Monterrey duró 169 días, entre el 4 de noviembre de 2013 y el 21 de abril de 2014.

Durante ese periodo, tres empleados del call center entraron sin autorización a cuentas de 68 mil 701 consumidores y, a partir de diciembre de 2013, más de 11 mil cuentas mensuales fueron revisadas hasta marzo de 2014.

La decisión de la FCC implica directamente que las empresas deben conocer a cabalidad el manejo de los datos trasladados a terceros, cláusulas de protección e incluso auditorías a los programas de privacidad.

Los quebrantos se refieren a la información personal de 51 mil 422 clientes de la telefónica usada para colocar 290 mil 803 solicitudes de desbloqueo de teléfonos a través del portal de la transnacional.

La investigación de FCC abordó si AT&T notificó inmediatamente a las autoridades sobre las vulneraciones vinculadas con la CPNI de los clientes.

Esa instancia argumentó que el incumplimiento de proteger razonablemente los datos viola el deber estatutario de la compañía bajo la Ley de Comunicaciones de 1934 de cuidar esa información y representa también una práctica injusta e injustificada.

Ese marco legal estipula que los clientes pueden confiar en que los proveedores han tomado medidas apropiadas para garantizar que personas no autorizadas no accedan, revisen o manipulen su información personal.

La FCC ha dejado claro que espera que las empresas de telecomunicaciones como AT&T tomen “cualquier precaución razonable” para proteger los datos de sus clientes y que está comprometida con el cuidado de la información personal de los clientes estadunidenses ante apropiación indebida, vulneración y difusión ilegal.

Basada en Dallas, Texas, AT&T es la segunda proveedora de telefonía inalámbrica en Estados Unidos con casi 117 millones de abonados.

Teleperformance, fundada en 1978, opera más de 12 mil escritorios en 17 instalaciones situadas en el Distrito Federal, Monterrey, Guadalajara, Aguascalientes, Durango, Chihuahua, Hermosillo y Puebla.

Esa corporación, cuyos ingresos rebasaron 2 mil millones de dólares en 2013 y que emplea a 175 mil personas en todo el mundo, ofrece prestación de servicios al cliente, respaldo técnico, *call centers*, cobro de deudas y redes sociales en rubros como finanzas, tecnología, viajes y turismo, telecomunicaciones, transporte y manufactura.

AT&T operaba los sistemas utilizados por los trabajadores del *call center* para acceder a los registros de los clientes y que estaban cubiertos por las medidas de seguridad de la telefónica. Pero esas medidas fallaron en prevenir o detectar a tiempo una vulneración masiva.

AT&T inició el 3 de abril de 2014 la averiguación de la vulneración sufrida ese mismo mes y avisó a la alta dirección un día después. Según la compañía, era evidente que el incidente se relacionaba potencialmente con un gran volumen de acceso a cuentas de clientes.

La telefónica sabía desde el inicio de su indagación que la base de datos que fue revisada contenía información de cobro y otros datos de CPNI.

A pesar de que la FCC indagó durante 2014, el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) anunció apenas el 13 de abril el inicio de la pesquisa por posibles violaciones a Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En este terreno ya existe un antecedente, pues el IFAI penalizó en septiembre último con 3 millones 989 mil 120 pesos a Seguros Banamex como responsable de datos recopilados, y a Revoware con 56 mil 097 pesos, como encargada del manejo de información. Esta última efectúa servicios telemercadeo para la primera.

El caso es mala propaganda para AT&T, que anunció en noviembre pasado la adquisición de Iusacell.

Acceso sin resguardo

En mayo de 2014 la Oficina de Cumplimiento de la FCC empezó la investigación a partir de reportes enviados por la telefónica al Portal de Vulneración de Datos CPNI del organismo.

La corporación informó a la dependencia que había descubierto que tres empleados del *call center* consultaron las cuentas de clientes para obtener datos que podrían ser utilizados para enviar peticiones en línea para desbloquear teléfonos celulares.

Al menos dos empleados sospechosos de haberse involucrado en el acceso no autorizado confesaron que vendieron la información obtenida de las violaciones a un tercero, conocido por ellos como *El Pelón*, en Monterrey.

En diciembre de 2012, un trabajador de AT&T sospechó que un empleado del *call center* estaba entregando información de los consumidores a terceros.

Ese empleado fue despedido por acceder a las cuentas sin dejar anotaciones sobre su propósito. En enero de 2013, AT&T descubrió información de que otro trabajador podría haber realizado también ese tipo de actividades.

El trabajador renunció al *call center* antes de la finalización de la investigación de AT&T, que aún no catalogaba los incidentes de 2012 y 2013 como vulneraciones de CPNI cuando sucedieron, porque la telefónica no concluyó que esas violaciones incluían el uso o difusión de los CPNI. Pero luego de la vulneración de abril de 2014, la empresa revisó los sucesos y los reportó al Servicio Secreto y al Buró Federal de Investigaciones en septiembre último.

El 8 de abril de 2014 Teleperformance, en consulta con AT&T, entrevistó a uno de los empleados sospechosos de la vulneración y concluyó que éste tenía una “conducta evasiva” durante la entrevista y, luego de someterlo al polígrafo, lo apartó de sus labores y empezó el proceso de despido.

Sin embargo, no está claro si la empresa procedió penalmente en contra de los trabajadores.

Hacia el 22 de abril, AT&T había recibido los discos duros de las computadoras que pudieron ser utilizadas en la vulneración y procedió a su análisis. AT&T notificó del incidente el 20 de mayo al Servicio Secreto y al FBI. Pero la ley estipula que un proveedor debe reportar una vulneración de CPNI no más allá de siete días hábiles. De hecho, la compañía indicó que había avisado a los clientes afectados el 3 de julio de 2014.

La corporación informó a la Oficina de Cumplimiento que había roto su vínculo laboral con el *call center* el 28 de septiembre. En marzo último, la telefónica reveló a la dependencia que investigaba potenciales vulneraciones adicionales en Colombia y Filipinas.

Dentro del acuerdo con la FCC, AT&T convino en elaborar y aplicar un plan de cumplimiento diseñado para asegurar un apego futuro a la Ley de Comunicaciones.

Ese plan incluye una evaluación de riesgo para identificar amenazas internas de acceso no autorizado, uso o difusión de información personal y CPNI.

Además, la compañía debe crear y mantener un programa de seguridad de información diseñado para proteger datos personales y CPNI de acceso no autorizado, uso o difusión.

“El IFAI debe emitir lineamientos de vulneración de privacidad”, como el ocurrido con AT&T, planteó Laurant.

Ante varias violaciones serias ocurridas en 2014, el Comité sobre Energía y Comercio de la Cámara de Representantes

aprobó la Ley de Seguridad de Datos y Notificación de Vulneraciones, que estipula que las empresas deben reportar esos quebrantos en los siguientes 30 días de ocurrida la invasión, y que está a la espera de que el pleno del Congreso la apruebe.