VARAPALO DE LA AEPD AL SECTOR DE LAS 'TELECO': 5,8 MILLONES DE MULTA A VODAFONE, MOVISTAR, ORANGE, MÁSMOVIL Y SIMYO

3 de febrero de 2022

La primera gran multa del año de la Agencia Española de Protección de Datos (AEPD) ha sido colectiva. El sector de las telecomunicaciones y sus principales operadores han recibido un severo correctivo del regulador **por no proteger adecuadamente las tarjetas SIM de los clientes**, y que los estafadores duplican con asiduidad. Un fuerte varapalo de la AEPD.

Vodafone ha sido sancionada con 3.940.000; MoviStar con 900.000 euros; Orange con 700.000 euros; Másmovil con 200.000 euros y Simyo con 70.000 euros. Sumado todo, 5.810.000 de euros.

De esta forma, quedan resueltos **procedimientos sancionadores abiertos en 2019** a petición de distintos particulares que interpusieron su reclamación ante Protección de Datos.

Es la primera vez que la AEPD multa de forma colectiva a las principales empresas del sector, según ha podido saber Confilegal. En el caso de **Vodafone**, en la página 83 de la resolución, se citan todas las **multas anteriores de este operador en materia privacidad**, una reincidencia que podría haber disparado la multa a casi cuatro millones de euros.

Curiosamente, las multas llegan cuando el propio regulador y las empresas del sector habían constituido un grupo de trabajo para abordar la problemática en materia de protección de datos. Eso ha hecho que la notificación de esas multas hayan caído como un jarro de agua fría.

Leandro Núñez, socio del despacho Audens y experto en privacidad, cree que el motivo de la sanción es claro, "cada vez se están produciendo más casos de SIM 'swapping', esta **es una estafa que supone duplicar la tarjeta del móvil** para así tener las claves del banco del estafado y hacer operaciones en su nombre. Es operativa cada vez es más común".

A juicio de este jurista, "la AEPD quiere frenar esta práctica irregular pero creemos que de forma equivocada. No parece que sea esta la forma de hacerlo. No es tanto buscar culpables en los operadores de telecomunicaciones, **no son ellos responsables de estas estafas**, el responsable es el banco que debería garantizar que nadie acceda a esas cuentas bancarias".

En cada una de las extensas resoluciones que se han dado a conocer, "la AEPD interpreta que se ha producido una ruptura de la confidencialidad de los datos personales de los usuarios".

"Esa ruptura viene avalada porque considera que **la tarjeta SIM es un dato personal** y al darle un duplicado a ese tercero, entiende que se vulnera la confidencialidad de esos datos".

Obligación de resultados

Este experto destaca que "las sanciones se imponen con la independencia de que las empresas de telecomunicación tengan procedimientos de seguridad para que eso no ocurra».

Al parecer esas medidas las vulneran los delincuentes falsificando el DNI y haciéndose pasar el dueño de la tarjeta. De hecho, la operativa que siguen los delincuentes es la de **engañar a los operadores de telecomunicación haciéndose pasar por el titular de la línea**.

Ese engaño se consuma, tanto por teléfono llamando al servicio de atención al cliente señalando que les han robado el móvil y necesitan un duplicado de la tarjeta. Así les dan una dirección para que se les envíe. Sin embargo, **esta práctica está cada vez más en desuso.**

La práctica más habitual es ir a las tiendas físicas de los operadores, allí presentan una denuncia policial de que han sido objeto de un robo y que ahí tenían la cartera, DNI, móvil, etc. Van con una fotocopia del DNI con la foto cambiada donde aparece el estafador. Así consiguen el duplicado de la tarjeta.

En las cinco resoluciones de Protección de Datos consultadas por Confilegal se señala que los procedimientos de seguridad eran insuficientes para frenar estas malas prácticas, "**la cuestión es que no dice qué medidas habría que implementar** para frenar esta supuesta malas práxis", aclara este jurista.

Núñez recuerda que todas estas resoluciones tienen un contexto temporal adecuado, "son casos ocurridos en el 2019, donde el SIM 'swapping' no existía, empezó a ocurrir ese año tras aplicarse la Directiva comunitaria PSD2 de medios de pago, la que obligó a los bancos a realizar un doble factor de autentificación con el envío de SMS".

A raíz de esta Directiva, y del consiguiente uso masivo de SMS, fue cuando los delincuentes empezaron a duplicar las SIM, "**los operadores de telecomunicación se encontraron con una operativa que puso en marcha la banca**, sin haber sido consultados. Con el tiempo han podido reforzar sus medidas de seguridad en estas prácticas, aunque para la AEPD, visto los resultados son insuficientes".

"Lo que hace la AEPD es sancionar estas prácticas. Viene a decir que esas medidas son insuficientes porque se produjo SIM 'swapping'. Reclama a los operadores que tengan unas medidas de seguridad idóneas para que no se produzcan fugas de datos".

En estas resoluciones, los dos grandes temas que son cuestionables para este jurista es que Protección de Datos "**está obligando a las empresas de telecomunicaciones a tener unas medidas de seguridad casi infalibles** y al

mismo tiempo señala que este es un tema de protección de datos. En mi opinión es un problema de secreto de las comunicaciones".

Este jurista explica que "no es tanto una filtración de datos de los operadores de telecomunicaciones a los delincuentes, los delincuentes ya tendrían los datos de las personas porque antes le hicieron un 'phishing'. Aquí lo que se produce **es un acceso a la línea telefónica** y eso, en todo caso, es la vulneración del secreto de las telecomunicaciones y no de la protección de datos. Otro derecho distinto".

En cuanto a las sanciones y su cuantía, Telefónica, Orange y MasmÓvil han tenido una bajada en la sanción inicial. Y es que, Movistar pasó de 2.000.000 a 900.000, MásMovil de 500.000 a 200.000 y a Orange de 1.500.000 a 700.000 euros.

"En cada resolución se indica que cuando se enteraron de la problemática se pusieron a colaborar para reducir el impacto de estas acciones. **En cuanto al tema se activó fueron rápidas y proactivas para reforzar sus medidas de seguridad**".

Cuestión de responsabilidad compartida

Por su parte, **Xavier Ribas**, socio responsable de Ribas & Asociados, cree que estamos ante "una situación originada por el rápido avance de la tecnología y de las técnicas delictivas que se apoyan en ella, mientras la normativa y las medidas defensivas de los usuarios de los responsables del tratamiento van a otra velocidad.

Este experto hace un análisis cronológico de los hechos, donde señala el papel del usuario, el propio banco y por último el operador telefónico que intervienen en estas prácticas de SIM 'swapping'.

Sobre el usuario, este experto indica que "a pesar de los esfuerzos de concienciación **los usuarios de telefonía móvil no se han adaptado a las nuevas formas de engaño** y de ingeniería social que utilizan los ciberdelincuentes".

"Es cierto que son la parte más vulnerable y que merecen protección, excepto en el caso de negligencia reiterada, como el usuario que denunció a Glovo ante la AEPD, y en la instrucción se descubrió que había sigo negligente en las custodia de sus claves".

Ribas recuerda que "el expediente se archivó porque Glovo acreditó que las credenciales del usuario habían quedado expuestas en múltiples brechas de seguridad, y a pesar de ello no había cambiado las claves. Así se pudo comprobar en la base de datos".

También aclara que "en el caso de la **duplicación de tarjetas SIM**, los delincuentes pudieron acceder a la cuenta bancaria e iniciar la transacción gracias a principal vulnerabilidad del usuario, que es su cibercandidez".

Sobre la entidad bancaria, Ribas recuerda que "una vez obtenido los datos, los delincuentes acceden a la cuenta bancaria e inician el intento de transferencia, que está sujeto a una autenticación reforzada mediante doble factor".

“Aunque la verificación mediante SMS está dentro de los parámetros actuales de la normativa bancaria, lo cierto es que **esta medida está quedando obsoleta y se está sustituyendo por aplicaciones de autentificación más robustas**”, comenta.

A su juicio, “el sector financiero deberá valorar la necesidad de sustituir los mensajes SMS por otros sistemas de autenticación más robustos”.

En cuanto al operador telefónico señala que “podemos citar el debate de hace unos días en el Tribunal Supremo sobre la seguridad y las dos tesis antagónicas que planteas, si es una obligación de medios o una obligación de resultado”.

Ribas recuerda que “también hay que tener en cuenta que la AEPD ha sancionado a empresas que requerían el DNI para el ejercicio del derecho de acceso. En este caso de la duplicación de la tarjeta SIM es evidente, **la verificación de la identidad del cliente es una acción proporcionada y obligada**”.

“Otra cuestión es el riesgo que supone la delegación de este control en encargados del tratamiento que pueden relajar en algún momento este control o que pueden ser víctimas a su vez de un ataque de **ingeniería social**”, afirma.

Este abogado destaca que “ya que el operador tiene culpa ‘in eligendo’ y culpa ‘in vigilando’, debe reforzarse el proceso de selección y homologación de los encargados del tratamiento y realizar controles al azar, los conocidos como **‘mistery shopping’** en los que un cliente falso intenta engañar al empleado del encargado del tratamiento”.

Como conclusión final señala que “aunque la sanción va dirigida en este caso a los operadores por considerar que no han sido diligentes en este proceso, lo cierto es que **las tres partes implicadas deben realizar un esfuerzo para utilizar la tecnología de forma adecuada** y tener en cuenta que la capacidad de innovación de los ciberdelincuentes siempre va un paso por delante”.

Fuente: www.confilegal.com