G A _ P

Gómez-Acebo & Pombo

El deber de notificar (como brecha de seguridad) un robo de ordenadores

Francisco Pérez Bes

Of counsel

Director del Área de Derecho y Economía Digital de Gómez-Acebo & Pombo

El robo o la pérdida de terminales que contienen información personal de la empresa es un riesgo que hay que gestionar, tanto a nivel preventivo como reactivo. La implantación de medidas técnicas y organizativas es fundamental en estos casos.

El artículo 33 del Reglamento 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (comúnmente conocido como Reglamento General de Protección de Datos o RGPD), introdujo por primera vez la obligación de notificar las violaciones de seguridad de los datos personales cuando concurran una serie de requisitos, «a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y libertades de las personas físicas».

El reglamento define esta figura en su artículo 4, cuando en su apartado 12 afirma que se considera *violación de la seguridad de los datos personales* «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos».

N. de la C.: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

Basándonos en esta definición, el robo o extravío de un terminal de almacenamiento de información personal a través del cual un tercero pudiera acceder inconsentidamente a datos de naturaleza personal puede considerarse —en principio— una brecha de seguridad susceptible de ser notificada al regulador.

En el caso que ahora nos ocupa, una empresa del sector asegurador comunicó a la Agencia Española de Protección de Datos la sustracción de varios equipos portátiles utilizados por empleados de una de sus sucursales. En virtud de la naturaleza del incidente producido, la empresa afectada notificó tal incidente como brecha de seguridad al considerar que el acceso a esos ordenadores permitiría obtener una serie de datos tales como los identificativos, de contacto, de salud y económico-financieros de clientes y empleados[1].

En esta ocasión, el riesgo de acceso era indirecto, puesto que los discos duros de los portátiles no contenían información personal de terceros. Esto es, el sistema de la empresa únicamente permitía ver información de clientes por medio de aplicaciones corporativas accesibles desde el sitio web de la entidad, en el cual sólo se podía entrar con usuario y contraseña.

En relación con este último extremo hay que añadir que la política interna de la empresa incluye la prohibición expresa de copiar o descargar información almacenada en el sistema, salvo autorización expresa, por lo que en ningún caso se deberían haber producido descargas de datos en los equipos de los empleados.

A requerimiento de la Inspección de Datos, la empresa aportó información sobre las medidas adoptadas por la compañía.

En esta ocasión, dado que el origen de la brecha proviene de un robo, cobran especial importancia las medidas de protección física que aplicaban a los terminales titularidad de la empresa, sin perjuicio de otras medidas adicionales que permitirían, de manera remota, bloquear el acceso, como usuarios, de los empleados afectados, así como resetear sus contraseñas.

Y, en cuanto a las acciones emprendidas por la empresa una vez producido el incidente de seguridad, es importante destacar que, desde el punto de vista del cumplimiento normativo, aquéllas deberán consistir en actuaciones que, de manera objetiva, puedan considerarse razonables y diligentes, pues ello permitirá acreditar ante la autoridad competente que tales medidas han sido acordes con la normativa sobre protección de datos.

Entre las posibles medidas (relacionadas con el caso que ahora nos interesa) que a estos efectos pueden implantarse, podemos destacar las siguientes:

— Iniciar, sin dilación, una investigación interna que persiga esclarecer los hechos y denunciar ante las fuerzas y cuerpos de seguridad del Estado el ilícito producido.

[1] Procedimiento núm. E/06442/2019.

— Tomar medidas cautelares, tanto físicas como lógicas, en previsión de un posible riesgo de que se produzca un acceso inconsentido a los sistemas de la empresa. Entre este tipo de medidas podemos destacar la instalación de alarmas, las políticas y protocolos de seguridad internos, así como la evidencia de que, tras acciones formativas, los empleados conocen y respetan los protocolos de seguridad de la información desarrollados por la empresa.

Evidentemente, cada situación va a requerir acciones y medidas diferentes que deberán ser adecuadas al tipo de información tratado, así como al tipo de incidente de seguridad que se produzca. En todo caso, la diligencia mostrada en la previsión y conocimiento de los ciberriesgos a los que se enfrenta la organización debe ser un primer paso, pues permitirá determinar con claridad qué tipo de medidas deben adoptarse en cada situación.

Especial consideración merece lo relativo a la prudencia demostrada por la empresa afectada por la brecha de seguridad a la hora de notificársela al regulador. Y es que, a pesar de la aparente poca relevancia que para la protección de datos pueda tener la sustracción o extravío de elementos de almacenamiento de información tales como USB, discos duros, teléfonos móviles, portátiles, etcétera, es importante valorar la posibilidad de que se vea afectada información personal de terceros, por lo que es importante mostrar un nivel de diligencia equivalente a la potencial gravedad del incidente y a su impacto en la privacidad de los posibles afectados.

Casos como éste nos permiten concluir que todas las empresas no sólo deben implementar y mantener actualizadas medidas técnicas y organizativas, preventivas y reactivas, sino que, llegado el caso de que se produzca un incidente de seguridad, deberemos poder acreditar ante el regulador la efectividad y eficacia de tales medidas.