Expansión | JURÍDICO

Las aplicaciones móviles, un riesgo legal para las empresas

Hasta que se apruebe el reglamento de protección de datos de la UE, los abogados apuestan por que las compañías creen protocolos de seguridad para salvaguardar e impedir el robo de información de sus clientes.

V. Moreno. Madrid

La posibilidad de espiar conversaciones realizadas a través de sistemas de mensajería instantánea como WhatsApp, la apropiación de datos en dispositivos móviles mediante aplicaciones como FourSquare o Instagram y el retraso de la Unión Europea a la hora de aprobar el anteproyecto de reglamento de protección de datos han dejado en evidencia la necesidad de que las empresas opten por crear protocolos de seguridad internos con el fin de protegerse jurídicamente y blindarse ante posibles querellas de clientes frente a una potencia pérdida o robo de datos.

"La mayor parte de las aplicaciones actuales carecen de los niveles de seguridad necesarios para garantizar la tranquilidad de las empresas frente al posible robo de datos de la compañía", explica Eduard Blasi, experto de Marimón Abogados en nuevas tecnologías. Por esa razón, las compañías deben de implementar sus políticas de privacidad y seguridad respecto a los dispositivos móviles ajenos a la empresa.

Dreamstime

Las aplicaciones de mensajería instantánea han mostrado tener muchos problemas de seguridad.

Bloquear el acceso

Según comenta el letrado, sería fácil para cualquier entidad imponer normas respecto a los dispositivos móviles de empresa –*smartphone*, tabletas, ordenadores portátiles–, como imposibilitar la descarga de ciertas aplicaciones, instalar sistemas de seguridad o bloquear el acceso a ciertos sitios web. Sin embargo, todo se complica frente a los teléfonos personales de los trabajadores. "Muchos empleados utilizan sus propios dispositivos para acceder de manera remota a su correo electrónico o se comunican mediante aplicaciones como WhatsApp, y esto puede generar un peligro legal para la empresa, ya que si alguien se apropiara de datos sensibles de algún cliente, la empresa sería la responsable jurídica de esta pérdida y la multa a la que se enfrentaría sería cuantiosa. Por eso, las compañías tienen que crear algún tipo de protocolo o acuerdos con sus trabajadores para limitar los riesgos", añade.

Las compañías son las que custodian los datos de sus clientes y deben protegerlos de su posible robo

Para Blasi, la medida más importante sería bloquear el acceso remoto al sistema de la empresa desde cualquier dispositivo móvil o la necesidad de fijar una autorización previa de la empresa para poder hacerlo. La compañía también podría imponer la obligación de firmar una suerte de contrato formal en el que estuvieran fijadas las normas de seguridad de la empresa o la imposición de instalar un antivirus en el dispositivo móvil para impedir la entrada de *malware* en el servidor de la compañía y el posible robo de datos. "Las empresas deben adoptar estas nuevas medidas, porque son ellas las que tienen que custodiar los datos de sus clientes, que ahora son virtuales y que pueden ser visualizados o utilizados ilícitamente desde esos dispositivos personales".

La normativa de la UE de protección de datos ya no responde a las necesidades de seguridad actuales

Reglamento europeo

Con el objetivo de mejorar la seguridad de las aplicaciones móviles y ampliar la privacidad, la Unión Europea lleva más de dos años trabajando en el anteproyecto de reglamento de protección de datos que, además de introducir conceptos como el derecho al olvido o crear el puesto de responsable de protección de datos en la empresa, incide en regular las fórmulas para prestar consentimiento en el tratamiento de datos –creación de iconos para mejorar la comprensión–, instaura nuevos conceptos como la privacidad por diseño y privacidad por defecto o el derecho de portabilidad de datos.

"La normativa europea anterior es de 1995 y ya no responde a las necesidades de seguridad actuales. Además, hasta ahora cada país ha hecho una transposición libre de la norma, pero este reglamento sería único para el conjunto de los países de la UE y eliminaría las diferentes interpretaciones de una misma ley", comenta el experto de Marimón Abogados.

Sin duda, el concepto que mejorará la seguridad jurídica de los datos personales en *smartphones* y tabletas será la privacidad por defecto y la privacidad por diseño. En el primer caso, se impondrá que los dispositivos móviles y desarrolladores implanten sistemas que garanticen la transparencia y permitan al titular el control de sus datos en todo momento. La privacidad por diseño exigirá el cumplimiento íntegro de la normativa sobre protección de datos en todo proceso productivo y prácticas de negocio, desde el inicio hasta el fin de su ciclo de vida.

Se impondrán multas de hasta un millón de euros a las empresas que no comuniquen brechas de seguridad

Aplicaciones que generan problemas

Entre las aplicaciones móviles que más han dado que hablar se encuentra WhatsApp. Este sistema de mensajería instantánea ha mostrado diferentes problemas en los últimos meses y ha dejado al descubierto muchas conversaciones privadas. De hecho, el Colegio de Abogados de Sabadell, haciéndose eco de un dictamen de la Agencia de Protección de Datos catalana, fue el primero en desaconsejar el uso por parte de los letrados de esta herramienta, ya que la aplicación cuenta con diversos problemas de vulnerabilidades que podrían dejar en evidencia las conversaciones de los abogados con sus clientes. De hecho, y como se ha hecho público, WhatsApp guardaba en una base de datos interna todos los mensajes enviados y recibidos –incluso los borrados– sin cifrar y además añadía información de geolocalización si los mensajes se enviaban con el GPS activado.

Pero esta no es la única que cuenta con problemas de seguridad. La aplicación móvil de Citi Bank para los usuarios de iPhone tuvo que hacer reajustes de seguridad al desvelarse que ésta guardaba datos relacionados con las cuentas de los clientes –contraseñas, número de cuenta– en un archivo oculto del 'smartphone'. Algo semejante ocurrió con la aplicación de Facebook para teléfonos inteligentes. Un problema del sistema móvil de la red social es que no encriptaba las contraseñas de acceso y posibilitaba el robo de información personal de los usuarios.

Más seguridad

El reglamento de protección de datos de la UE introducirá una novedad importante: el deber de comunicar las violaciones de seguridad. El texto del anteproyecto comunitario estipula la exigencia de que se comuniquen los posibles atentados –brecha o violación– contra la seguridad que sufra una empresa. En caso de incumplimiento de esta obligación, la autoridad de control podría imponer una multa de hasta un millón de euros o, si se trata de una gran empresa, de hasta el 2 % de su volumen de negocios anual.

SENTENCIA

Una empresa no puede degradar de puesto a un trabajador sin indemnizarle

Expansión. Madrid

Hay que tener cuidado cuando se asciende a un trabajador, ya que degradarlo puede salirle muy caro a la empresa si luego no está conforme con su trabajo. El Tribunal Superior de Justicia de Asturias ha declarado que un trabajador tiene derecho a recibir una indemnización por despido al rescindir su contrato tras cambiarle a un puesto inferior porque menoscababa su dignidad.

El conflicto se refiere al entrenador de un equipo de natación femenino de alto rendimiento. Sin embargo, el club decidió unilateralmente, dados los problemas que existía con las deportistas, reubicar al trabajador en el puesto de ayudante del entrenador del conjunto masculino, que competía en un nivel inferior.

Finalmente, empresa y trabajador acudieron a un acto de conciliación, aunque no llegaron a un acuerdo. El objetivo del exentrenador era conseguir que le indemnizaran por extinguir su contrato con el club de natación, al igual que ocurriría en el caso de un despido no motivado. En primera instancia, el tribunal se inclinó a favor de la empresa, pero el TSJ de Asturias ha aceptado el argumento del empleado, al considerar que el cambio de puesto "menoscababa su dignidad".

Por un lado, la sentencia reconoce que el cambio de entrenador a ayudante hizo que estuviera "casi sometido" a la autoridad de otra persona, cuando inicialmente no fue contratado para ello. Además, también valora el hecho de que al trabajador se le prohibiera cualquier contacto con las nadadoras con las que trabajaba en primer lugar, ya que considera que el club no debería haber adoptado esta medida, ya que la considera de índole personal y no profesional.

Según el tribunal, el trabajador debe ser indemnizado no sólo porque se haya producido una modificación sustancial en sus condiciones laborales, tal y como exige el Estatuto de los Trabajadores, sino también por la forma de hacerlo, ya que se daña su dignidad al prohibirle el contacto con personas físicas.