Alerta
Informativa ESN:
COVID-19

Perspectiva de Protección de Datos

La Agencia de Protección de Datos advierte que las brechas de seguridad durante el estado de alarma deben seguir notificándose en plazo.

6 de abril de 2020

La Agencia Española de Protección de Datos ("AEPD") ha emitido un comunicado disponiendo que la suspensión de plazos de los procedimientos administrativos establecida en el Real Decreto 463/2020 por el que se declara el estado de alarma ("RD463") no afecta a la obligación de notificar las brechas de seguridad que afecten a datos de carácter personal en el plazo de 72 horas.

Como es sabido, el Reglamento UE 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales establecen, entre otras obligaciones del responsable del tratamiento, la de notificar a la autoridad de control (en España, la AEPD) cualquier violación de seguridad que detecte tan pronto como sea posible y, en cualquier caso, en el plazo máximo de 72 horas (de forma telemática y a través de la sede electrónica de la AEPD). A estos efectos, la Ley entiende por violación de seguridad cualquier incidente que comprometa la confidencialidad, integridad o accesibilidad de los datos tratados.

Por otra parte, la Disposición Adicional Tercera del RD463 decretó la suspensión de términos e interrupción de plazos para tramitar procedimientos ante la administración, añadiendo que el cómputo se reanudaría al finalizar el estado de alarma.

Pudiera haberse concluido, por tanto, que el plazo de 72 horas para notificara la AEPD una brecha de seguridad no resultaba obligatorio durante el estado de alarma, sobre todo en éstas circunstancias en que no sólo es más difícil detectar una violación de seguridad (momento, el de detección, en el que empieza a correr ese plazo de 72 horas); sino investigarla o, incluso, activar los protocolos de notificación (al fin y al cabo, las medidas tomadas durante la crisis han determinado que muchos trabajadores estén de baja, afectados por un ERTE o simplemente permanezcan en su casa afectados por las medidas de confinamiento).

Pero la AEPD discrepa. Y su decisión, al parecer, viene motivada por la multitud de ciberataques realizados con ocasión de la situación de vulnerabilidad generada por esta crisis (como ya adelantamos en nuestras Alertas "Ciberataques vinculados al COVID-19" y "Detectada campaña de envío de SMS en los que se suplanta al SEPE para hacerse con datos bancarios de trabajadores sometidos a ERTEs").

Por ello hace hincapié en la importancia de no bajar ahora la guardia ante esos ciberataques.

La AEPD se justifica en que el estado de alarma no supone una suspensión del derecho fundamental a la protección de datos personales, según ya explicaba en su Comunicado sobre apps y webs de autoevaluación del Coronavirus. Pero a esto podría oponerse que es difícil justificar que tal obligación formal afecte al núcleo del derecho fundamental a la protección de los datos o *habeas data* del artículo 18.4 de nuestra Constitución (véase por ejemplo la STC 254/1993). Y aunque la AEPD recuerde la posibilidad de realizar una notificación escalonada, esta posibilidad en absoluto soluciona las mayores dificultades que los responsables sufren, según se especifica más arriba, en esta situación.

En fin, en absoluto afecta esto a la necesidad de que el responsable, cuando sea probable que la brecha de seguridad entrañe un alto riesgo para los derechos y libertades de los afectados, les comunique también la brecha. Y es que esa otra obligación ni está tan sometida a los formalismos de la notificación a la AEPD (más difíciles de cumplir en estos momentos) ni constituye, al fin y al cabo, un procedimiento administrativo.

Vicente Arias
Socio de TMT
T: +34 91 429 43 33 / **M:** +34 699 096 525
varias@eversheds-sutherland.es

Celia Bouzas
Asociada Senior
T: +34 91 429 43 33 / **M:** +34 683 349 060
cbouzas@eversheds-sutherland.es

Para más información relativa a covid-19 acceda al siguiente link en nuestra página web