Procedimiento Nº: E/02651/2019

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 18/01/2019 se recibe notificación en la Unidad Tecnológica de esta Agencia de una posible brecha de seguridad, relativa a la publicación en prensa de información que un Diputado del Parlamento Andaluz (en lo sucesivo, El Parlamento). Según manifestaciones del DPD del Parlamento, esta notificación se realiza de forma preventiva y en aplicación de los mayores estándares de prudencia, por lo que cabría pues que el acceso fuera lícito o no imputable al Parlamento.

Con fecha de 01/02/2019 se recibe en esta Agencia, justificante de brecha de seguridad en el que El Parlamento manifiesta que tras la realización del análisis oportuno se ha concluido que no se estaba ante una brecha.

Y adjunta:

- Informe del DPD en el que manifiesta, entre otros aspectos, que con fecha 18/01/2019 le fue comunicado la existencia de un posible acceso no autorizado a información obrante en el Registro de la Cámara, continente de datos de carácter personal de un portavoz de un grupo parlamentario.

En concreto, atendiendo a la información dispuesta por los servicios jurídicos de la Cámara en la fecha citada, el mencionado portavoz registró de entrada en el Parlamento de Andalucía un documento dirigido a la Comisión del Estatuto de los Diputados, apareciendo referencias al mismo en una publicación habida al día siguiente en el diario ABC.

Que en cuanto tuvieron noticia de los hechos informaron al interesado, el cual ya conocía lo sucedido ya que registró de entrada en el Parlamento de Andalucía nuevo escrito exponiendo los hechos acaecidos, requiriendo su análisis y, en su caso, la depuración de responsabilidades, y se procedió a realizar una notificación a la autoridad de control en materia de protección de datos, requerida por el artículo 33.1 del RGPD para el supuesto de violaciones de seguridad, aportando cuanta información se disponía en tal momento y empleando para ello los cauces habilitados por la misma. Se solicitó igualmente, análisis de los sistemas al Servicio de informática con la mayor diligencia.
En relación con el interesado, y en consonancia con las conclusiones extraídas, se estima que en el presente supuesto no aplica lo dispuesto en el artículo 34 del RGPD, dado que los hechos sucedidos no parecen tener la consideración de violación de la

seguridad de los datos personales. Se estará por tanto a lo que resuelvan los servicios jurídicos de la Cámara en relación con el régimen de información al interesado.

- Informe del Departamento de Informática que tras analizar el sistema de información para la gestión de la actividad parlamentaria incluyendo registro de entrada y salida (Ágora Plus), los recursos de almacenamiento de datos en red, el correo electrónico corporativo y el agente de seguridad instalado en todos los ordenadores del Parlamento, concluye que no existe evidencia alguna acerca de la existencia de brecha de seguridad en los sistemas y redes del Parlamento de Andalucía.

Con fecha de firma de 01/03/2019, la Directora de esta Agencia insta a la Subdirección General de Inspección de Datos a realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

Se requiere al Parlamento copia del análisis de riesgos del sistema de información para la gestión de la actividad parlamentaria (Ágora Plus) y sistemas de almacenamiento en red, información del número de usuarios con accesos a los referidos sistemas e instrucciones o normas de confidencialidad facilitadas a estos usuarios.

En referencia número de usuarios con acceso a los sistemas de información e instrucciones o normas de confidencialidad facilitadas a estos usuarios, con fecha de 05/04/2019 se recibe en esta Agencia, escrito de alegaciones remitido por el DPD del Parlamento manifestando que existen dados de alta 228 usuarios, distribuidos entre personal al servicio del Parlamento de Andalucía, Diputados, grupos parlamentarios y Secretaría General de Relaciones con el Parlamento; y que el acceso a Ágora Plus únicamente puede realizarse desde la red interna del Parlamento de Andalucía.

Y adjuntan la siguiente documentación:

- Política de Seguridad de la Información que, como aspecto relevante en cuanto al riesgo de los tratamientos, en su punto 7 GESTIÓN DE RIESGOS se indica:

A todos los sistemas sujetos a esta política se les realizará un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos.

Este análisis se repetirá:

o Regularmente, al menos una vez cada legislatura.
o Cuando cambie la información manejada.
o Cuando cambien los servicios prestados.
o Cuando ocurra un incidente grave de seguridad.
o Cuando se reporten vulnerabilidades graves.

- Gestión de la Seguridad del Sistema TIC del Parlamento de Andalucía

- Normas Básicas de Seguridad de la Información de obligado cumplimiento de toda persona con acceso a Datos de Carácter Personales y Sistemas de Información y que recoge, entre otros aspectos, en su punto 2.1 las normas de confidencialidad de información y en su punto 2.5 las responsabilidades del usuario.

- Registro de Actividades de Tratamiento donde se recogen en cada una de las actividades, la descripción, el plazo de conservación de los datos, la licitud del tratamiento, la categoría de los datos personales, el origen de los datos, la comunicación de los datos, las posibles transferencias internacionales en su caso y las medidas de seguridad. En este registro se recoge en los correspondientes apartados de seguridad *"Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica."*

• Con misma fecha de 05/04/2019 se recibe en esta Agencia, escrito adicional de alegaciones remitido por el DPD del Parlamento remitiendo la siguiente información:

- Estatuto de los trabajadores del Parlamento
- Reglamento del Parlamento de Andalucía
- Plan de adecuación al RGPD de fecha de 19 de noviembre de 2018
- Análisis de riesgos: Registro

En este documento se analiza la actividad de tratamiento, la evaluación de impacto, la gestión del riesgo y las escalas para determinar la evaluación de impacto. En este estudio aparecen dos amenazas con nivel máximo de riesgo, 12 sobre 12, que son la fuga de información (muy inusual) y el acceso intencionado por personal no autorizado (ataque interno)

- Análisis de riesgos: Gestión parlamentaria (Ágora Plus)

Al igual que en el caso anterior, en este documento se analiza la actividad de tratamiento, la evaluación de impacto, la gestión del riesgo y las escalas para determinar la evaluación de impacto. Ninguna amenaza dentro de esta actividad de tratamiento supera el nivel 3 de un máximo nivel de riesgo de 12.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 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 (Reglamento general de protección de datos), (en lo sucesivo RGPD) define las quiebras de seguridad de los datos personales como aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Desde el pasado 25/05/2018, la obligación de notificar a la Agencia las brechas o quiebras de seguridad que pudiesen afectar a datos personales es aplicable a cualquier responsable de un tratamiento de datos personales, lo que subraya la importancia de que todas las entidades conozcan cómo gestionarlas.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación.

Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

También hay que señalar, que la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control, determinando lo siguiente:

“1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de

conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

En el presente caso, de la documentación obrante en el expediente en fecha 18/01/2019 fue notificada a la Unidad Tecnológica de esta Agencia la existencia de una posible brecha de seguridad, relacionada con la publicación de información de un diputado autonómico, si bien la comunicación recibida se realizaba de manera preventiva y prudencial.

Posteriormente, se manifestaba que una vez realizados los análisis e investigaciones oportunas se había concluido que no se estaba ante una brecha en sentido estricto, no habiéndose producido accesos no autorizados a la información.

Por otra parte, requerida información acerca de análisis de riesgos del sistema de gestión de la actividad parlamentaria, almacenamiento en red, información del número de usuarios con acceso y de las instrucciones o normas facilitadas sobre

confidencialidad de la información, hay que señalar que el reclamado tenía implementadas medidas adecuadas para garantizar que los datos personales no fueran accesibles por terceros, etc.

III

Por tanto, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

De conformidad con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución al PARLAMENTO DE LA CC.AA. DE ANDALUCIA.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Mar España Martí
Directora de la Agencia Española de Protección de Datos