- **Procedimiento Nº: PS/00144/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y con base en los siguientes

ANTECEDENTES

PRIMERO: Las actuaciones de inspección se inician por la recepción de un escrito de notificación de brecha de seguridad de datos personales remitido por VOX ESPAÑA (en adelante VOX) en el que se notifica a la Agencia Española de Protección de Datos (en adelante AEPD) que, con fecha de 20 de septiembre de 2019, han tenido conocimiento a través del Instituto de Ciberseguridad (en adelante INCIBE) de la publicación en un medio digital de enlaces donde se pone de manifiesto un robo de información de datos de afiliados de VOX.

Al poner VOX en conocimiento del Grupo de Delitos Telemáticos de la Guardia Civil estos hechos, les comunica que, tras haber efectuado investigaciones, la información que figura publicada corresponde a un incidente anterior ya notificado a la AEPD en fecha 13/12/2018, relativo a la publicación de un enlace en el que figuran suscriptores de noticias de VOX en su Web.

En el presente caso, según manifiesta VOX, la segunda brecha de seguridad ahora notificada se refiere al ataque a un equipo informático de VOX asignado a un dirigente de VOX en Barcelona (Sabadell) del que se había sustraído un fichero con datos de afiliados al partido y publicados en la dirección web https://keybase.pub/anoncatalonia/VOX/.

En esta segunda notificación (de fecha 25/09/2019), VOX ha aportado escrito remitido a los afiliados afectados donde se les comunica que uno de los dirigentes de Cataluña (Sabadell) ha sufrido un ataque en el equipo informático que le fue asignado que ha permitido el acceso a un fichero temporal con datos de afiliados de la localidad de Sabadell.

SEGUNDO: A la vista de la citada notificación de quiebra de seguridad de los datos personales, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES
Fecha de notificación de brecha de seguridad de los datos personales: 25 de septiembre de 2019

ENTIDADES INVESTIGADAS
VOX ESPAÑA, con NIF G86867108 y con domicilio en C/ Bambú 12, 28036 Madrid.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN
Respecto de la primera brecha de seguridad de los datos personales (de fecha

13/12/2018) informada a VOX por el INCIBE y relativa a un ataque a la Web de VOX, se abrieron diligencias previas de actuación con referencia E/10207/2018 motivada por la notificación remitida a la AEPD por VOX en la que se ponía de manifiesto un ciberataque del grupo *La Nueve de Anonymous* contra la Web de VOX teniendo como resultado la publicación de un enlace a los suscriptores de noticias.

Respecto de la segunda brecha de seguridad de datos personales (notificada a la AEPD en fecha 25/09/2019) ahora analizada contra un ordenador de VOX asignado a un dirigente relativa al acceso a datos de afiliados en Sabadell:

1. Con fecha 4 de octubre de 2019, desde la Inspección de Datos se accede a la dirección web https://keybase.pub/anoncatalonia/VOX/ obteniendo como resultado "Pagina no encontrada".

VOX ha aportado impresión de pantalla de la información disponible en https://keybase.pub/anoncatalonia/VOX/ en el momento de la comunicación del INCIBE y figura la referencia al fichero *"afiliados_sabadelll.xlsx".*

2. Con fechas 9 de octubre de 2019 y 6 de marzo de 2020 se requiere información a VOX y, de la respuesta recibida en fecha 24 de octubre de 2019 y 17 de marzo de 2020, se desprende lo siguiente:

Respecto de la cronología de los hechos. Medidas de minimización de la incidencia

- Con fecha 21 de septiembre de 2019, el INCIBE comunicó a VOX el acceso por ciberdelincuentes a datos de afiliados de VOX que fueron publicados en el perfil de Anonymus Catalonia (@anonktalonia). En dicho enlace aparecían datos de suscriptores de un ataque previo en el año 2018 (actuaciones de referencia E/10207/2018) y un documento en formato Excel con datos de afiliados al partido en Sabadell.

Se procedió al estudio de dicho fichero Excel comprobando que los datos fueron extraídos del ordenador personal de un dirigente de VOX de Barcelona (Sabadell).

- El 22 de septiembre, el dirigente de VOX en Barcelona interpuso una denuncia ante la Guardia Civil que procedió a bloquear todos los enlaces a la web de VOX. A este respecto VOX ha aportado denuncia ante el Grupo de Delitos Telemáticos de la Guardia Civil de fecha 22 de septiembre de 2019.

- En esta misma fecha se procedió a la comunicación de la brecha de seguridad a los afectados.

Respecto de las causas que hicieron posible la incidencia

- VOX manifiesta que se han vulnerado las medidas de seguridad del ordenador asignado al dirigente de Barcelona, que ha permitido que terceros ajenos pudieran acceder a un fichero temporal que contenía los datos de los afiliados de Sabadell.

- VOX manifiesta que en los documentos que firman los dirigentes del partido

respecto de la confidencialidad y deber de secreto no se permite el mantenimiento de ficheros temporales con datos de afiliados.

A este respecto, Vox ha aportado "*Acuerdo de confidencialidad y secreto profesional. Persona autorizada para el tratamiento de datos"* de fecha 2 de febrero de 2018 firmado por el dirigente cuyo ordenador fue *hackeado.*

Respecto de las medidas de seguridad implantadas con anterioridad al incidente

- VOX ha aportado informe de estado y auditoria de seguridad de sistemas para verificar el cumplimiento de la legislación en materia de protección de datos según la notificación del expediente mencionado y el resultado de la auditoria es de "Cumplimiento". Este informe es de carácter confidencial y se encuentra incorporado al expediente.

TERCERO: Con fecha 16 de junio de 2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD.

CUARTO: Con fecha 2 de octubre de 2020 se formuló propuesta de resolución, en la que se proponía,

<<Que por la Directora de la Agencia Española de Protección de Datos :

- *Se sancione a **VOX ESPAÑA**, con NIF **G86867108**, por infracción del Artículo 32.1, b) en relación con el art 5.1.f) del RGPD, de conformidad con lo dispuesto en el artículo 83.4 del RGPD, considerada infracción grave a efectos de prescripción en el artículo 73.g) de la LOPDGDD, y por infracción del artículo 5.1.f) del RGPD, de conformidad con lo dispuesto en el artículo 83.5 del RGPD, considerada infracción muy grave a efectos de prescripción en el artículo 72.1.i) de la LOPDGDD, con apercibimiento.*

- *Se requiera a **VOX ESPAÑA**, con NIF **G86867108**, que implante en el sistema de información del que es responsable las medidas adecuadas que eviten en el futuro la repetición de hechos similares al analizado en el presente procedimiento.>>*

QUINTO: La entidad investigada no ha presentado alegaciones a la Propuesta de Resolución.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: VOX reconoce y así resulta acreditado que, en fecha 20/09/2019, ha sufrido un ataque externo contra el equipo informático de VOX asignado a un dirigente en Barcelona (Sabadell) del que se había sustraído un fichero con datos de afiliados al partido y posteriormente publicados en la dirección web del atacante https://keybase.pub/anoncatalonia/VOX/.

SEGUNDO: Consta que VOX ha comunicado a los afiliados afectados que uno de los equipos informáticos de los que es responsable ha sufrido un ataque externo que ha permitido el acceso y publicación de los datos de los afiliados al partido en Internet por terceros ajenos.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los arts. 47 y 48.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

Establece el artículo 5 del RGPD lo siguiente:

"1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).”

III

Establece el artículo 4.12 del RGPD 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*.

Establece el artículo 33.1 del RGPD lo siguiente:

“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.”

De las actuaciones practicadas se desprende que VOX informó a esta AEPD dentro de las 72 horas de tener constancia de la brecha de seguridad de los datos personales -según dicción del artículo 30 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas- dando, en consecuencia, cumplimiento a lo establecido en el artículo 33.1 del RGPD

IV

Establece el artículo 32 del RGPD lo siguiente:

.

“1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

1. *Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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." (El subrayado es de la Agencia Española de Protección de Datos).

V

Establece el artículo 28 de la LOPDGDD lo siguiente:

"1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas." (…)

VI

Establecen los Considerandos 51 y 75 del RGPD lo siguiente:

(51) *Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales.*

(75) *Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular (…) en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas,* (…)

De las actuaciones practicadas, se ha verificado que las medidas de seguridad con las que contaba la entidad investigada en relación con los datos que sometía a tratamiento en calidad de responsable, no eran las adecuadas al momento de producirse la quiebra de seguridad de datos personales, con la consecuencia de la exposición pública en internet de los datos personales de afiliados de la localidad de Sabadell. Es decir, los afectados afiliados a VOX de esa localidad se han visto desprovistos del control sobre sus datos personales haciéndose público un determinado posicionamiento o ideología política cuya revelación pública no tiene por qué haber sido consentida por su titular.

Esta posibilidad supone un riesgo que se ha de ponderar a la hora de tratar determinados datos con categoría especial conforme señala el artículo 9 del RGPD, y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la confidencialidad de estos datos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento y en función del mismo establecer las medidas que hubieran impedido la pérdida de control de los datos por parte del responsable del tratamiento y, por tanto, por parte de los titulares de los datos que los proporcionaron a éste.

De las actuaciones practicadas se desprende que VOX, a la fecha de notificación de la brecha de seguridad, no disponía de las medidas de seguridad adecuadas en sus sistemas de información de acuerdo con lo dispuesto en el artículo 32 del RGPD, en relación con el artículo 28 de la LOPDGDD.

VII

Establece el artículo 71 de la LOPDGDD, bajo la rúbrica "*Infracciones*" lo siguiente: *Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.*

Establece el artículo 72 de la LOPDGDD, bajo la rúbrica "infracciones consideradas muy graves" lo siguiente: *"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679".

En el presente caso concurre la circunstancia prevista en el artículo 72.1.a) de la LOPDGDD arriba indicado.

Establece el artículo 73 de la LOPDGDD, bajo la rúbrica "Infracciones consideradas graves" lo siguiente: "*En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

(…)

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679."

En el presente caso concurre la circunstancia prevista en el artículo 73.f) de la LOPDGDD arriba indicado.

VIII

Esta falta de diligencia a la hora de implementar las medidas de seguridad adecuadas en los ordenadores de VOX que asignaba a sus dirigentes constituyen el elemento de la culpabilidad que requiere la imposición de sanción.

Asimismo, la ausencia de consideración del riesgo que puede suponer el acceso no autorizado por terceros a datos de afiliados relacionados con un partido político y su posterior difusión pública agrava el reproche culpabilístico y sancionador de la conducta llevada a cabo por VOX.

IX

Establece el artículo 58.2 del RGPD lo siguiente*:*

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

(…)

Establece el artículo 76 de la LOPDGDD bajo la rúbrica "*Sanciones y medidas correctivas* ", señala lo siguiente:

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

2. *Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679".*

De lo anterior, consta que *VOX* ha infringido el artículo 32.1, b) en relación con el artículo 5.1.f) del RGPD, infracción tipificada en el artículo 83.4 del RGPD, considerada infracción grave a efectos de prescripción en el artículo 73.g) de la LOPDGDD, y el artículo 5.1.f) del RGPD, infracción tipificada en el artículo 83.5 del RGPD, considerada infracción muy grave a efectos de prescripción en el artículo 72.1.a) de la LOPDGDD.

En el presente caso, en atención a la diligencia llevada a cabo por VOX en lo referente a la notificación sin dilación indebida de la brecha de seguridad a esta AEPD, así como la comunicación a los interesados y el inicio de acciones tendentes a minimizar las consecuencias negativas de la citada quiebra de seguridad, se considera conforme a derecho no imponer sanción consistente en multa administrativa y sustituirla por la sanción de apercibimiento de conformidad con lo dispuesto en el artículo 76.3 de la LOPDGDD en relación con el articulo 58.2 b) del RGPD.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO:

1. IMPONER a VOX ESPAÑA, por infracción del Artículo 32.1, b) en relación con el art 5.1.f) del RGPD, de conformidad con lo dispuesto en el artículo 83.4 del RGPD, y por infracción del artículo 5.1.f) del RGPD, de conformidad con lo dispuesto en el artículo 83.5 del RGPD, una sanción de apercibimiento.

2. REQUERIR a VOX ESPAÑA, que implante en el sistema de información del que es responsable las medidas adecuadas que eviten en el futuro la repetición de hechos similares al analizado en el presente procedimiento y comunique a esta Agencia dichas medidas en el plazo de tres meses.

SEGUNDO: NOTIFICAR la presente resolución a ***VOX ESPAÑA,*** con ***NIF G86867108***

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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