- *** Procedimiento Nº: PS/00254/2019**

938-300320

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: En fecha de 13/12/2018 se recibe de un escrito de notificación de quiebra de seguridad remitido por VOX ESPAÑA (en adelante VOX) en el que informan que han tenido conocimiento, a través de las redes sociales, de un ataque informático realizado por el Grupo ******GRUPO.1***, el 12 de diciembre de 2018 a las 19:30 horas, que ha permitido el acceso a la base de datos de suscriptores de noticias de la entidad.

La información accedida corresponde a datos básicos y VOX considera que puede haber unos treinta mil afectados

Al tener conocimiento de los hechos VOX contrató un servicio especializado forense y procedió a aislar la base de datos comprometida.

SEGUNDO: A la vista de la citada comunicación, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación teniendo conocimiento de los siguientes extremos:

1. Con fecha 13 de diciembre de 2018, desde la Inspección de Datos se accede a diversas noticias publicadas en las webs ******URL.1, ***URL.2, ***URL.3*** en las que se pone de manifiesto el ataque realizado por el Grupo ******GRUPO.1*** a los servidores de la página web de VOX y el acceso a datos de unos 30.000 usuarios.

   En las noticias se informa que el grupo ******GRUPO.1*** ha publicado en su cuenta de Twitter (******CUENTA.1***) el ataque a la web de VOX y la información a la que ha tenido acceso, por otra parte, VOX también ha publicado en su cuenta de Twitter (******CUENTA.2***) la existencia del ataque y que ha sido puesto en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado.

2. Con fecha 13 de diciembre de 2018, desde la Inspección de Datos se comprueba la existencia de un “tweet” firmado por ******CUENTA.1*** donde se informa del acceso a 30.000 registros de VOX y se publica una página con los datos de nombre y apellidos parcialmente anonimizados.

3. Con fecha 21 de diciembre de 2018 se requiere información a VOX y de la respuesta recibida con fecha 15 de enero de 2019 se desprende:

3.1 Respecto de la cronología de los hechos

El 12 de diciembre de 2018 a las 19:30 horas, VOX tuvo conocimiento, a través de las redes sociales, de un ataque informático a la web alojada en un servidor externo de la compañía 1&1 Internet España, S.L. (en adelante 1&1) con la que tiene suscrito un contrato de encargado del tratamiento.

El ataque fue realizado por el Grupo ******GRUPO.1*** tal y como se publica en su cuenta de Twitter ******CUENTA.1***

VOX procedió a inhabilitar el equipo atacado y a dar traslado de la incidencia de seguridad a la Agencia Española de Protección de Datos, el 13 de diciembre y a formalizar denuncia ante la Guardia Civil el 14 de diciembre.

VOX contacta con la empresa proveedora de hosting 1&1 y con la entidad S21Sec especializada en seguridad para la investigación del ciberataque.

VOX manifiesta que los datos afectados corresponden a la base de datos de suscriptores a noticias del partido para el envío de newsletter que mantenía 30228 registros.

El 14 de diciembre a las 20:36 se comunicó a todos sus integrantes un mensaje indicando el ataque sufrido a la web.

VOX manifiesta que no tienen conocimiento de la utilización por terceros de los datos sustraídos en el ciberataque.

3.2 Respecto de la categoría de los datos afectados

VOX manifiesta que "*Los datos sustraídos por los piratas son datos del tratamiento de suscriptores a las notificas del partido, no son datos de especial protección, es un tratamiento simplemente informativo general de las actividades y agenda del partido, lo que no supone ni adscripción política ni ideológica* (…) *es simplemente un tratamiento para el envío de una newsletter informativa a interesados"*

En el documento de Registro de *Actividades del Tratamiento,* respecto del tratamiento de datos para el envío de newsletter, figura en el apartado *"Categoría de datos" y* subapartado "*Datos identificativos"* el nombre y apellidos, dirección postal o electrónica y teléfono. Y en el subapartado de "*Datos* sensibles" "*No Existen".*

En el documento de Análisis de Riesgos apartado "*Identificación de los tratamientos de datos personales", respecto del tratamiento para el envío de newsletter, figura como Categoría BASICO.*

3.3 Respecto de las acciones tomadas para minimizar la incidencia

Des habilitación del formulario donde se recaban los datos para los suscriptores a la newsletter.

A este respecto, con fecha 13 de diciembre de 2018, desde la Inspección de Datos se ha accedido a la web de VOX en la dirección ******URL.4*** verificando que en la opción de suscripción figura el mensaje "*Suscripciones en operación de mantenimiento*" sin solicitar ningún dato personal.

Borrar todos los datos de la base de datos atacada.

3.4 Respecto del informe de auditoría sobre la web objeto del ataque

[…]

3.5 Respecto del informe de la incidencia

VOX ha remitido a esta Agencia informe realizado por la empresa S21Sec contratada para analizar las causas que han provocado el incidente de seguridad. De este informe se desprende:

[…]

3.6 Respecto de la resolución final de la incidencia

[…]

TERCERO: Con fecha 25 de septiembre de 2019, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción del artículo 32.1 del RGPD tipificada como infracción grave en el artículo 73 f) de la LOPDGDD y en el Artículo 83.4 del RGPD.

CUARTO: Notificado el citado acuerdo de inicio, el reclamado presentó escrito de alegaciones en el que, en síntesis, manifestaba que:

VOX dispone de un sistema que podemos categorizar como seguro especialmente para el uso al cual se dedica y que el ataque sufrido podría no haber sido detectado hasta su ejecución o publicación en las redes sociales.

S21Sec que ciertamente encontró varias vulnerabilidades, pero no pudo asegurar al cien por cien las herramientas utilizadas por los atacantes, pues los mismos se tratan de terroristas informáticos que utilizan técnicas depuradas.

En función de las recomendaciones de S21Sec enviamos informe a la Agencia de todas las medidas implementadas en nuestro sistema de información para mejorar la seguridad en cuanto a:

[…]

No pueden considerarse datos ideológicos los suscriptores de las newsletter. El criterio mantenido por la AEPD hasta ahora contradice dicha consideración, tal como se pone de manifiesto en los Informes de 24 de enero de 2001, 28 de febrero de 2003, y de 29 de abril de 2008, entre otros. Existe la posibilidad de que las personas que han accedido al formulario de suscripción a noticias pudieran ser meramente gente interesada en las actividades del partido VOX, sin necesidad de imperativamente estar afiliado al mismo, por lo cual podría quedar desvirtuado el que dicho dato reflejara una adscripción ideológica.

En otros procedimientos que versan sobre hechos similares, la AEPD ha procedido al archivo de las actuaciones. En este caso VOX actuó de modo diligente y con total celeridad para aminorar los efectos desfavorables en los derechos de los afectados.

QUINTO: Con fecha 12/12/2019, el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, teniéndose por incorporadas las actuaciones previas de investigación, E/10207/2018, así como las alegaciones y los documentos del investigado.

SEXTO: Con fecha 3 de febrero de 2020, por el Instructor del procedimiento se formuló propuesta de resolución en el sentido de que por la Directora de la Agencia Española de Protección de Datos se sancione a VOX ESPAÑA, con NIF G86867108, con APERCIBIMIENTO por la infracción del artículo 32 del RGPD, tipificada como infracción grave en el artículo 73 f) de la LOPDGDD.

SÉPTIMO: De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

UNO.- Con fecha 13/12/2018, desde la Inspección de Datos se accede a diversas noticias publicadas en las webs ******URL.1, ***URL.2, ***URL.3*** en las que se pone de

manifiesto el ataque realizado por el Grupo ******GRUPO.1*** a los servidores de la página web de VOX y el acceso a datos de unos 30.000 usuarios.

En las noticias se informa que el grupo La Nueve ha publicado en su cuenta de Twitter (******CUENTA.1***) el ataque a la web de VOX y la información a la que ha tenido acceso, por otra parte, VOX también ha publicado en su cuenta de Twitter (******CUENTA.2***) la existencia del ataque y que ha sido puesto en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado.

DOS.- Con fecha 13/12/2018, desde la Inspección de Datos se comprueba la existencia de un "tweet" firmado por ******CUENTA.1*** donde se informa del acceso a 30.000 registros de VOX y se publica una página con los datos de nombre y apellidos parcialmente anonimizados.

TRES.- VOX procedió a inhabilitar el equipo atacado y a dar traslado de la incidencia de seguridad a la AEPD, el 13/12/2018 y a formalizar denuncia ante la Guardia Civil el 14 de diciembre.

CUATRO.- El 14/12/2018 a las 20:36 se comunicó a todos sus integrantes un mensaje indicando el ataque sufrido a la web.

CINCO.- En el Informe de S21Sec que encargó VOX para analizar las causas que han provocado el incidente de seguridad, se indica lo siguiente:

Se ha hecho un análisis básico automatizado de seguridad y se ha encontrado 22 vulnerabilidades en total, siendo 1 de carácter grave y 2 de carácter medio, que han sido remitidas a sus responsables para su corrección.

• Se ha realizado un análisis básico del código fuente de la aplicación del servidor, encontrando varias vulnerabilidades graves confirmadas que deben ser corregidas y que en general tienen que ver con la validación de los parámetros de entrada, y que deben ser corregidas a la mayor brevedad.

• Se han detectado algunas carencias en materia de seguridad que se recogen en el apartado de recomendaciones, y que se consideran particularmente importantes articular cuanto antes, dado que el perfil del servidor se considera de alto riesgo.

Una de las vulnerabilidades que se han dictaminado como grave "podrían permitir a un atacante recuperar usuario y contraseña interceptando una conexión existente".

El informe describe la vulnerabilidad como "la aplicación no comprueba los parámetros de entrada y puede ser utilizada para infectar usuarios y para robo de sesión".

•S21Sec concluye que, aunque no se ha podido asegurar al cien por cien las herramientas utilizadas por los atacantes, consideran que podría haber sido una inyección de SQL vía las vulnerabilidades del sistema y el posible acceso a directorios

del servidor web antiguo en el que se podría haber volcado backups de la web con datos a los que los atacantes tuvieron acceso.

•*S21Sec recomienda una serie de medidas técnicas y realizar un análisis en profundidad de la web ya que considera que va a seguir siendo objetivo de campañas de hackeo y espionaje.*

SEIS.- En fecha de 13/06/2019 VOX aporta un escrito dónde se recogen las medidas adoptadas a raíz del informe de S21Sec.

SIETE.- En fecha de 12/10/2019 VOX presentó dos informes de las entidades HADOQ IT, S.L, y SERVYTEC NETWORKS, S.L., que ponen de manifiesto que se han solucionado las vulnerabilidades detectadas y se ha alcanzado un nivel óptimo de seguridad.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el art. 58.2 del RGPD y en los art. 47 y 48.1 de LOPDGDD.

II

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 Agencia Española de Protección de Datos, al día siguiente de producirse la violación de datos personales, dando cumplimiento a lo establecido en el artículo 33.1 del RGPD.

III

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.

2. 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.)

De las actuaciones practicadas se ha verificado que las medidas de seguridad que contaba la entidad investigada en relación con los datos que sometía a tratamiento, no eran las adecuadas al momento de producirse la violación de datos, pues se hallaron, según el informe aportado (…)*varias vulnerabilidades graves confirmadas que deben ser corregidas y que en general tienen que ver con la validación de los parámetros de entrada, y que deben ser corregidas a la mayor brevedad.(…)*

La consecuencia de esta falta de medidas de seguridad adecuadas fue la exposición pública en internet de los datos personales de suscriptores para la recepción de información relacionada con la actividad del responsable. Es decir, los afectados se han visto desprovistos del control sobre sus datos personales.

IV

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. (…) (*El subrayado es de la Agencia Española de Protección de Datos.)

V

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,* (…)El subrayado es de la Agencia Española de Protección de Datos.

Al contrario de lo que indica VOX en sus alegaciones formuladas al acuerdo de inicio, desde esta Agencia no se está considerando los datos personales objeto de la violación de seguridad, como datos ideológicos que merezcan subsumirse bajo el paraguas del art. 9 del RGPD que bajo la rúbrica "*Categorías especiales de datos", incluye como tales datos personales que revelen* (…), *las opiniones políticas*(…), sino que del tipo de datos que han sido objeto de exposición y del tipo concreto de exposición, esto es, en internet, se pone de manifiesto un determinado riesgo que hay que tener en cuenta, tal como se indica a continuación.

Los datos en cuestión, versan sobre la suscripción a una newsletter de la actividad del partido político, y que, si bien no implica necesariamente datos de

carácter ideológico, la exposición pública a través de internet de esta información, puede dar lugar a la realización de determinadas combinaciones con otras informaciones -*también publicadas en internet o por otras fuente, como comentarios en redes sociales, participación en foros, seguimiento de determinados perfiles de usuario en redes sociales, etc.,* - y situar a sus titulares en un determinado posicionamiento en ese sentido.

Sobre la posibilidad de combinación de informaciones referidas a un titular de datos personales, se puede traer a colación el Dictamen 4/2007 del Grupo de Trabajo del Articulo 29, "*Sobre el concepto de datos personales*" que si bien analiza las posibilidades de identificar a alguien a través de combinaciones con otras informaciones, resultan de gran claridad, cuando nos referimos al riesgo de atribuir una determinada ideología política, partiendo únicamente de los datos de un suscriptor a la información de dicho partido, y combinándola con otra.

En concreto indica lo siguiente: (…)*cuando hablamos de «indirectamente» identificadas o identificables, nos estamos refiriendo en general al fenómeno de las «combinaciones únicas», sean estas pequeñas o grandes. En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser «identificable», porque esa información combinada con otros datos (tanto si responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras. Aquí es donde la Directiva se refiere a «uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social». Algunas de esas características son tan únicas que permiten identificar a una persona sin esfuerzo (el «actual presidente del Gobierno de España»), pero una combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo. Este fenómeno ha sido estudiado ampliamente por los estadísticos, siempre dispuesto a evitar cualquier quebrantamiento de la confidencialidad*(…)*Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones.*(…)

Como se ha indicado anteriormente, en este caso la búsqueda en internet, por ejemplo, del nombre, apellidos o dirección de correo electrónico de alguno de los afectados puede ofrecer resultados que combinándolos con el de la suscripción a recibir noticias sobre la actividad del partido político, es decir, los que han sido objeto de la brecha de seguridad, nos revelen, una determinada ideología política, cuya revelación no tiene por qué haber sido consentida por su titular.

Esta posibilidad supone un riesgo que se ha de valorar a la hora de tratar determinados datos con esta característica y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y 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.

VI

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 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 referido.

VII

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "Principios de la Potestad sancionadora", en el artículo 28 la bajo la rúbrica "Responsabilidad", lo siguiente:

1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa

Respecto del elemento subjetivo en la comisión de la infracción del artículo 32.1 del RGPD, debe tenerse en cuenta que VOX no contaba con las medidas de seguridad adecuadas a fin de evitar la violación de seguridad acontecida, prueba de ello es, en primer lugar, el sentido del primer informe del incidente de seguridad donde se hace constar que se *hallaron varias vulnerabilidades graves confirmadas* que deben ser corregidas y que en general tienen que ver con la validación de los parámetros de entrada, y según se desprende del informe aportado, *deben ser corregidas a la mayor brevedad,* y en segundo lugar, las acciones que se recomiendan que se adopten y las que afirman que se adoptaron en su escrito de 13 de junio de 2019.

Esta falta de diligencia a la hora de implementar las medidas de seguridad adecuadas constituyen el elemento de la culpabilidad que requiere toda imposición de sanción.

En cuanto a las posibles causas que provocó la violación de seguridad, en el informe de la entidad S21Sec se hacía constar lo siguiente: […]

Respecto de los ataques informáticos a través de técnicas como inyección SQL, esta Agencia se ha pronunciado en otras resoluciones, sirva citar a modo de ejemplo la recaída en el Procedimiento Sancionador nº PS/00187/2017, dónde se hacía constar lo siguiente:

(…)*El intruso utilizó una técnica denominada "Inyección de SQL" para conseguir acceso al entorno del sistema Planet Vtech alojado en el servicio Amazon Web Services. La Inyección de SQL es un tipo de ataque conocido al menos desde 2003. Ha estado en la lista[1] de las 10 vulnerabilidades más utilizadas entre los años 2003 y 2011 y ha afectado a centenares de miles[2] de sitios web de todo el mundo a pesar de que su solución es conocida y sencilla de implementar.(…)*

(…)Existen vulnerabilidades asociadas a técnicas de inyección de SQL documentadas desde 2002[3]. Según la clasificación de OWASP14, los ataques basados en este tipo de técnicas han estado entre los 10 más relevantes desde 2004[4]. (…)

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

De lo indicado hasta ahora, se desprende la falta de diligencia de VOX a la hora de implementar medidas de seguridad *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 (art. 32 RGPD),* que da contenido al elemento culpabilístico de la acción típica y antijurídica.

VIII

Establece el artículo 58.2 del RGPD lo siguiente*:*

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

(…)

[1] *http://cwe.mitre.org/top25*

[2] *https://www.netsparker.com/blog/web-security/sql-injection-vulnerability-history*

[3] *https://www.cvedetails.com/vulnerabilities-by-types.php*

[4] *https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project*

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* " 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.

3. 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.

En el presente caso, en atención a la diligencia llevada a cabo por VOX en lo referente a la comunicación sin dilación de la violación de seguridad a esta Agencia Española de Protección de Datos, así como el inicio de acciones tendentes a minimizar las consecuencias negativas de la citada violación de seguridad, y lo indicado en los hechos probados seis y siete de la presente resolución, que ponen de manifiesto que tras el incidente de seguridad y los informes que encargaron a los expertos en seguridad, la entidad ha solucionado las vulnerabilidades detectadas y se ha mejorado el nivel seguridad, se considera conforme a derecho no imponer sanción consistente en multa administrativa y sustituirla por la sanción de apercibimiento de

conformidad con 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: IMPONER a ***VOX ESPAÑA***, con NIF ***G86867108***, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a ***VOX ESPAÑA***.

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