- **Procedimiento Nº: PS/00117/2020**

938-300320

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 una notificación inicial remitida por VTS MEDIA, S.L. en la que informan a esta Agencia sobre la detección de una brecha de seguridad el día 24/10/2019, relacionada con la exposición en Internet de *logs* técnicos (registros de actividad de los servidores), en los que inicialmente no se apreció que hubiera información personal. Indican que posteriormente, en fecha 3/11/2019, aparece en un medio de comunicación la exposición de información personal de usuarios, e investigados en profundidad los *logs* se detecta información personal.

SEGUNDO: A la vista de la citada notificación de brecha de seguridad, 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 la brecha de seguridad: 5 de noviembre de 2019.

ENTIDADES INVESTIGADAS

VTS MEDIA, S.L. (en adelante VTS), con NIF B63546253 y con domicilio en c/ Doctor Trueta 183, Piso 8, Pta. 1, 08021 Barcelona.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

1.- HECHOS

Manifestaciones:

VTS manifiesta en la notificación de la brecha de seguridad que "*con motivo de un fallo en los servidores de logs (basados en Elasticsearch) se contrató un servicio temporal externo entre los días 24 de mayo de 2019 y 25 de octubre de 2019 consistente en tres servidores cloud externos. En estos servidores se instaló un nuevo cloud sin ningún dato histórico, pero el día 5 de septiembre se copiaron los logs generados en este periodo de tiempo a un cluster nuevo que quedó al descubierto por este error en la interpretación de la documentación, en concreto, un funcionamiento inadecuado del firewall lo que permitió la conexión a nuestro Elasticsearch sin necesidad de utilizar credenciales y ver los logs correspondientes".*

Indican en esta notificación inicial que el número de afectados ha sido unos 300.000 con datos básicos, direcciones IP, datos de contacto y DNI de sus usuarios.

En una segunda notificación de ampliación de datos sobre la brecha de seguridad aumentan el número de usuarios afectados a 550.000, e incluyen en la tipología de los datos credenciales de acceso o identificación.

Sobre datos de medios de pago de los clientes indican que solo les llega de su proveedor de pagos parte de la numeración de la tarjeta de crédito de los usuarios. Aportan copia de fichero de *log* donde indican dicha circunstancia.

Aportan también en esta segunda notificación un informe denominado “MEDIDAS DE SEGURIDAD VTSMEDIA” donde reflejan las averiguaciones sobre las posibles causas de la ocurrencia de la brecha en una descripción y cronología de los hechos, el detalle de los datos expuestos y las medidas de seguridad tanto presentes como las implementadas con posterioridad a la brecha de seguridad.

Descripción de los hechos:

- En el informe de “MEDIDAS DE SEGURIDAD VTSMEDIA” aportado por la entidad se realiza una descripción de hechos, indicando que utilizaban un indexador de *logs* “ElasticSearch” para guardar *logs* técnicos y que debido a un fallo en “ElasticSearch” decidieron instalar un nuevo *cluster* (grupo de servidores) en un proveedor de nube “Scaleway”

  Manifiestan que el sistema se instaló siguiendo la documentación oficial, y la protección se realizó utilizando un *firewall* (cortafuegos) para que el acceso solo fuera posible desde las direcciones IP de la entidad.

- Manifiestan también que no fallaron sus procedimientos de implementar la debida seguridad, ya que han conseguido determinar en la investigación interna que las reglas protección que configuran el *firewall* se crearon y aplicaron correctamente (adjuntan una prueba de eGarante, indicando que han seguido la recomendación de la página de la Guardia Civil) en la que indican que se puede ver que las reglas de protección del *firewall* fueron creadas el 27/05/2019.

  Indican que han revisado históricos de fallos en la empresa “Scaleway” y han encontrado reportes de usuarios con problemas similares en el pasado con respecto al *firewall* y el panel del control. El día 29/05/2019 (2 días después) esta empresa reporta una incidencia sobre el funcionamiento de su panel, por una supuesta inestabilidad de la API.

  Manifiestan que han solicitado los *logs* referentes a estas operaciones a la empresa, recibiendo como contestación que han sido borrados y que ya no disponen de esa información.

- Manifiestan que no detectaron esta anomalía ya que podían entrar normalmente desde su red privada. Ninguno de sus técnicos revisó si las reglas de *firewall* se estaban aplicando.

- Aportan también una cronología detallada de los hechos que se resume a continuación:

24-05-2019: A raíz de un fallo en el *cluster* de *Elasticsearch*, que contienen *logs* técnicos internos, se contrataron unos nuevos servidores en un proveedor externo de forma provisional. Se configuraron en el proveedor "*Scaleway.com*" las reglas de *firewall.*

24-10-2019: Miembros del equipo de soporte al usuario reciben un *ticket* (comunicación de incidencia) de una persona externa que dice haber encontrado una vulnerabilidad en la infraestructura de la entidad.
- Atención al cliente le pregunta por más detalles.
- Reciben a las 19:16 (hora local española) la respuesta del investigador donde notifica la IP, Puerto y tipo de instancia (*elasticsearch*) expuesta.
- La persona que atendió el *ticket* sin conocer la gravedad, lo dejó pendiente para poder consultarlo con un técnico que ya no estaba en horario laboral, éste finaliza a las 18:30.

25-10-2019:
- A las 10:00 un técnico revisa los datos aportados en el *ticket.*
- Verifica que efectivamente el servicio estaba expuesto porque las reglas de *firewall* no se estaban aplicando a pesar de haber sido creadas, configuradas y aplicadas en el servicio de *scaleway*.
- Procede a parar el servicio y eliminar el *Cluster* temporal que seguía todavía activo.
- La persona técnica no conocía el contenido ni alcance de ese *Cluster*.
- Traslada una respuesta a "atención al cliente" para dar respuesta al *ticket*.
- La persona confirma la resolución de la incidencia.

03-11-2019:
- A las 19:10 un miembro de la empresa recibe una noticia de prensa y la comparte con todo el equipo técnico CTO, DPO y el responsable de infraestructura, notando que está relacionado con el *cluster* de *elasticsearch* eliminado.
- Se inician investigaciones técnicas en referencia al posible contenido expuesto del *cluster* de *elasticsearch* eliminado.
- Se realiza una primera investigación interna para evaluar el alcance de la incidencia. Se descubren datos de usuarios y se inician las investigaciones.

04-11-2019:
- El equipo técnico al completo realiza una primera valoración, encontrando dos índices con datos personales de clientes. Tras un día investigando deja constancia de los datos de usuarios encontrados.
- Se publica el comunicado inicial.
- Se añade un aviso en la cabecera de la web enlazando al comunicado que sigue activo a día del informe 12/11/2019.
- Publicación en las redes sociales enlazando al comunicado.
- Se envían correos electrónicos con la nota informativa y enlace al comunicado a los usuarios afectados.
- Se preparan medidas para evitar futuros sucesos similares.
- Se inician tareas derivadas de las medidas mencionadas.
- Se atienden a medios de comunicación que contactan para pedir más información.

05-11-2019:
- A las 00:39 se realiza el envío el informe a la AEPD.
- Se atienden solicitudes de información o supresión de usuarios.

06-11-2019:
- El equipo técnico continúa revisando a fondo los *logs* (145 millones de registros) y encuentran nuevos datos de usuarios.
- Se percatan que hay procesos que borran los *logs* de envío de emails a los 30 días.
- Por el motivo anterior se decide considerar afectado a todo usuario con correo electrónico validado.
- Primer contacto con INCIBE.

07-11-2019:
- Se concluye la investigación y se precisa al detalle el número de afectados y datos expuestos.
- Se decide aplicar una política de renovación de contraseñas preventiva a ciertos usuarios afectados.

08-11-2019:
- Se realiza una nueva comunicación a los usuarios.
- Se fuerza el cambio de contraseña a unos 2000 usuarios.

09-11-2019: Se continúa con investigaciones para confirmar que no hay más datos expuestos

11-11-2019: Se amplía la información del comunicado público con más detalles.

La entidad ha aportado copia de las comunicaciones remitidas a los usuarios.

Sobre los datos expuestos:

Informan que el total de registros en el *Cluster* de *Elasticsearch* generados durante el periodo 24/05/2019 hasta el 04/09/2019 y expuestos hasta el 25/10/2019 es de 141.545.213 registros.

En todos los registros las contraseñas aparecen cifradas, salvo algunas que indican corresponden a un "*debug*" intencionado que no se eliminó por lo que quedaron expuestas 7.526 ocurrencias de un total de 1.757 usuarios únicos afectados.

Los números de tarjetas bancarias de los usuarios aparecen truncados. Indican que con esos datos es imposible realizar ninguna operación o compra.

Los números identificativos corresponden a documentos de identidad de diferentes países, en el caso de España, mayoritariamente DNI y NIE. Solo aparece el número, no está especificado el nombre, tampoco contiene la imagen, ni el tipo de documento ni más información en relación a dicho documento, de un total de 1915 usuarios únicos afectados.

Otros datos corresponden al detalle necesario para realizar retirada de las donaciones y premios conseguidos en la web, con un total de 897 registros con datos personales: de 697 Titulares únicos, 527 Teléfonos únicos y 663 direcciones postales únicas (sin

incluir ciudad, provincia ni país). Un total de 28.767 registros únicos con teléfonos pertenecientes a 2.657 usuarios únicos afectados por el número teléfono.

En todos los *logs* de acciones, se añade la IP de donde ha sido ejecutada dicha acción con un número aproximado de registros debido a la complejidad técnica para extraer esta información, unos 9.170.853 registros. El número de IP únicas es de 759.806 correspondientes a un total de 215.878 usuarios únicos afectados por la exposición de su IP.

El número de registros con dirección de correo electrónico legible aproximado debido a la complejidad técnica para extraer esta información, es de 50.000.000. Número aproximado de emails únicos en esos registros: 330.000, que se corresponde con el número aproximado de usuarios únicos afectados por dicho dato.

Durante *chats* (o conversaciones) entre emisor y usuarios se produce un registro de las conversaciones. El total de registros con conversaciones expuestas es de 1.502.933 correspondientes a 8.964 usuarios únicos con conversaciones. En los *logs* aparecen el mensaje en claro (texto) y la IP del usuario.

Se trata de servidores de videos de índole sexual como *"*****SERVIDOR.1**"* o *"*****SERVIDOR.2**"*.

Han aportado extractos de los *logs* donde se aprecia la estructura de los datos expuestos. En ellos se aprecia que la información expuesta de las cuentas de los emisores (personas que emiten los videos con contenidos sexuales también denominadas comúnmente *Camgirls*) consiste en al menos su nombre y apellidos, teléfono y dirección postal completa.

Indican que han realizado investigaciones de ciberinteligencia en colaboración con el INCIBE y tanto ellos como INCIBE no han detectado que se hayan filtrado los *logs* o que estén disponibles a disposición de terceros en ningún sitio de Internet, siguiendo la realización de esta rutina de detección semanalmente.

Manifiestan que el INCIBE les felicitó expresamente por la gestión y la colaboración realizada con ellos. Adjuntan correo electrónico que INCIBE envió el día 28 de noviembre a las 16:05 horas donde consta que no detectaron usos posteriores de los datos ni filtración en Internet y la felicitación por la gestión y colaboración.

2.- MEDIDAS PREEXISTENTES

La entidad ha aportado copia del Registro de Actividades de Tratamiento (RAT) de las que es responsable, de fecha 22/02/2019. Ha aportado, así mismo, copia de un Análisis de Riesgos versión 1.1, si bien éste se encuentra fechado el 14/11/2019

Como se ha indicado, al realizar el cambio a "*Scaleway*" en el *firewall* se crearon y aplicaron las reglas de configuración del *firewall,* aportando la entidad varias impresiones de pantalla certificadas por eGarante con fecha 9/11/2019 en las que se ven aplicadas tres reglas para el tráfico entrante en los servidores.

En otra pantalla se lee que el 27/05/2019 no existen incidentes reportados y que en fecha 29/05/2019 se detecta inestabilidad.

Sobre la diligencia previa en la contratación del servicio de *Scaleway*, los representantes de la entidad manifiestan que en el momento de elegir dicho proveedor de servicios se tuvo en cuenta:

1- Que es uno de los proveedores de servidores más grandes de Francia (anteriormente conocido como Online.net).

2- Dispone de certificaciones ISO 27001 y 50001 así como también HDS.

3- Sus *datacenters* son TIER III (clasificación según estándar ANSI/TIA-942) y se encuentran en ******PAÍS.1***

4- La política de privacidad fue auditada y se determinó conforme a los requisitos de la normativa de protección de datos, donde se contempla un apartado propio en el caso de que sucedan brechas de seguridad.

Indican que la propia política de privacidad, que se debe aceptar necesariamente para contratar con *Scaleway,* incluye todos los elementos recogidos en el artículo 28.3 del RGPD en lo que respecta al contenido del contrato entre responsable y encargado. Todo lo anterior llevó a la conclusión interna de que era una elección óptima de cara a las necesidades técnicas y de seguridad, pero también legales.

3.- MEDIDAS POSTERIORES A LA BRECHA DE SEGURIDAD

Los representantes de la entidad han manifestado que se están realizando modificaciones sobre las medidas con posterioridad a los hechos, detallando las siguientes:

- Se realiza la contratación del CISO (*Chief Information Security Officer)* para el día 11/11/2019.
- Mejorar la comunicación entre proveedores de este tipo de servicios.
- Determinar listado de *logs* con datos no necesarios para la revisión técnica y eliminar esos *logs* concretos.
- Cifrado de la totalidad del contenido de los *logs*.
- Revisión de política de borrado de *logs* y disminuir tiempos en la medida de lo posible.
- Recifrado de datos con claves nuevas y aplicación de algoritmos *hash* a las contraseñas.
- Revisión adicional de todos los sistemas con almacenados de cualquier tipo de datos, para eliminar datos innecesarios o cifrar los que corresponda

Adicionalmente detallan una serie de medidas de seguridad destinadas a la detección y gestión de vulnerabilidades basadas en metodologías DevSecOps (metodología de trabajo que integra la seguridad en el desarrollo del software y su operación). Se incluyen entre otras medidas la utilización de herramientas para el análisis automático del entorno web imitando un agente malicioso externo, auditorias periódicas y revisiones de todas las incidencias por un analista de seguridad.

Para la minimización de los efectos adversos de la brecha de seguridad, la entidad realizó las siguientes acciones:

03-11-20193
Revisión del estado de la máquina donde estaban los datos expuestos y verificación de su apagado.
Primer análisis de los datos expuestos.
Se arregla el fallo que impedía recibir emails al correo de privacidad desde fuera de la empresa.

04-11-2019
El equipo técnico realiza una primera valoración, encontrando dos índices con datos personales.

El equipo técnico deja constancia que no ha encontrado otros datos de usuarios.
Se publica el comunicado inicial.

Se añade un aviso en la web enlazando al comunicado.

Publicación en las redes sociales enlazando al comunicado.

Se envían correos electrónicos con la nota informativa y enlace al comunicado a los usuarios afectados, diferenciando entre los datos menos sensibles (emails e IP's) de los más sensibles (documentación y dirección postal).

Se preparan medidas para evitar futuros sucesos similares.

Se inician tareas derivadas de las medidas mencionadas, entre ellas revisar la securización de todos los servicios del sistema (accesos a máquinas y redes internas sobre todo).

Se atienden a medios de comunicación que contactan para pedir más información.

05-11-2019
Se realiza el envío del informe a la AEPD.

Se atienden las peticiones de información del suceso y/o supresión de datos.

El equipo técnico continúa con las tareas surgidas del anterior punto.

06-11-2019
El equipo técnico realiza otra revisión más exhaustiva. Se percatan de la existencia de otro índice dentro de los *logs* técnicos con más datos de usuario expuestos.

Encuentran que faltan datos disponibles que pudieron estar expuestos debido a que unos índices se borran automáticamente al cabo de un mes y otros al cabo de 3.

07-11-2019

El equipo de infraestructura recupera el *backup* de los índices borrados usado para rellenar el histórico del nuevo *Cluster*.

En la revisión realizada a estos nuevos datos, se encuentran nuevos datos personales y los números totales de afectados.

Se decide desarrollar una política de renovación de contraseñas a los usuarios afectados con previo aviso.
Se decide rectificar el comunicado público.

Se colabora con INCIBE y envía el informe completo a INCIBE

08-11-2019
Se aplica el cambio de contraseña forzado a los usuarios afectados mencionado en el anterior punto 3.

11-11-2019 Se publica el nuevo comunicado público con los cambios surgidos.

TERCERO: Con fecha 17 de junio de 2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a VTS, por la presunta infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD.

CUARTO: Con fecha 1/07/2020 y registro de entrada 022543/2020, VTS presentó alegaciones al acuerdo de inicio en el sentido de que no desea realizar ninguna manifestación al respecto, quedando a disposición de esta AEPD para colaborar en todo lo que sea necesario. En consecuencia, a tenor de lo dispuesto en los artículos 64.2.f) y 85 de la Ley 39/2015, de 1 de octubre del Procedimiento Administrativo Común de las Administraciones Públicas, el acuerdo de inicio puede ser considerado propuesta de resolución. En consecuencia, esta Agencia procede a dictar 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: con fecha 24/10/2019 VTS, en calidad de responsable del tratamiento, expuso en internet información personal de sus clientes recabada durante el periodo de mayo a octubre. Se confirmó la brecha de seguridad el 3/11/2019 tras las investigaciones iniciadas y la publicación de la noticia en un medio de comunicación.

SEGUNDO: Con fecha 5/11/2019, VTS notificó a esta Agencia una brecha de seguridad como consecuencia de la exposición en Internet de *logs* técnicos (registros de actividad de los servidores) en los que se encontraban embebidos y técnicamente de difícil acceso datos personales de los clientes.

TERCERO: Las categorías de datos afectados son direcciones IP, DNI, direcciones de email con contraseñas, números de tarjetas truncadas y *chats* de los clientes.

QUINTO: Con fecha 9/11/2019, se restablece la seguridad del sistema de información de VTS.

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 artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

Se imputa al reclamado la comisión de una infracción por vulneración del Artículo 32 del RGPD, que señala que *"transcripción".* La infracción se tipifica en el Artículo 83.4 del RGPD y es calificada de Grave en el artículo 73.f) de la LOPDGDD.

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 VTS 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.

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.

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.)

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

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, 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 o social significativo; 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, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados., (…)"*

De las actuaciones practicadas se ha verificado que las medidas de seguridad con las que contaba VTS en relación con los datos que sometía a tratamiento en calidad de responsable, no eran las adecuadas al momento de producirse la brecha de seguridad, 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 tanto técnicas como organizativas 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.

Otra consideración es que el tratamiento de datos al que están suscritos los afectados, se refiere a la actividad definida en el art 9 del RGPD como categorías especiales de datos personales.

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 conducta sexual, partiendo únicamente de los datos de un suscriptor y combinándola con otras.

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, 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 contenido de los *logs* expuestos de los clientes, podría revelar un determinado comportamiento y vida sexual, y que no tiene por qué haber sido consentida por su titular.

Esta posibilidad supone un riesgo añadido que se ha de valorar previamente y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de los derechos y libertades de los afectados, en virtud de lo dispuesto en el citado art 9 del RGPD.

Este riesgo y el impacto sobre los derechos y libertades de los afectados debe ser tenido en cuenta por el responsable del tratamiento y, en función del mismo, establecer las medidas de índole técnica y organizativas que impidan la pérdida de control de los datos por parte del responsable del tratamiento y, por tanto, también por los titulares de los datos que se los proporcionaron.

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 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.

VIII

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."

Esta falta de diligencia a la hora de implementar las medidas de seguridad adecuadas de índole técnico y organizativo constituyen el elemento de la culpabilidad suficiente 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 suscriptores de información relacionada con el servicio contratado, y su posterior difusión pública, agrava el reproche culpabilístico y sancionador de la conducta llevada a cabo por VTS.

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*", 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."

X

En el presente caso, en atención a la diligencia llevada a cabo por VTS en lo referente a la notificación sin dilación indebida de la brecha de seguridad a esta Agencia Española de Protección de Datos, la comunicación diligente y reiterada por diversos medios a los afectados, la complejidad técnica de los sistemas de información, el inicio diligente y rápido de acciones tendentes a minimizar las consecuencias negativas de la brecha de seguridad, no constar reincidencia, que la brecha de seguridad tuvo su origen en un fallo de seguridad sobrevenido en el nuevo proveedor del servicio *Scaleway* habiendo comprobado VTS que disponía de las adecuadas las medidas certificadas de seguridad (TIER III, según estándar ANSI/TIA 942) instaladas por defecto, permite considerar una disminución de la culpa en los hechos imputados, por lo que 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 valorada la culpabilidad en los hechos imputados cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a VTS MEDIA S.L., con NIF B63546253, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD y 73.f) de la LOPDGDD, una sanción de apercibimiento.

SEGUNDO: Requerir a VTS MEDIA S.L. para que en el plazo de tres meses aporte a esta AEPD la siguiente documentación:

- Aportar procedimiento reglado de actuación ante una incidencia de seguridad informática que permita conocer si ha afectado a datos personales y que identifique las ubicaciones y recursos afectados (brecha de seguridad).

- Aportar auditoría, que deberá incluir análisis de riesgos y evaluación de impacto conforme lo dispuesto en el artículo 35 del RGPD, realizada tras la brecha de seguridad que certifique el correcto funcionamiento y configuración del sistema de información al objeto de evitar en el futuro incidencias como la analizada en el presente procedimiento. Esta auditoría también deberá realizarse y quedar a disposición de la AEPD cuando se produzcan modificaciones en los recursos o tratamientos que afecten a datos personales.

TERCERO: NOTIFICAR la presente resolución a **VTS MEDIA S.L.,** con NIF B63546253, y domicilio en c/ Doctor Trueba 183, Piso 8º, Puerta 1, 08021 Barcelona.

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