- **Expediente Nº: E/03299/2021**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: El ***A.A.A.*** (en adelante, la parte reclamante) con fecha 23 de febrero de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **TELCOM BUSINESS SOLUTIONS S.L**. con **CIF B92563626** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que ha sido puesta en venta, en un foro de la Internet oscura, información que puede comprometer la privacidad de clientes de la parte reclamada.

El número de afectados según la reclamación asciende a 9.000.

Junto a la reclamación aporta:

Dos documentos Word con pantallazos del mencionado foro, donde el usuario ******USUARIO.1*** publica mensajes en ruso y en uno de ellos, incluye una captura de pantalla de una hoja Excel, con datos personales de los afectados.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

Con fecha 25/03/21 se recibe en esta Agencia escrito de respuesta al requerimiento de información solicitado.

TERCERO: Con fecha 12 de marzo de 2021 se admitió a trámite la reclamación presentada por la parte reclamante, al amparo de lo establecido en el artículo 65.5 de la LOPDGDD.

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

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

Respecto de las causas que hicieron posible la brecha

(…).

Respecto de los datos afectados.

(…).

Comunicación a los afectados:

(…).

Respecto de las medidas de seguridad implantadas

Con anterioridad a la brecha:

(…).

Con posterioridad a la brecha:

(…).

Respecto de la notificación con posterioridad a las 72 horas.

La notificación la hace TELCOM BUSINESS SOLUTIONS S.L, después de enterarse por el traslado de la reclamación desde esta Agencia.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo.

No se tiene información de eventos análogos.

FUNDAMENTOS DE DERECHO

I

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

II

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante brecha de seguridad) como "*todas aquellas violaciones de la seguridad que ocasionen 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."*

Hay que señalar que la recepción de una reclamación sobre una brecha de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado.

III

El Artículo 32 del RGPD establece:

"Seguridad del tratamiento

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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y

tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haber tenido acceso a datos personales personas no autorizadas a ello.

La parte reclamada, alega que los datos afectados, no son datos especialmente protegidos, al ser de carácter identificativos y económicos-financieros, y tratarse de datos correspondientes a empresas/autónomos, que están fuera del ámbito de la regulación de protección de datos personales al pertenecer a personas jurídicas.

Teniendo en cuenta el artículo 19.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que según su literal establece que:

"1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios".

Y teniendo en cuenta también el artículo 19.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que según su literal establece que:

"2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas".

Los datos relativos a las personas jurídicas y sus correlativos tratamientos no se encuentran incluidos en el ámbito de aplicación del RGPD, tal y como establece su considerando 14. Ahora bien, sí se protegen los datos personales de las personas físicas, debiéndose tener en cuenta la consideración que incluye el artículo 19 de la LOPDGDD precitado relativa a los datos de los empresarios individuales.

Tras el requerimiento de información llevado a cabo por la Inspección de esta AEPD, la parte reclamada ha informado de todas las actuaciones llevadas a cabo para paliar el incidente.

Cabe destacar la buena disposición de la parte reclamada en el sentido de que, en cuanto ha tenido conocimiento del incidente, ha puesto en marcha las medidas oportunas para evitar que se pueda repetir en el futuro.

De la documentación aportada por la parte reclamada en el curso de estas actuaciones de investigación no se desprende que, con anterioridad a la brecha de seguridad, la parte reclamada careciera de medidas de seguridad razonables en función de los posibles riesgos estimados.

Asimismo, no existen evidencias de que no hubiera actuado de forma diligente una vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

IV

El artículo 33 del RGPD dispone:

"Notificación de una violación de la seguridad de los datos personales a la autoridad de control

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

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

3. La notificación contemplada en el apartado 1 deberá, como mínimo:
a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

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

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las

medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

En el presente supuesto, se ha notificado la brecha de seguridad en un plazo no superior a 72 horas, la parte reclamada, la notifica diligentemente después de enterarse por el traslado de la reclamación desde esta Agencia.

IV

El artículo 34 del RGPD establece*:*

"Comunicación de una violación de la seguridad de los datos personales al interesado

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. L 119/52 ES Diario Oficial de la Unión Europea 4.5.2016

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1; c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

La parte reclamada había adoptado las medidas de protección técnicas y organizativas apropiadas y estas medidas se habían aplicado a los datos personales afectados por la brecha de seguridad.

La parte reclamada alega que no es necesario comunicar a los afectados, amparándose en la "guía para la gestión y notificación de brechas de seguridad", adjunta baremación realizada a partir de la guía publicada por esta Agencia en su Anexo III. Además, la parte reclamada indica que son datos que ya son públicos en

sus correspondientes páginas web y por tratarse de empresas no entran en el ámbito del dato personal y que los correos electrónicos y nombres corresponden al personal de dichas empresas dentro de su ámbito laboral.

La parte reclamada ha tomado medidas ulteriores que garantizaban que ya no existía la probabilidad de que se concretara un alto riesgo para los derechos y libertades de los interesados. A mayores y ante la notificación de la AEPD, se han realizado las siguientes acciones: ***(…).***

No constan ante esta AEPD reclamaciones de posibles afectados.

V

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a TELCOM BUSINESS SOLUTIONS S.L.

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

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

940-0419

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