Expediente Nº: E/05954/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad ***AVANZA EXTERNALIZACIÓN DE SERVICIOS S.A, CAJAMAR CAJA RURAL, SOCIEDAD COOPERATIVA DE CRÉDITO*** en virtud de denuncia presentada por ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha de 17 de junio de 2015 tiene entrada en esta Agencia un escrito de ***A.A.A.*** en el que declara que la empresa ***AVANZA EXTERNALIZACION DE SERVICIOS S.A.*** (***CEGIMA*** hasta 29/01/2015) obliga a sus empleados a trabajar utilizando las claves de acceso de otros trabajadores.

La denunciante se ha dirigido por escrito el 29 de mayo y 8 de junio de 2015, a ***AVANZA EXTERNALIZACION DE SERVICIOS S.A.*** (en adelante ***AVANZA)***, solicitando le sean facilitadas sus claves de acceso para entrar en la aplicación (***TOKEN***) de ***CAJAMAR*** en la que trabaja, ya que en este momento está utilizando las correspondientes a su compañera, ***B.B.B.*** usuario ******USUARIO.1,*** destinada en la actualidad a otro departamento de ***AVANZA***, ya que considera que se está incurriendo en un delito de suplantación de personalidad.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

En relación con el acceso a ***CAJAMAR*** por parte de sus trabajadores y la asignación de usuarios y contraseñas:

- ***AVANZA***, presta a la entidad ***CAJAMAR*** servicios de Back Office Financiero. Sólo hay una persona encargada de la supervisión técnica del trabajo.
- Aproximadamente 100 trabajadores de ***AVANZA*** tienen acceso a las aplicaciones que gestionan los ficheros de ***CAJAMAR*** para el desarrollo de la prestación de servicios.
- Para dar de alta a los usuarios, por parte del supervisor de ***AVANZA*** se realiza una petición a ***CAJAMAR***, la cual asigna el nombre de usuario y una contraseña inicial, que debe ser cambiada obligatoriamente por el trabajador al iniciar la primera sesión y antes de acceder por primera vez. Así mismo, ***CAJAMAR*** asigna a cada usuario el perfil correspondiente al trabajo que va a realizar en función del servicio concreto al que este adscrito el trabajador.
- Cada trabajador dispone de su propio usuario y contraseña de acceso al sistema de ***CAJAMAR***, en función del servicio al que está adscrito, ***CAJAMAR*** es la encargada del control de los accesos que se realizan a su sistema. En ningún caso un trabajador utiliza el usuario y la contraseña de otro trabajador.
- El acceso al sistema de información de ***CAJAMAR*** por parte de los usuarios de ***AVANZA*** conlleva una serie de controles tanto a nivel de identificación del usuario como del ordenador desde el que se accede, para lo cual ***CAJAMAR*** dispone de la relación de ordenadores (nombres de maquina) desde los que se van a realizar los accesos, facilitada por ***AVANZA***, y solo desde estos ordenadores se va a permitir el acceso.

- Se comprueba que el control de seguridad implementado por ***CAJAMAR*** establece un sistema de acceso cifrado punto a punto, para lo cual facilita un software denominado ***TOKEN***, que es instalado en el ordenador del usuario, de manera que cada usuario solamente puede acceder desde su ordenador. Dicho ***TOKEN*** además permite que la contraseña de acceso al sistema de información de ***CAJAMAR*** sea dinámica, de manera que dicha contraseña de acceso contiene una parte fija conocida solamente por el usuario y una parte variable que la facilita el ***TOKEN.***

Respecto al acceso de la denunciante al sistema de ***CAJAMAR***:

- Se aporta copia del correo electrónico de fecha 14 de enero de 2014 en el que se da de alta por ***CAJAMAR*** el usuario de la denunciante, y del correo electrónico con fecha 2 de junio de 2015, en el que se solicita la baja de dicho usuario.

En relación con el listado de trabajadores y de las pantallas de acceso donde consta el acceso con el usuario ******USUARIO.1*** aportados a la Agencia por la denunciante ***AVANZA*** ha manifestado que:

- La única persona que tiene acceso al listado de usuarios de ***CAJAMAR*** es la supervisora, por lo que no reconoce el listado aportado por la denunciante como elaborado por la empresa.
- En los listados de usuarios de ***CAJAMAR*** del mes de mayo y del mes de junio de 2015 se verifica que el usuario ******USUARIO.1*** no consta en ninguno de los dos listados.
- Se verifica que en el mes de junio de 2015, todas las personas que constan en el listado aportado por la denunciante, excepto dos, se encuentran en situación de alta en la compañía
- Se acredita documentalmente mediante carta de 18 de diciembre de 2014, remitida por ***CEGIMA*** (en la actualidad ***AVANZA)*** a ***B.B.B.,*** titular del usuario ******USUARIO.1,*** que desde ese momento, queda adscrita al servicio de recuperación de deuda.

AVANZA aporta los siguientes documentos para acreditar su debida diligencia:

- ***Documento de seguridad***, donde se manifiesta que se ha elaborado de acuerdo a lo dispuesto en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal, aprobado mediante real decreto 1720/2007 de 21 de diciembre.
- ***Documento donde se describen las funciones y obligaciones de los usuarios*** y Procedimientos de Alta y Baja de los usuarios.
- ***Control de acceso a los sistemas de información*** de ***CAJAMAR***
- ***Normas de contraseñas*** dadas por ***CAJAMAR***.

En relación con los escritos remitidos el 29 de mayo y 8 de junio de 2015, por la denunciante a ***AVANZA*** se manifiesta que la Directora de Recursos Humanos lleva a cabo las siguientes acciones:

- Con fecha 29 de mayo de 2015, se mantuvo una reunión con la denunciante a la que también asistió un representante de los trabajadores. En la reunión se solicitó a la denunciante mayor detalle sobre los términos de su escrito y se acordó revisar los perfiles con los responsables del servicio, para poder dar una respuesta definitiva y corregir, en su caso, los posibles errores.
- Se encargó a la supervisora de la plataforma la revisión del cumplimiento de los protocolos de seguridad de la compañía en este caso particular.

- Con fecha 8 de junio de 2015, tras finalizar el análisis interno, la supervisora dio respuesta verbal a la denunciante, indicándole que su usuario no estaba siendo utilizado por ningún otro compañero y que se había procedido a solicitar a ***CAJAMAR*** la baja de su usuario con fecha 2 de junio tras su reasignación a otro servicio.

Respecto a los servicios prestados a ***CAJAMAR***:

- Con fecha 6 de mayo de 2016, mediante correo electrónico, ***AVANZA*** ha remitido a esta Agencia copia del anexo al contrato marco de prestación de servicios suscrito con ***CAJAMAR*** de fecha 1 de junio de 2009, donde se detalla el servicio de verificación de expedientes hipotecarios de la entidad bancaria así como de la adenda al citado contrato marco, de fecha 1 de febrero de 2015, por la que se modifican las condiciones económicas del mismo.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

En el supuesto que nos ocupa, respecto del tratamiento de datos realizado por ***AVANZA***, ha de tenerse en cuenta que el artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), establece como regla general el previo consentimiento del interesado para la comunicación de datos personales a un tercero. Así dispone en su apartado 1 lo siguiente: *"1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado."*

El artículo 3. i) de la citada norma define la "*cesión o comunicación de datos*" como "*toda revelación de datos realizada a una persona distinta del interesado*".

No obstante lo anterior, la propia LOPD habilita, en su artículo 12, el acceso de terceros a los datos personales cuando el acceso a los datos se realice para prestar un servicio al responsable del fichero o del tratamiento, al señalar en su apartado 1: *"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento."*

El citado artículo 12.1 de la LOPD permite, por tanto, el acceso a datos de carácter personal a la persona o entidad que presta un servicio al responsable del fichero, sin que, por mandato expreso de la ley, pueda considerarse dicho acceso como una cesión o comunicación de datos.

En el presente caso, de la documentación aportada se desprende que ***AVANZA*** presta servicios de Back Office Financiero a ***CAJAMAR***, durante el periodo comprendido entre 01/10/2013 y 30/06/2016.

III

En lo que respecta a la seguridad de los datos personales, el artículo 9 de la LOPD establece que:

"1. *El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.*

2. *No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.*

3. *Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."*

En este sentido el artículo 93 del RLOPD, respecto a la identificación y autenticación de los datos establece que:

"1. *El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.*

2. *El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.*

3. *Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.*

4. *El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible."*

Así las cosas, ha de señalarse que ***AVANZA*** aporta documentación consistente en ***contrato de servicios*** firmado con ***CAJAMAR***, así como ***documento de seguridad, documento donde se describen las funciones y obligaciones de los usuarios y Procedimientos de Alta y Baja de los usuarios***, ***control de acceso a los sistemas de información*** de ***CAJAMAR*** y ***normas de contraseñas*** dadas por ***CAJAMAR***.

La Directora de Recursos Humanos de ***AVANZA*** tras recibir los escritos presentados por la denunciante el 29 de mayo y 8 de junio de 2015, al convocar a la denunciante a una reunión donde se acordó revisar los perfiles con los responsables del servicio, para poder dar una respuesta definitiva y corregir, en su caso, los posibles errores, encargar a la supervisora de la plataforma la revisión del cumplimiento de los protocolos de seguridad de la compañía en este caso particular, y tras finalizar el análisis interno, darle la supervisora una respuesta verbal a la denunciante, en la que se le indica que su usuario no estaba siendo utilizado por ningún otro compañero y que se había procedido a solicitar a ***CAJAMAR*** la baja de su usuario con fecha 2 de junio tras su reasignación a otro servicio.

Añadir que en relación con el listado de trabajadores y de las pantallas de acceso donde consta el acceso con el usuario ******USUARIO.1*** aportados a la Agencia por la denunciante ***AVANZA*** ha manifestado que:

- La única persona que tiene acceso al listado de usuarios de ***CAJAMAR*** es la supervisora, por lo que no reconoce el listado aportado por la denunciante como elaborado por la empresa.

- En los listados de usuarios de ***CAJAMAR*** del mes de mayo y del mes de junio de 2015 se verifica que el usuario ******USUARIO.1*** no consta en ninguno de los dos listados.
- Se verifica que en el mes de junio de 2015, todas las personas que constan en el listado aportado por la denunciante, excepto dos, se encuentran en situación de alta en la compañía
- Se acredita documentalmente mediante carta de 18 de diciembre de 2014, remitida por ***CEGIMA*** (en la actualidad ***AVANZA)*** a ***B.B.B.,*** titular del usuario ******USUARIO.1,*** que desde ese momento, queda adscrita al servicio de recuperación de deuda.

Dicho esto, se ha de tener en cuenta que al Derecho Administrativo Sancionador, por su especialidad, le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad del principio de presunción de inocencia.

En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta *"que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio".*

De acuerdo con este planteamiento, el artículo 137.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, establece que "*Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario."*

En definitiva, la aplicación del principio de presunción de inocencia impide imputar una infracción administrativa cuando no se hayan obtenido evidencias o indicios de los que se derive la existencia de infracción.

En este sentido y para este caso, se ha de señalar que de la documentación aportada no se desprenden indicios razonables que permitan establecer que el usuario de la denunciante esté siendo utilizado por otro trabajador, ya que se ha constatado que ***AVANZA*** ha solicitado a ***CAJAMAR*** la baja de su usuario con fecha 2 de junio de 2015, tras su reasignación a otro servicio.

Tampoco existen indicios de los que se infiera que la denunciante ha utilizado el usuario ******USUARIO.1,*** asignado a otra compañera para acceder a los ficheros de ***CAJAMAR***, ya que en las fechas indicadas por la denunciante, dicho usuario no figuraba en ninguno de los listados facilitados por ***CAJAMAR***, ya que desde el 18 de diciembre de 2014, la titular de ese usuario se encontraba adscrita a otro servicio y ***CAJAMAR*** asigna a cada usuario el perfil correspondiente al trabaja que va a realizar en función del servicio concreto al que esté adscrito el trabajador.

IV

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a ***AVANZA EXTERNALIZACIÓN DE***

SERVICIOS S.A, CAJAMAR CAJA RURAL, SOCIEDAD COOPERATIVA DE CRÉDITO y a ***A.A.A..***

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, 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 del referido texto legal.

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