- **Expediente N.º: EXP202500101**

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: Con fecha 2 de diciembre de 2024, se presentó reclamación ante la Agencia Española de Protección de Datos contra **FINANCIERA EL CORTE INGLES E.F.C., S.A.** con NIF **A81322448** (en adelante, la parte reclamada o Financiera). Los motivos en que basa la reclamación son los siguientes:

El reclamante manifiesta que recibe una llamada en su número de teléfono para reclamarle una deuda en concepto de compras de una tarjeta de El Corte Inglés, y señala que responde que acudirá personalmente al establecimiento El Corte Inglés de ******LOCALIDAD.1***, para aclarar lo sucedido. En dicho establecimiento le informan de que consta un cargo de ******CANTIDAD*** euros por concepto de compras, realizadas con una tarjeta que consta a su nombre con la terminación ******TARJETA.1*** el día ******FECHA.1*** correspondiente a un comercio con ubicación en ******LOCALIDAD.2***. Le indican que está relacionada con una cuenta bancaria de ******ENTIDAD.1***, con número de cuenta ***(…)***, la cual no es de su titularidad.

Una vez confirmada la acción fraudulenta por el establecimiento, se bloquea todo lo que está a nombre del reclamante y se abre expediente en el establecimiento haciendo constar todo lo sucedido. Desde la Central del Corte Inglés le informan que existen dos tarjetas más a su nombre sin tener el reclamante conocimiento de ello, por lo que solicita que las den de baja y cancelen todo. Asimismo, modifica las claves de acceso de su cuenta de cliente para evitar más fraudes, y en su área de cliente comprueba que no existen contratos o documentos firmados en los que él haya autorizado esas tarjetas.

El reclamante solicita a la central del Corte Inglés todo su expediente y contratos, contestándole desde la financiera que no pueden realizar esta acción y que tienen que esperar a que les informen desde fraude.

El 28 de noviembre de 2024, el reclamante recibe en su buzón otra tarjeta con otra terminación a la que no ha dado su consentimiento.

Junto a la notificación se aporta:

- Aporta reclamación efectuada ante la OMIC.

- Foto de la tarjeta y cargo realizado.

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 Financiera, 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.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 10 de enero de 2025 como consta en el acuse de recibo que obra en el expediente.

Con fecha 7 de febrero de 2025 se recibe en esta Agencia escrito de alegaciones poniendo de manifiesto lo siguiente:

- La parte reclamante era cliente de la entidad reclamada hasta el 20 de enero de 2025 día en que procedió a anular su tarjeta de compra.

- El 25 de noviembre de 2024, la Financiera contactó con el Reclamante en aras de informarle sobre un recibo pendiente de abono de su Tarjeta por un importe de ******CANTIDAD.*** €, correspondiente a un cargo efectuado el ******FECHA.1***. Dicho cargo no fue reconocido por la parte reclamante y se personó en la oficina del Servicio de Atención al Cliente (SAC en lo sucesivo) de El Corte Inglés de ******LOCALIDAD.1*** para esclarecerlo sucedido. En esta oficina se le informó que sus datos habían sido recientemente modificados: su número de teléfono móvil, e-mail y domicilio postal, así como que la compra objeto del recibo impagado se había realizado con una tarjeta finalizada en ******TARJETA.2***, y no con la terminada en ******TARJETA.1***, que el Reclamante identifica en su escrito, por lo que se apreció una potencial suplantación de identidad de la parte reclamante.

- Que, ante estos hechos, el agente que atendió a la parte reclamante modificó su número de teléfono móvil, e-mail y domicilio postal, informándole de la apertura de un expediente sobre la incidencia, registrada con el número ***(…)***, e indicándole que se le enviaría posteriormente a su correo electrónico para su conocimiento y correcto seguimiento (en adelante, el "Expediente"). Asimismo, el 25 de noviembre de 2024 y en presencia de la parte reclamante, el SAC procedió a bloquear su tarjeta, así como, por precaución, la del otro interviniente del Contrato de TC. Se destaca en este sentido, que, en cumplimiento de los protocolos internos de la Financiera, lo anterior dio lugar a la emisión automática de otras dos nuevas tarjetas físicas vinculadas al Contrato de TC de la parte reclamante. Esta operativa, tal y como se desprende del Informe de la Delegada de Protección de Datos de Financiera, corresponde con la operativa interna que se aplica al bloqueo de tarjetas por robo o extravío, en cuya virtud se anula instantáneamente la tarjeta vigente hasta el momento (potencialmente en poder del suplantador), sin posibilidad de volver a ser utilizada, y se cursa la emisión automática de una nueva tarjeta (sin activar), sin que se requiera la firma de un nuevo contrato, dado que se emite al amparo del contrato ya suscrito.

- Con fecha de 26 de noviembre de 2024, el expediente fue analizado por la Unidad de Prevención del Fraude de la Financiera (en adelante, la "UPF") llegándose a las siguientes conclusiones:

    - El fraude tuvo origen en la modificación de datos (en primer lugar, número de teléfono móvil) efectuada el día 12 de octubre de 2024 por el canal *Interactive Voice Response* IVR (en lo sucesivo, asistente virtual o IVR). Los protocolos de seguridad de la Financiera exigen que, para modificar el número de teléfono móvil facilitado contractualmente por cualquier canal, se envíe una clave de un solo uso (en lo sucesivo, OTP) cruzada al correo electrónico asociado al contrato de tarjeta del cliente para finalizar el proceso. Esta circunstancia se produjo y permitió la posterior modificación de la contraseña desde su Área Privada y resto de datos en días posteriores.
    - El suplantador, una vez modificada la dirección postal del Reclamante, solicitó el envío de una nueva tarjeta por extravío de la anterior, siendo esta la utilizada para la operación fraudulenta. Que para todo lo anterior, el correo electrónico personal del Reclamante tuvo que ser interceptado, bien por estar su correo electrónico vulnerado o bien facilitarse (la OTP) al suplantador a través de engaño o artificio similar (phishing), así como, los datos personales del Reclamante tales como nombre, apellidos, DNI, número de teléfono y código postal debían de ser conocidos por el suplantador, pues son datos requeridos a diferentes niveles para la verificación de cualquier cambio y/o modificación de los datos personales contenidos en las fichas de clientes.

- El mismo 26 de noviembre de 2024, la UPF remitió sus conclusiones al Departamento de Operaciones de la Financiera, solicitando la regularización del adeudo de la parte reclamante por la cantidad de ******CANTIDAD.*** €, y asumiendo la Financiera, por tanto, el quebranto patrimonial de la operación fraudulenta.

- En atención al deseo manifestado por la parte reclamante de dar de baja su Tarjeta, el pasado 20 de enero de 2025, sus datos constan bloqueados en los sistemas de la Financiera y solo serán tratados según lo dispuesto en el artículo 17.3.e del RGPD.

Y aportan la siguiente documentación relevante:

- **Documento N.º 2**, copia de la solicitud de la Tarjeta junto con el Contrato de TC
- **Documento N.ª3**, Informe elaborado por la Delegada de Protección de Datos en relación con el Requerimiento de Información EXP202500101 de la AEPD, recogiendo con más detalle lo expuesto en el escrito de alegaciones.
- **Documento N.º 5**, copia de la comunicación enviada a la dirección de correo electrónico del Reclamante facilitada el 25 de noviembre de 2024 informando de todos los hechos sucedidos, del bloqueo de sus datos personales y de que

la Financiera ha asumido íntegramente el quebranto patrimonial producido como consecuencia de la suplantación de su identidad con su Tarjeta El Corte Inglés.

TERCERO: Con fecha 2 de marzo de 2025, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

1) Realizado requerimiento de información a la entidad reclamada, con fecha de 15 de septiembre de 2025 se recibe en esta Agencia escrito donde la reclamada hace las siguientes manifestaciones:

1. **Procedimiento de identificación del cliente a través del canal IVR**: el asistente virtual identifica al cliente solicitándole una serie de datos y, en cada petición, le ofrece, además del intento inicial, dos intentos adicionales para que el cliente facilite el dato que se le requiere. Si el cliente no colabora o no se le entiende, el asistente redirige la llamada a un agente humano. Existen dos modalidades de identificación: mediante usuario y contraseña de su área privada o facilitando el número de DNI, código postal y teléfono asociado al contrato de la tarjeta. En el caso de la parte reclamante, fue este último el utilizado.

2. **Procedimiento de modificación de datos a través del canal IVR**: cuando el cliente solicita modificar su teléfono o su correo electrónico, el proceso es el siguiente:
   a. Advertencia de envío de OTP: el asistente remite al cliente un SMS o correo electrónico con la clave One Time Password (OTP) para registrar la modificación de sus datos de forma cruzada: si el cliente desea cambiar el teléfono, la OTP se envía a su correo electrónico; en cambio, si desea modificar el correo electrónico, la OTP se remite por SMS a su teléfono. En el caso [de la parte reclamante], según la transcripción recogida de la llamada del IVR y los logs de la herramienta de gestión de identidades de la Financiera, el primer cambio de datos se ejecutó a través de una clave OTP enviada a su correo electrónico de contacto.
   b. Petición nuevos datos: el asistente solicita el nuevo número teléfono o dirección de correo electrónico que el cliente desea asociar a su tarjeta. Si son los mismos anteriormente grabados no hay cambio, por el contrario, si se desea modificar alguno de estos datos, se solicita el nuevo teléfono o correo electrónico que desea asociar. La OTP se envía de forma cruzada, es decir, si se desea cambiar el número de teléfono, la OTP se envía al correo electrónico y viceversa.

Según consta en el escrito, para cada uno de los pasos guiados del asistente virtual, si el asistente no logra interpretar correctamente los datos que debe

facilitar el cliente, o se produce un error en la actualización de los datos, la comunicación se deriva a un agente humano.

Añaden que estos procedimientos han sido desarrollados y diseñados teniendo en cuenta el estado de la técnica en cada momento y los medios y criterios de identificación a través de canales digitales, que se corresponden con los análisis de riesgos y medidas de seguridad implantadas por parte de la Financiera, descritos más adelante. Sin embargo, y como parte del plan actual de control y mitigación de riesgos desarrollado por la Financiera, a partir de esta incidencia se ha decidido suprimir el servicio de identificación y modificación de datos en el entorno virtual, debido al notable incremento y la creciente sofisticación del fenómeno de la suplantación de identidad en el último tiempo, y se está rediseñando dicho proceso y estableciendo nuevos controles para tratar de evitar, dentro de su esfera de actuación, que se produzcan tales situaciones.

Vuelven a destacar la conclusión a la que llegó la Unidad de Prevención del Fraude *"el correo electrónico personal del Reclamante tuvo que ser interceptado, bien por estar su correo electrónico vulnerado o bien facilitarse (la OTP) al suplantador a través de engaño o artificio similar (phishing), así como, los datos personales del Reclamante tales como nombre, apellidos, DNI, número de teléfono y código postal debían de ser conocidos por el suplantador, pues son datos requeridos a diferentes niveles para la verificación de cualquier cambio y/o modificación de los datos personales contenidos en las fichas de clientes."* Ya referida en el escrito de alegaciones al traslado de la reclamación.

Añaden que la investigación que llevó a cabo la Unidad de Prevención del Fraude de la Financiera determinó que la cuenta de correo electrónico de la parte reclamante había sido intervenida en varias ocasiones antes de los hechos denunciados puesto que la búsqueda en el sitio web "***(…)***" arrojó dos resultados. (…)

1. **Procedimiento de cambio de contraseña**: declaran que este se hizo a través del Área Privada de la parte reclamante del sitio web la financiera. El procedimiento según sus manifestaciones es:
   a. Debe introducir de forma obligatoria su número de DNI y su clave personal de acceso de seis dígitos.
   b. En caso de no recordar la clave, el cliente puede optar por seleccionar la pestaña "He olvidado mi contraseña". Al elegir esta alternativa, la herramienta vuelve a solicitar el número del DNI del cliente y requiere que valide su identidad, introduciendo en primer lugar el número de teléfono de contacto asociado a su tarjeta. Se verifica, y en caso de ser coincidente, se le envía al mismo una clave OTP que recibe a través de un SMS. Posteriormente, el cliente introduce la clave OTP en la pantalla habilitada al efecto del formulario web para completar el proceso de identificación, tras lo cual queda habilitado para modificar su contraseña desde su Área Privada.

1. **Cronología del cambio de datos, canal, dato modificado y verificación para el cambio**: detallan lo siguiente y adjuntan el documento 4 señalado más abajo:

- 12/10/2024 10:07: canal telefónico IVR, cambio número de teléfono, envío OTP a la dirección de correo electrónico.
- 12/10/2024 10:08: canal web/área cliente, cambio contraseña, envío OTP al núm. Móvil.
- 12/10/2024 10:09: aviso a la parte reclamante de inicio de sesión desde nuevo dispositivo
- 14/10/2024 07:20: canal web/área cliente, cambio email, envío OTP al núm. Móvil.
- 14/10/2024 07:21: canal web/área cliente, cambio de domicilio, no hay OTP de verificación
- 22/10/2025 21:09: canal web/área cliente, cambio cuenta bancaria, envío OTP al núm. Móvil.

1. **Medidas implementadas como consecuencia de la presente incidencia**

a. Supresión de la posibilidad de cambio de número de teléfono o email asociado al contrato a través del canal telefónico, tanto mediante agente virtual (IVR) como por agente humano.

b. Supresión de la funcionalidad de cambio del número de teléfono o de la dirección de correo electrónico a través del Área Privada de la web y de la aplicación móvil de la Financiera. Como consecuencia de ello, la Financiera está en proceso de redefinir los nuevos procesos de cambio de datos en canales no presenciales.

c. Intensificación de los controles de monitorización por parte del área de Fraude, mediante la retroalimentación de la herramienta con nuevas reglas de pago seguro. A tales efectos, tal y como se señaló en la manifestación Sexta, la Financiera ha reforzado la herramienta de fraude (que actualmente cuenta con más de ciento veinte (120) reglas de análisis para prevenir este tipo de situaciones), entre las que se destacan las medidas de monitorización sobre el proceso de autenticación. En particular, sobre este último punto, se ha reforzado el seguimiento del log de autenticación, del envío de la clave OTP y del alta y modificación de contraseña a través del Área Privada del cliente.

d. Se han potenciado las campañas de comunicación a los clientes y empleados, en aras de concienciar y advertir sobre los potenciales riesgos de suplantación de identidad, así como para informar sobre las medidas a adoptar para evitar este tipo de situaciones

2) Se comprueba que, con fecha de 30 de enero de 2026, que, una vez cambiado el teléfono por parte del suplantador, se pueden cambiar a través del Área de Cliente: la contraseña, el domicilio y la cuenta bancaria asociada al contrato. Por el contrario, se ha verificado en el momento de esta comprobación que, para cambiar el número de teléfono o la dirección de correo electrónico, es obligatorio presentarse físicamente en el departamento de Atención al Cliente de uno de sus centros comerciales.

3) Requerida información adicional a la entidad financiera, en escrito de alegaciones recibido con fecha de 16 de febrero de 2026, la entidad Financiera viene a realizar las siguientes manifestaciones relevantes:

- Las claves de un solo uso (OTP) representan un método de autenticación altamente seguro, reconocido por la normativa europea, incluyendo el Reglamento eIDAS sobre firma electrónica, como herramienta válida para verificar la identidad de los usuarios.
- El protocolo que sigue el agente humano al que se deriva en caso de solicitar el cambio de número de teléfono o dirección de correo electrónico por el canal telefónico sigue el mismo protocolo que el canal IVR que dio lugar a la presente reclamación. No obstante, señalan, que se ha suspendido temporalmente la gestión de modificaciones de los datos de contacto de los clientes —específicamente el correo electrónico y el número de teléfono— tanto a través del canal telefónico, ya sea por la IVR como por agente humano, como desde el área de Cliente de la web o app de Financiera. En estos casos, la gestión es llevada a cabo por personal cualificado del SAC, quien solicita el documento de identidad del cliente para identificarlo antes de proceder a cualquier cambio, garantizando así que las modificaciones se realicen en condiciones seguras y controladas.
- Se mantienen implementados controles estrictos, medidas preventivas y un sistema de monitorización continua mediante su motor de detección de fraude transaccional, que permite identificar y mitigar riesgos de manera proactiva. Según informan, este mecanismo dispone de más de 120 reglas de denegación, de las cuales, 30 reglas basadas en el cambio de número de teléfono, 10 reglas basadas en el cambio de correo electrónico, 7 reglas basadas en el cambio de domicilio y 40 reglas basadas en el cambio de dispositivo.

4) Analizada toda la documentación presentada por la entidad financiera, se comprueba que el suplantador consiguió cambiar el número de teléfono asociado al contrato de la parte reclamante a través del asistente virtual del canal telefónico. Para ello, el suplantador **debía tener acceso al buzón de correo electrónico de la parte reclamante ya que a este buzón se envió el código de verificación de la operación.**

Una vez cambiado el número de teléfono asociado al contrato de la parte reclamante al que se enviarían las contraseñas de un solo uso, el suplantador pudo modificar la contraseña de acceso, la dirección de correo electrónico, el domicilio y la cuenta bancaria, a través del Área de Cliente del sitio web de la entidad financiera. Para la verificación de estas operaciones se remitieron códigos de confirmación por SMS (OTP) al número de teléfono que previamente había modificado el suplantador.

Cabe destacar que tanto para el cambio de contraseña como para el posterior acceso al Área de Cliente es necesario la introducción del NIF del titular del contrato, por lo que se desprende que **el suplantador además de tener acceso al buzón de correo electrónico también conocía el NIF** de la parte reclamante.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 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 Presidencia de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Seguridad del tratamiento

El artículo 32 del RGPD estipula 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.

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."

III
Conclusión

En el presente caso, los hechos que impulsaron el inicio de actuaciones previas de investigación conforme al artículo 67 de la LOPDGDD, tras la recepción de la reclamación por la AEPD, se referían al cargo no autorizado de ******CANTIDAD.*** € en su tarjeta vinculada al contrato que mantenía con la Financiera.

Durante las actuaciones previas de investigación se ha comprobado que el fraude se produjo mediante la modificación del número de teléfono móvil del reclamante, para lo cual se envió la OTP al correo electrónico asociado al contrato de tarjeta del reclamante. El correo electrónico personal del reclamante tuvo que ser interceptado o bien facilitarse la OTP al suplantador, así como el resto de los datos personales del reclamante, incluyendo su NIF.

Frente a este fraude, la entidad reclamada procedió a modificar sus datos personales, bloquear sus tarjetas y emitir nuevas tarjetas físicas. Así mismo, el día siguiente a la comunicación de estos hechos, la Unidad de Prevención del Fraude de la Financiera analizó el expediente, concluyendo que se había tratado de un fraude, y procediendo a la devolución de los importes sustraídos.

Asimismo, Financiera adoptó una serie de medidas para dificultar que situaciones futuras similares vuelvan a producirse, según el detalle que consta reproducido en el Antecedente Cuarto.

A este respecto, cabe citar la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 26 de septiembre de 2024, dictada en el asunto C-768/2021, analiza un supuesto de brecha de datos personales en el que una autoridad de control (el Comisionado para la Protección de Datos y la Libertad de Información del Estado Federado de Hesse, Alemania) decidió no imponer sanción atendiendo a las circunstancias del caso concreto. En dicha sentencia se afirma lo siguiente:

> *"37 A este respecto, ha de señalarse que el RGPD deja a la autoridad de control un margen de apreciación en cuanto a la manera en que debe subsanar la deficiencia constatada, puesto que el artículo 58, apartado 2, del mismo confiere a dicha autoridad la facultad de adoptar diversas medidas correctoras. Así, el Tribunal de Justicia ya ha declarado que la elección del medio adecuado y necesario corresponde a la autoridad de control, que debe realizar tal elección tomando en consideración todas las circunstancias del caso concreto y cumpliendo con toda la diligencia requerida su misión consistente en velar por el pleno respeto del RGPD (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C 311/18, EU:C:2020:559, apartado 112).*
> *38 Sin embargo, este margen de apreciación está limitado por la necesidad de garantizar un nivel coherente y elevado de protección de los datos personales mediante una aplicación rigurosa de las normas, como se desprende de los considerandos 7 y 10 del RGPD.*
> *(…)*

41 En consecuencia, no puede deducirse ni del artículo 58, apartado 2, del RGPD ni del artículo 83 de este la existencia de una obligación a cargo de la autoridad de control de adoptar, en todos los casos, cuando constate una violación de la seguridad de datos personales, una medida correctora, en particular una multa administrativa, siendo su obligación, en tales circunstancias, reaccionar adecuadamente para subsanar la deficiencia constatada. (…) En estas circunstancias, como señaló el Abogado General en el punto 81 de sus conclusiones, el autor de una reclamación cuyos derechos han sido vulnerados no dispone de un derecho subjetivo a que la autoridad de control imponga una multa administrativa al responsable del tratamiento.

(…)

43 A este respecto, no se excluye que, con carácter excepcional y habida cuenta de las circunstancias particulares del caso concreto, la autoridad de control pueda abstenerse de adoptar una medida correctora aunque se haya constatado una violación de la seguridad de datos personales. Tal puede ser el caso, en particular, cuando la violación constatada no haya persistido, por ejemplo cuando el responsable del tratamiento, que, en principio, había aplicado medidas técnicas y organizativas apropiadas en el sentido del artículo 24 del RGPD, haya adoptado, tan pronto como haya tenido conocimiento de dicha violación, las medidas adecuadas y necesarias para que la violación finalice y no vuelva a producirse, habida cuenta de las obligaciones que le incumben, en particular, en virtud de los artículos 5, apartado 2, y 24 del mencionado Reglamento.

44 La interpretación según la cual la autoridad de control, cuando constata una violación de la seguridad de datos personales, no está obligada a adoptar en todos los casos una medida correctora con arreglo al artículo 58, apartado 2, del RGPD se ve corroborada por los objetivos perseguidos por este artículo 58, apartado 2, y por el artículo 83 de dicho Reglamento, respectivamente.

45 Por lo que respecta al objetivo perseguido por el artículo 58, apartado 2, del RGPD, del considerando 129 de este se desprende que esta disposición tiene por objeto garantizar la conformidad del tratamiento de datos personales con dicho Reglamento y la regularización de las situaciones de incumplimiento de este para que se ajusten al Derecho de la Unión, mediante la intervención de las autoridades de control nacionales (sentencia de 14 de marzo de 2024, Újpesti Polgármesteri Hivatal, C 46/23, EU:C:2024:239, apartado 40).

46 De lo anterior se infiere que la adopción de una medida correctora puede, con carácter excepcional y habida cuenta de las circunstancias particulares del caso concreto, no imponerse, siempre que la situación de infracción del RGPD ya haya sido subsanada y que se garantice la conformidad de los tratamientos de datos personales con dicho Reglamento por su responsable y que tal abstención de la autoridad de control no menoscabe la exigencia de una aplicación rigurosa de las normas, tal como se ha recordado en el apartado 38 de la presente sentencia."

El TJUE reconoce en esta sentencia el margen de apreciación que tienen las autoridades de control para, en el ejercicio de sus funciones, desarrollar y optar entre los poderes atribuidos por el artículo 58 del RGPD, teniendo en cuenta las circunstancias del caso concreto y velando por el pleno respeto del RGPD. La consigna que debe regir siempre la actuación de una autoridad de control es asegurar un nivel alto de protección de los datos personales.

Así, cabe que, aun cuando se hubiera constatado o se tuvieran indicios de que se ha producido una vulneración en materia de protección de datos, las autoridades de control se abstengan de ejercitar sus poderes correctivos cuando esta presunta infracción hubiera sido subsanada y se garantice la conformidad de los tratamientos de datos personales con el RGPD.

Lo señalado por el TJUE en la sentencia antes citada, refuerza la idea de proporcionalidad de actuación de las autoridades de control que se recoge, con anterioridad a que fuera dictada la mencionada sentencia, en los artículos 65.4 y 65.6 de la LOPDGDD, por los que se permite a la AEPD, en atención a las circunstancias del caso concreto, la inadmisión a trámite o el archivo de reclamaciones, cuando, tras el traslado de las mismas al responsable del tratamiento, este demostrara haber adoptado medidas para el cumplimiento de la normativa aplicable.

En consecuencia, de conformidad con la STJUE de 26 de septiembre de 2024, en el asunto C-768/2021 y atendiendo a las singulares circunstancias que conforman este caso, en particular, la cancelación de las tarjetas, la modificación de las contraseñas del reclamante, así como el posterior bloqueo de todos sus datos, y la devolución total de los importes sustraídos, esta Agencia considera que no procede el despliegue de sus poderes correctivos previstos en el artículo 58 del RGPD.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Por lo tanto, de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos,
SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **FINANCIERA EL CORTE INGLES E.F.C., S.A.** y a la parte reclamante.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública. La publicación se realizará 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 Presidencia 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.

940-101025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos