- Expediente nº.: EXP202204668

RESOLUCIÓN DE RECURSO DE REPOSICIÓN

Examinado el recurso de reposición interpuesto por ANF AUTORIDAD DE CERTIFICACIÓN (en lo sucesivo, la parte recurrente) contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos de fecha 14 de abril de 2023, y en base a los siguientes:

HECHOS

PRIMERO: Con fecha 14 de abril de 2023, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente EXP202204668, procediéndose al archivo de las actuaciones previas de investigación.

Dicha resolución fue notificada a la parte recurrente en fecha 25 de abril de 2023 según consta en el acuse de recibo que figura en el expediente.

Dicha Resolución tenía como base los siguientes Hechos:

<<…PRIMERO: Con fecha de 21 de abril de 2022 la Directora de la Agencia Española de Protección de Datos acuerda iniciar actuaciones de investigación en relación con los hechos que se describen a continuación:

Como consecuencia de la comunicación de fecha 30 de marzo de 2022 efectuada por la SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL (en adelante SEDIA), en la que se ponen en conocimiento de esta Agencia sendos escritos de la ASSOCIACIÓ PER A LA DEFENSIÓ DE L'ADMINISTRAT I EL CONTRIBUENT (ADAC) y de ANF AUTORIDAD DE CERTIFICACIÓN (ANF AC), en los que se relatan presuntas irregularidades relacionadas con la expedición de certificados electrónicos cualificados por parte de prestadores de servicios de confianza.

Se referencian las prácticas llevadas a cabo por diversas entidades consistentes en la instrumentalización de certificados electrónicos cualificados para el acceso no autorizado a sedes de la Administración Pública y la obtención de informes provenientes de las mismas, tal como antecedentes penales, declaraciones tributarias, información de la Seguridad Social e información de la Central de Información de Riesgos del Banco de España (CIRBE).

Se insta la apertura de actuaciones de investigación por la necesidad de analizar las implicaciones en materia de protección de datos personales y seguridad de la información, en orden al esclarecimiento de los hechos denunciados.

Reclamado: CIRBOX TECNOLOGÍA Y SEGURIDAD, S.L. con NIF B88571310.

Hechos según manifestaciones de la parte reclamante:

La SEDIA da traslado de las reclamaciones presentadas por ANF AC y ADAC que fueron dirigidas a ese organismo. En ellas se manifiesta un posible supuesto uso fraudulento de certificados electrónicos para acceder y vender la información personal de terceros (los titulares de los certificados) mediante la utilización de la plataforma CIRBOX (cuyo responsable es CIRBOX TECNOLOGÍA Y SEGURIDAD, S.L., en adelante CIRBOX).

Indican que con la instrumentalización de certificados electrónicos cualificados realizan de facto la venta a terceros de información privada y confidencial de ciudadanos y empresas. Se indica que los certificados podrían haber sido expedidos sin conocimiento de los titulares, pudiendo acceder con ellos a información relativa a sus titulares de diferentes Administraciones Públicas.

Aportan un enlace a un video sobre el funcionamiento de la plataforma CIRBOX, en el que se aprecia que el cliente de la plataforma (normalmente una empresa) debe introducir el número de teléfono móvil y la dirección de correo electrónico de la persona de la que se van a obtener los datos (titular de los datos, en adelante usuario final).

Los reclamantes ponen de manifiesto que el cliente de la plataforma podría registrar su propio número de teléfono en lugar del teléfono del usuario final, e igualmente con la dirección de correo electrónico, y de esta forma acceder a los datos sin conocimiento de su titular, el usuario final.

Manifiestan haber realizado pruebas registrándose como cliente de la plataforma y de tres solicitudes culminadas (relativas a dos personas distintas) se introdujo la misma dirección de correo electrónico como dato de los usuarios finales, que CIRBOX debería tener identificada como la de su cliente, y un mismo número de teléfono móvil para todas ellas.

Se solicitó un segundo informe de renta respecto a una de esas personas, cuya solicitud resultó cancelada por CIRBOX, que alegó como motivo que se había repetido el correo electrónico y el teléfono móvil de solicitudes anteriores.

Se realizó una solicitud a nombre de un nuevo usuario final, aportando el DNI de otra persona, lo que fue detectado por CIRBOX cancelando la solicitud, comunicando el cese de la relación y cancelando el acceso a la plataforma.

Indican que no existe o no se da a conocer la política de privacidad del servicio, que no se suscribe contrato de encargado del tratamiento, que no se informa al usuario final del tratamiento de sus datos personales, que no cuentan con el consentimiento explícito del usuario y que los informes pueden ser descargados cuantas veces se desee.

Fecha en la que tuvieron lugar los hechos reclamados el 7 de marzo de 2022.

SEGUNDO: 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 los poderes de investigación otorgados a las autoridades de

control en el artículo 57.1 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:

ENTIDADES INVESTIGADAS

Durante las presentes actuaciones se han investigado las siguientes entidades:

CIRBOX TECNOLOGÍA Y SEGURIDAD, S.L. con NIF B88571310.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

PUNTO 1. Se ha realizado una inspección presencial a CIRBOX TECNOLOGÍA Y SEGURIDAD, S.L. (CIRBOX), entidad responsable de la plataforma CIRBOX. Durante la inspección sus representantes manifestaron lo siguiente:

«CIRBOX es una sociedad limitada con un volumen de ventas de unos 25000 euros anuales y 5 empleados, que fue creada en 2020, si bien empezó realmente su actividad en 2022.

Ofrece un servicio SaaS (Software as a Service) mediante la plataforma CIRBOX, disponible mediante acceso web y API para los clientes que la contratan. Esta plataforma permite a los clientes de CIRBOX la obtención de informes que emiten las distintas Administraciones Públicas a sus titulares, personas físicas y jurídicas, a solicitud de estos. Los informes para personas físicas son los siguientes: Informe de vida laboral de la Seguridad Social, Informe de la Central de Información de Riesgos del Banco de España (CIRBE), Informe de renta y modelo 347 de la AEAT.

El servicio está ideado principalmente para grandes empresas que ofrecen financiación a sus clientes [usuarios finales] en la comercialización de sus productos, y que, para el estudio de esta financiación, solicitan a sus clientes documentación como los informes citados. Mediante la plataforma CIRBOX, los informes son obtenidos directamente de las Administraciones Públicas utilizando un certificado digital del titular de los datos, por lo que se asegura su autenticidad. No obstante, se establece la obligatoriedad a los clientes de CIRBOX de informar a sus clientes (en adelante usuarios finales) de que pueden ser ellos mismos los que gestionen directamente la solicitud de sus informes ante las administraciones Públicas, por sus propios medios, para proceder a su entrega en papel u otro formato, o bien opcionalmente autorizar el servicio de CIRBOX de obtención de informes mediante certificado digital. CIRBOX pacta con cada cliente en particular la información que se debe incluir en sus argumentarios de venta utilizados por sus gestores.»

«Los certificados digitales de los usuarios finales, utilizados para la obtención de los informes mediante la plataforma CIRBOX, son emitidos exprofeso para ello, por lo que pueden considerarse certificados de un solo uso, siendo este uso única y exclusivamente la solicitud de emisión de los informes requeridos de las Administraciones Públicas. Hay que precisar que, por motivos técnicos, para la obtención de algunos informes como los de la CIRBE, se necesita utilizar el certificado dos veces, por la propia forma de funcionamiento de ese organismo. Además los días festivos y fines de semana la CIRBE no presta servicio, por lo que, unido a posibles

fallos de disponibilidad, la obtención de un informe se puede demorar varios días, por lo que los certificados digitales se emiten con un periodo de validez de una semana. Una vez expirado el certificado, a la semana de su emisión, es imposible su utilización.

Existen dos tipos de perfiles de acceso a la plataforma para los clientes de CIRBOX:

- Perfil operador, que únicamente permite gestionar solicitudes de informes, al objeto de registrarlas y consultar las pendientes, pero sin visualizar los informes una vez obtenidos.
- Perfil supervisor, que puede tanto solicitar como ver los informes.

De forma habitual, y según sus necesidades, se crea a los clientes un solo acceso como supervisor a la plataforma CIRBOX y varios accesos como operadores, para limitar al máximo la visibilidad de los informes por parte de los empleados del cliente que no lo necesiten para la realización de sus funciones.

El REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante Reglamento eIDAS) les obliga a cumplir con tres requisitos imprescindibles para la emisión de un certificado digital:
- Que el usuario acredite capacidad de representación: para una persona física mediante su documento de identidad (DNI o NIE), para una persona jurídica mediante poder de representación.
- Una fe de vida que acredite de la identidad del solicitante.
- La acreditación de la voluntad inequívoca del solicitante de que quiere el certificado.

Por ello CIRBOX tiene implementadas en su proceso las siguientes medidas:
- Recoge copia del documento de identidad (DNI o NIE) del usuario final, que le es entregada por el cliente de CIRBOX.
- CIRBOX delega en su cliente (que ejerce de Punto de Verificación Presencial o PVP) la acreditación de la identidad del usuario final, remitiendo a CIRBOX un certificado de identificación del solicitante. Para ello CIRBOX como Autoridad de Registro (RA) firma un acuerdo de PVP con su cliente, que se compromete a la verificación de la identidad del usuario final según los criterios establecidos en el Reglamento eIDAS.
- CIRBOX recoge la aceptación del usuario final utilizando los datos de contacto que su cliente le facilita (dirección de correo electrónico y número de teléfono móvil), asegurado mediante un proceso en dos pasos que incluye la remisión de un SMS (mensaje corto) al móvil del usuario con una OTP (One Time Password o clave de un solo uso) que el usuario debe introducir para la emisión del certificado digital. Se informa al usuario tanto los términos y condiciones del servicio como la política de privacidad (ésta última en dos capas).»

«Además, tanto un representante legal del cliente de CIRBOX como los empleados del cliente a los que se autoriza a ejercer las labores de PVP firman un documento anexo al acuerdo de PVP denominado "Alta de personal interno para labores de PVP" en el que las personas que van a ejercer esas labores aceptan las siguientes instrucciones sobre el cumplimiento de las funciones de verificación presencial para la emisión de los certificados digitales:
- Identificar a los solicitantes de certificados digitales.

- Verificar la exactitud y autenticidad de la información suministrada por el solicitante (usuario final).
- Realizar el cotejo de las copias de la documentación respecto al original presentado para tramitar la formalización de los contratos de prestación de servicios de certificación con el solicitante.
- Entregar la documentación presentada por el solicitante a CIRBOX para que esta pueda autentificarla y archivarla.
- En su caso, informar a los solicitantes de la importancia y responsabilidad que implican los certificados digitales.
- Conocer y respetar lo dispuesto en el procedimiento de punto de verificación presencial y las políticas de certificación y CPS publicadas en la página web de la Autoridad de Certificación (CA) www.uanataca.es.»

«No existen más instrucciones sobre la forma de recoger los datos del número de teléfono móvil y la dirección de correo electrónico del usuario, datos que van a ser utilizados para la recogida de la autorización del usuario final en dos pasos, ya que cada cliente sigue su propio procedimiento dentro de sus líneas de negocio para recabar el consentimiento de los usuarios finales (sus clientes) para el tratamiento de estos datos y del resto de sus datos personales. Como se ha indicado, CIRBOX actúa como Autoridad de Registro (RA) y el cliente de CIRBOX como PVP que se encarga de recabar los datos, verificar su exactitud y comprobar la identidad del usuario final a los efectos de la emisión del certificado digital necesario para la obtención de los informes. Por la propia naturaleza del servicio de emisión de certificados, las entidades involucradas están sometidas a control.

Por otra parte está implementado un sistema para detectar que no se repita el teléfono móvil o la dirección de correo electrónico de los usuarios finales en diferentes solicitudes. También está establecido un límite máximo de dos solicitudes en curso para el mismo DNI. Además, un operador de CIRBOX realiza una serie de comprobaciones manuales sobre la solicitud antes de la emisión del certificado digital:
- Comprobación de que los datos de nombre y apellidos y número de DNI de la solicitud coinciden con los de la imagen del documento del DNI aportado, así como los del certificado de identificación y el propio certificado.
- Comprobación de que el DNI está en vigor.

Adicionalmente, para la efectiva prestación del servicio se requiere que el usuario final lo acepte mediante el procedimiento en dos pasos citado, así como que acepte que los informes van a ser entregados al cliente de CIRBOX. Los certificados se emiten por parte de la entidad UANATACA, SA como Autoridad de Certificación (CA), informándose también de ello al usuario.

La CA acepta y emite los certificados cuyas solicitudes le indica la RA que están bien. La CA audita previamente a las RA verificando que sus procesos de identificación de los usuarios titulares de los certificados son los correctos.»

«Durante el proceso el usuario final debe elegir el PIN del certificado para su emisión. Este PIN queda cifrado en los sistemas informáticos sin ser accesible por ningún empleado de CIRBOX, siendo utilizado automáticamente por el sistema al efectuar la solicitud de los informes a los organismos públicos.

Los informes se entregan exclusivamente al cliente de CIRBOX que los ha solicitado, no teniéndose acceso a los mismos desde CIRBOX o ningún otro cliente. Ningún empleado de CIRBOX tiene habilitado informáticamente el acceso a los contenidos de los informes. Por ello, solo pueden visualizar los datos y estados relativos a las solicitudes de los informes para efectuar las funciones que tienen encomendadas, pero no los informes. Los informes están disponibles 30 días para su descarga, y, transcurrido este tiempo se eliminan.

Hasta la fecha CIRBOX no realiza comprobaciones de identidad de los usuarios finales por medios remotos como videoconferencia o video-identificación, camino que apunta el art. 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.»

Consta adjunto al acta de inspección el modelo de contrato que CIRBOX suscribe con sus clientes para la prestación del servicio, que en el ANEXO II de Protección de Datos Personales cita a CIRBOX como encargado del tratamiento y a sus clientes como responsables del tratamiento. Se comprueba que se cita que se firma en cumplimiento de lo previsto en los artículos 28 y 29 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos (en adelante RGPD).

Constan adjuntos al acta de inspección el modelo de acuerdo de PVP y el modelo de certificado de identificación o prueba de vida. Se verifica que en el acuerdo de PVP consta que la emisión de un certificado digital requiere una verificación de la identidad del solicitante (Prueba de Vida) según el Reglamento eIDAS y que la identificación se realizará con personal interno y según los criterios establecidos en el citado Reglamento.

Consta adjunto al acta de inspección copia del modelo de documento "Alta de personal interno para labores de PVP". Se verifica que en el documento el personal dedicado a labores de PVP quedan informados de las instrucciones, y en concreto, de verificar la exactitud y autenticidad de la información que suministran, realizar el cotejo de las copias de la documentación respecto al original presentado, así como entregar la documentación a CIRBOX para que éste pueda autenticarla y archivarla.

También constan como instrucciones que deben conocer y respetar lo dispuesto en el procedimiento de PVP y las políticas de certificación publicadas en la página web de la autoridad de certificación UANATACA así como, en su caso, informar a los solicitantes de la importancia y responsabilidad que implican los certificados digitales.

Consta adjunta al acta de inspección copia de la Declaración de Prácticas de Certificación de UANATACA y del certificado ISO/IEC 27001.

Siendo confidencial el contenido del documento de la auditoría que UANATACA como CA les ha realizado, durante la inspección se extrae un resumen de conclusiones en el que se leen las calificaciones de "Conforme" en los capítulos de conocimientos y

procedimientos, así como que "el procedimiento cumple con lo establecido en la Declaración de Prácticas de Certificación de UANATACA".

Aportan certificación de que CIRBOX ha implementado y mantiene un Sistema de Gestión de Seguridad de la Información para los Sistemas de Información que soportan los procesos de negocio relacionados con la emisión de certificados digitales y notificaciones electrónicas, almacenar certificados digitales en la nube y obtener reportes informes de las administraciones públicas, de acuerdo con el estado de aplicabilidad vigente a la fecha de emisión del certificado (Primera emisión: 10/12/2019 y última 16/03/2021) cumpliendo los requerimientos del estándar ISO/IEC 27001:2013.

(…)

Tienen conocimiento de una denuncia presentada ante la SEDIA, que les ha realizado un requerimiento. Suponen que la reclamación presentada ante la Agencia Española de Protección de Datos puede provenir de los mismos reclamantes.

Constan adjuntas al acta de inspección copia de la querella presentada y copia del auto de incoación dictado por el juez.

<u>PUNTO 2.</u> En la inspección realizada se efectuaron las siguientes comprobaciones sobre el procedimiento de emisión de los certificados y la obtención de los informes de los organismos públicos utilizando la plataforma CIRBOX:

- Se ha comprobado que durante el proceso de solicitud de informe el cliente de CIRBOX debe adjuntar la imagen del DNI y el Certificado de autenticación del usuario final para que se habilite el botón de envío de solicitud.

- Se ha verificado que un operador de CIRBOX debe comprobar dicha documentación con los datos de la solicitud para validar la misma. Las comprobaciones del operador pueden arrojar como resultado la cancelación de la solicitud por los siguientes motivos, registrados en la aplicación: DNI caducado, DNI no corresponde a la solicitud, DNI no legible o no es DNI, identificación con datos incorrectos, identificación con problema en firma, identificación documento incorrecto, identificación no identifica al solicitante, Móvil o correo electrónico ya usado por otro.

- Se ha verificado que los datos de correo electrónico y teléfono móvil que se introducen durante el proceso de solicitud de informe se utilizan para solicitar la autorización del usuario final, informando durante el proceso de diferentes aspectos:
. En la cuenta de correo electrónico del usuario final consignada durante la solicitud de informe se recibe un correo con el texto "para continuar con la solicitud de sus informes haga clic en el siguiente enlace".
. En dicho correo aparecen los enlaces "Avisos legales" y dentro del texto del aviso legal un enlace a la "Políticas de privacidad".
. Accediendo al enlace de que dispone el correo para continuar con la solicitud de informe se verifica que se accede en la denominada landing page (o página de aterrizaje) para el usuario final, donde se le explica que el servicio de CIRBOX facilita la obtención de informes (se especifica el tipo de informe que han solicitado), que se obtendrán en su nombre y que para ello se emitirá un certificado digital para ese uso

exclusivo, a través de CIRBOX, informándose del destino del informe (cliente de CIRBOX que lo ha solicitado).
En esta página de landing se indica al usuario que debe solicitar, mediante el botón "enviar código", la remisión de un código que le llegará a su línea móvil (se le especifica el número de móvil) y que debe introducir el código recibido en su campo, así como elegir un PIN. Se verifica que efectivamente aparece un botón para solicitar el código y campos de introducción de texto, para el código que se reciba y para la elección del PIN. Figura así mismo información básica sobre protección de datos. En el texto de Información básica de protección de datos se indica que la finalidad es prestar al usuario los servicios ofrecidos a través de la plataforma CIRBOX, que se comunican datos para la emisión del certificado electrónico a UANATACA, como Autoridad de Certificación (AC), y al cliente de CIRBOX que haya solicitado el informe, y que les asiste el derecho de acceder, rectificar o suprimir los datos, así como otros de derechos reconocidos en las normativas de Protección de Datos. Se indica que para información adicional y detallada puede consultar la política de privacidad.
Se verifica la existencia en la página de landing de dos enlaces a "Condiciones del Servicio" y "Política de Privacidad" detallada, que se descargan durante la inspección.
. Se ha comprobado que al presionar el botón de "enviar código" se recibe un código en el móvil que se especificó como del usuario final. Se comprueba que introducido dicho código y elegido un PIN para el certificado, al finalizar el proceso de la pantalla de landing, en la dirección de correo especificada en el campo denominado "Correo electrónico para envío de informe", del cliente de CIRBOX, se recibe un aviso de que el informe solicitado puede ser accedido.

- Accediendo a la plataforma CIRBOX utilizando las credenciales de usuario que se utilizaron para crear la solicitud de informe, se comprueba que la solicitud se encuentra en estado "completada". Se comprueba la existencia de un botón de descarga del informe solicitado.

- Realizadas comprobaciones sobre las vistas y accesos a la plataforma CIRBOX disponibles para los empleados de CIRBOX, se verifica que los datos que se pueden visualizar son la fecha, la referencia de la solicitud, el nombre completo del usuario final, el CIF o NIF, el tipo de informe solicitado, y el estado de la solicitud (entre los estados se aprecian iniciada, pendiente cliente, cancelada, completada). No se encuentra ningún acceso al contenido de los informes.

- Se comprueba la existencia de solicitudes canceladas.

PUNTO 3. Durante las actuaciones de inspección se han identificado relevantes las siguientes referencias normativas:

- REGLAMENTO (UE) N o 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
En sus articulo 18 y 20, sobre infracciones y Potestad:
"2. Son infracciones muy graves:

b) La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre, señaladas en el Reglamento (UE) 910/2014 y en esta Ley, cuando ello afecte a la mayoría de los certificados cualificados expedidos en el año anterior al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este periodo es menor

3. Son infracciones graves:
b) Actuar en el mercado como prestador cualificado de servicios de confianza, ofrecer servicios de confianza como cualificados o utilizar la etiqueta de confianza «UE» sin haber obtenido la cualificación de los citados servicios.
d) No proteger adecuadamente los datos de creación de firma, sello o autenticación de sitio web cuya gestión se le haya encomendado en la forma establecida en el artículo 9.1.b) de esta Ley.
h) La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre, señaladas en el Reglamento (UE) 910/2014 y en esta Ley, cuando no constituya infracción muy grave.
[…]

Artículo 20. Potestad sancionadora.

La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial."

- Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.>>

SEGUNDO**:** La parte recurrente ha presentado en fecha 24 de mayo de 2023, en esta Agencia Española de Protección de Datos, recurso de reposición, en el que muestra su disconformidad con la resolución, reiterando los argumentos expuestos en su escrito de reclamación, indicando que: << *CIRBOX no recoge directamente los datos de los interesados, emplea empresas intermediarias que según contrato denomina Punto de Verificación Presencial "PVP". Las evidencias obtenidas identifican a UANATACA como el PCSC que al menos intervino en la emisión de los certificados aportados. UANATACA ha sido por tanto receptor de esa información personal sin contar con el consentimiento informado expreso del titular de los datos.*

Los PVP saben que están comprando información secreta de los interesados, no existe acreditación alguna que permita pensar que el PVP al recoger la información apercibió a los interesados del destino de la misma, y aunque lo hubiera hecho, se trata de tratamientos ilícitos.

El fin perseguido por CIRBOX acceder subrepticiamente a la información confidencial custodiadas por las AA.PP. y venderla, el de UANATACA elaborar y vender

certificados al objeto de poder suplantar la identidad de sus titulares, y presumiblemente el del PVP utilizar estos datos secretos para determinar la solvencia de determinadas personas.

En definitiva por mucho contrato de encargado del tratamiento que alegue CIRBOX que firma su cliente (PVP), CIRBOX está tratando los datos personales para fines propios, para desarrollar su objeto de negocio. En consecuencia, debe ser considerado responsable del tratamiento.

Pero es más, la única documentación obtenida de una relación real de un PVP con CIRBOX, acredita que no solo no se firma tal anexo, sino que no existe.

Es ineludible la obligación de realizar una evaluación de los riesgos que conlleva el tratamiento. Incluso si el responsable del tratamiento considera que dicho tratamiento no entraña probablemente riesgo.

CIRBOX, tiene entre otras obligaciones el nombrar un Delegado de Protección de Datos, que no lo tiene.

Pues bien, en la denuncia quedó demostrado que ese control no se ejerce, empezando por no comprobar la existencia e identidad del operador del Punto de Verificación Presencial (PVP), pues a pesar de haber pedido la documentación del DNI y poder de representación, se permite acceder a la prestación del servicio sin la verificación previa.

CIRBOX es responsable del tratamientos de datos realizados en su plataforma y el uso de los certificados por persona distinta a su titular es contrario a la legislación vigente.

Es evidente que los corresponsales del tratamiento no han desarrollado un procedimiento de consentimiento explicito, ya sea escrito o digital.

Solicita que se proceda al desarchivo de las actuaciones, e inicio del correspondiente procedimiento sancionador, dada la existencia de indicios de la comisión de infracciones en materia de protección de datos personales >>.

FUNDAMENTOS DE DERECHO

I
Competencia

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP) y el artículo 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

II

Contestación a las alegaciones presentadas

La parte recurrente solicita que se proceda al desarchivo de las actuaciones basándose, casi en su totalidad, en manifestaciones ya realizadas por el recurrente y que han sido investigadas por la AEPD, investigación tras la cual los hechos denunciados fueron desestimados en los Fundamentos de Derecho II y III ambos inclusive, de la Resolución recurrida, tal como se transcribe a continuación:

<<II
Licitud y seguridad del tratamiento

El artículo 6 del RGPD, bajo la rúbrica "Licitud del tratamiento", detalla en su apartado 1 los supuestos en los que el tratamiento de datos es considerado lícito:

"1. El tratamiento sólo será lícito si cumple al menos una de las siguientes condiciones:
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

A su vez, el artículo 6.1 de la LOPDGDD, indica, sobre el tratamiento de los datos personales basado en el consentimiento del afectado que: "1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen (…)".

Por su parte, seguridad del tratamiento, recogido en el artículo 32 del RGPD, establece que:

"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".

El Considerando 74 del RGPD establece:

"Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas."

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y

organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan 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, respectivamente.

En primer lugar, en relación con el artículo 6.1 del RGPD, la documentación que obra en el expediente no pone de manifiesto que la conducta de la entidad CIRBOX pueda ser contraria al principio de licitud.

La entidad CIRBOX utiliza certificados digitales para el acceso a las sedes electrónicas de las Administraciones públicas y que con relación a estos certificados digitales la entidad CIRBOX, responsable de la plataforma, actúa como Autoridad de Registro (AR).

Pues bien, una Autoridad de Registro (AR, en inglés RA) es una entidad que identifica de forma inequívoca al solicitante de un certificado. La Autoridad de Registro suministra a la Autoridad de Certificación los datos verificados del solicitante a fin de que la Autoridad de Certificación emita el correspondiente certificado y UANATACA actúa como Autoridad de Certificación (AC).

Debe significarse que una Autoridad de Certificación (AC) es una entidad de confianza responsable de emitir y revocar los certificados digitales utilizados en las transacciones y firmas electrónicas. Esta confianza se consigue gracias a la figura de la AC, que actúa como parte interviniente en la relación entre empresas o empresas y particulares. Así, cuando se realiza cualquier transacción entre dos partes, la AC otorga confianza a los documentos gestionados y firmados al no ser parte interesada.

Gracias a la infraestructura de claves criptográficas con las que cuenta una Autoridad de Certificación, se confía y garantiza la identidad del firmante así como el contenido de las transacciones realizadas.

Algunas de las funciones de la Autoridad de Certificación son: proporcionar servicios como la publicación de certificados, listas de certificados revocados, comprobación de validez de los certificados, etc. Además, la AC registra la fecha y hora exactas en las que se ha firmado electrónicamente un documento, lo que se conoce como sellado de tiempo.

Así mismo, las empresas clientes de CIRBOX actúan como Punto de Verificación Presencial (PVP) al objeto de acreditar la identidad del usuario final en la solicitud del certificado electrónico.

Respecto a la acreditación de la identidad del titular de los datos, se evidencia que existen los siguientes controles:

- CIRBOX firma un acuerdo de PVP con su empresa cliente.
- En estos acuerdos de PVP se estipula que la identificación se realizará con personal interno de la empresa cliente y según los criterios establecidos en el Reglamento eIDAS.
- En el acto de identificación se debe emitir un certificado, que es enviado a CIRBOX para acreditar la identificación, junto con una imagen del documento de identidad.
- Los empleados concretos del cliente que van a ejercer las labores de identificación de los titulares de los certificados digitales firman un documento donde quedan autorizados a ello e informados de las instrucciones para la identificación, incluyendo entre otras instrucciones la verificación de la exactitud y autenticidad de la información suministrada, y la realización del cotejo de las copias de la documentación respecto al original presentado.

Las empresas clientes firman un contrato de prestación de servicios con CIRBOX con anexo de Protección de Datos.

En el supuesto que nos ocupa, dentro del proceso de solicitud de certificados digitales e informes se utiliza el teléfono y la dirección de correo electrónico del usuario final, informándole por dichas vías tanto de los términos y condiciones del servicio como de la política de privacidad, ésta última en dos capas. Se informa así mismo de la emisión del certificado, indicando que va a ser utilizado con la única finalidad de obtener los informes y facilitárselos a la empresa que se los solicita, y de la autoridad de certificación (AC) que lo emite. Se recaba la aceptación para la emisión del certificado y los informes mediante un proceso con clave OTP dirigida al móvil del usuario final.

Por lo tanto, para que se produzca la apropiación de datos por suplantación de identidad, la entidad que ejerce de PVP debería incumplir sus compromisos y además introducir un número de móvil propio, en lugar del número del titular de los datos, para

recibir la clave OTP y terminar el proceso de aceptación, y una dirección de correo electrónico propia para recibir la información. CIRBOX tiene implementado un control "Móvil o Correo electrónico ya usado por otro" para evitar que se repitan estos datos en diferentes solicitudes y los propios reclamantes citan estos controles como impedimentos que han encontrado al intentar simular un posible fraude.

Otros controles de CIRBOX pueden arrojar como resultado la cancelación de la solicitud por los siguientes motivos, registrados en la aplicación: DNI caducado, DNI no corresponde a la solicitud, DNI no legible o no es DNI, identificación con datos incorrectos, identificación con problema en firma, identificación documento incorrecto, identificación no identifica al solicitante. Se ha verificado que existen solicitudes canceladas.

Sobre el plazo de conservación de los datos, en la política de privacidad recabada se especifica una semana para el certificado digital y un mes para los informes. Los representantes de la entidad han manifestado que el certificado se expide exclusivamente para la emisión de los informes solicitados y los informes se encuentran disponibles para su descarga durante el plazo de un mes exclusivamente para la empresa que los solicitó.

En segundo lugar, en relación con el artículo 32 del RGPD CIRBOX ha declarado que sus empleados no tienen acceso a los informes, solo al estado de las solicitudes, y realizadas comprobaciones en los sistemas de la entidad, no se ha encontrado evidencias de la existencia de acceso a los informes por parte de los empleados de CIRBOX.

Consta certificación de que CIRBOX ha implementado y mantiene un Sistema de Gestión de Seguridad de la Información para los sistemas de información que soportan los procesos de negocio para gestionar la emisión de certificados digitales, según estándar ISO/IEC 27001:2013. Consta así mismo Declaración de Prácticas de Certificación de UANATACA, Autoridad de Certificación.

En definitiva, se ha constatado la falta de indicios racionales de la existencia de una infracción en el ámbito competencial de la Agencia Española de Protección de Datos, no procediendo, en consecuencia, la apertura de un procedimiento sancionador.

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". Este principio se encuentra expresamente recogido para los procedimientos administrativos sancionadores en el artículo 53.2.b) de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las

Administraciones Públicas, que reconoce al interesado el derecho "A 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 caso, de las actuaciones realizadas y de la documentación obrante en el procedimiento no se infiere la existencia de una actuación infractora de CIRBOX en el ámbito competencial de la Agencia Española de Protección de Datos, por lo que procede el archivo de la reclamación>>.

III

La parte recurrente también solicita el desarchivo de las actuaciones sobre la base de dos cuestiones nuevas que no habían sido previamente denunciadas: que CIRBOX no tiene una evaluación de impacto de protección de datos (EIPD), ni delegado de protección de datos.

Pues bien, no fueron mencionadas en la reclamación inicial por lo que no corresponde resolver sobre las mismas en esta fase de revisión.

La parte recurrente no puede pretender que en fase de recurso se tengan en cuenta hechos que no manifestó en una fase procedimental anterior. La LPACAP dispone en su artículo 118 la siguiente regla procesal: "*No se tendrán en cuenta en la resolución de los recursos, hechos, documentos o alegaciones del recurrente, cuando, habiendo podido aportarlos en el trámite de alegaciones, no lo haya hecho. Tampoco podrá solicitarse la práctica de pruebas cuando su falta de realización en el procedimiento en el que se dictó la resolución recurrida fuera imputable al interesado*." Esta norma contiene una regla que no es más que la concreción positiva para el ámbito administrativo común del principio general de que la Ley no ampara el abuso del derecho (artículo 7.2 del Código Civil). Dicho principio tiene por finalidad, entre otros, impedir que resulte inútil el trámite de alegaciones y pruebas de los procedimientos de aplicación, como así resultaría si los interesados pudieran elegir, a su arbitrio, el momento en el que presentar pruebas y alegaciones, por cuanto que ello sería contrario a un elemental orden procesal.

IV

Respecto a lo alegado por la parte recurrente de la decisión de la Agencia Española de Protección de Datos de no iniciar el procedimiento sancionador no puede estimarse acorde ni proporcionada, se hace necesario recordar que el denunciante, "*incluso cuando se considere a sí mismo "víctima" de la infracción denunciada, no tiene un derecho subjetivo ni un interés legítimo a que el denunciado sea sancionado* (…) *El poder punitivo pertenece únicamente a la Administración que tiene encomendada la correspondiente potestad sancionadora –en este caso, la AEPD- y, por consiguiente, sólo la Administración tiene un interés tutelado por el ordenamiento jurídico en que el infractor sea sancionado*. En estos términos se ha pronunciado la Audiencia Nacional en su sentencia de 2 de junio de 2015, en la que recuerda que, de conformidad con la jurisprudencia del Tribunal Supremo (STS de 9 de junio de 2014), para lo que sí se reconoce legitimación al denunciante es "*para demandar el desarrollo de la actividad investigadora que resulte conveniente para la debida averiguación de los hechos que*

hayan sido denunciados, pero no para que esa actividad necesariamente finalice en una resolución sancionadora".

Corresponde a la Agencia Española de Protección de Datos ejercer los poderes de investigación regulados en el artículo 58.1 del RGPD, entre los que figura la facultad de ordenar al responsable y al encargado del tratamiento que faciliten cualquier información que requiera para el desempeño de sus funciones.

Correlativamente, el artículo 31 del RGPD establece la obligación de los responsables y encargados del tratamiento de cooperar con la autoridad de control que lo solicite en el desempeño de sus funciones. Para el caso de que éstos hayan designado un delegado de protección de datos, el artículo 39 del RGPD atribuye a éste la función de cooperar con dicha autoridad.

Del mismo modo, el ordenamiento jurídico interno también prevé la posibilidad de abrir un período de información o actuaciones previas. En este sentido, el artículo 55 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, otorga esta facultad al órgano competente con el fin de conocer las circunstancias del caso concreto y la conveniencia o no de iniciar el procedimiento.

En cualquier caso, los procedimientos se inician de oficio por la AEPD, que es quien determina la responsabilidad de los hechos constatados.

Por lo tanto, en lo que concierne a su pretensión con respecto al resultado del expediente mismo, la apertura de un procedimiento sancionador, se considera que carece de legitimación activa para ello.

En consecuencia, en el presente recurso de reposición, la parte recurrente no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

V

Debido a razones de funcionamiento del órgano administrativo, por ende, no atribuibles al recurrente, hasta el día de la fecha no se ha emitido el preceptivo pronunciamiento de esta Agencia respecto a la pretensión del recurrente.

De acuerdo con lo establecido en el artículo 24 de la LPACAP, el sentido del silencio administrativo en los procedimientos de impugnación de actos y disposiciones es desestimatorio. Con todo, y a pesar del tiempo transcurrido, la Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación, según dispone el art. 21.1 de la citada Ley. Por tanto, procede emitir la resolución que finalice el procedimiento del recurso de reposición interpuesto.

Vistos los preceptos citados y demás de general aplicación, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por ANF AUTORIDAD DE CERTIFICACIÓN contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 14 de abril de 2023, en el expediente EXP202204668.

SEGUNDO: NOTIFICAR la presente resolución a ANF AUTORIDAD DE CERTIFICACIÓN.

De conformidad con lo establecido en el artículo 50 de la LOPDPGDD, 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 LOPDPGDD, y de acuerdo con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer 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) 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 LPACAP. 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