- **Expediente N.º: EXP202207027**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes:

ANTECEDENTES

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:

Con fecha 30 de marzo de 2022, esta Agencia tuvo conocimiento a través de la comunicación efectuada por la Secretaría de Estado de Digitalización e Inteligencia Artificial (en adelante, SEDIA), en la que se hace saber a esta Agencia sendos escritos de la ASSOCIACIÓ PER A LA DEFENSIÓ DE L'ADMINISTRAT I EL CONTRIBUENT (en adelante, ADAC) y de ANF AUTORIDAD DE CERTIFICACIÓN (en adelante, 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 DEH NOTIFICACION ELECTRONICA HABILITADA S.L. con NIF B86198306 (en adelante, DEH) consistentes en la instrumentalización de certificados electrónicos cualificados para el acceso no autorizado a sedes de las Administraciones Públicas con el objetivo de la gestión de las notificaciones provenientes de las mismas.

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

Hechos según manifestaciones de la parte reclamante:

En las reclamaciones presentadas por ANF AC y ADAC ante la SEDIA se manifiesta un posible robo de información mediante el uso fraudulento de certificados electrónicos utilizando la plataforma CERTIBOX, de la entidad DEH, cuando el titular se presta a ceder el control de sus claves a DEH, y suplantación de identidad utilizando certificados electrónicos emitidos por la empresa UANATACA, SA, (en adelante, UANATACA) prestador cualificado en la emisión de certificados de firma electrónica.

Se indica que los certificados podrían ser expedidos sin conocimiento de los titulares, con deficiencias en la verificación de la identidad del solicitante, y perdiendo el titular el control de su certificado y por tanto de los posibles accesos a sus datos al incitarle a facilitar el PIN (clave) del certificado.

Aportan un informe de un detective privado contratado por ANF AC. Se indica en este informe que ANF AC prestador cualificado de servicios de confianza puede estar

sufriendo competencia desleal e intrusismo de terceros. El detective cita en el informe haber contratado la emisión de un certificado digital, a través de TECNICOS CONTABLES Y ASESORES, SL, (en adelante TCT).

Indica que en el documento a cumplimentar para la solicitud de emisión del certificado se autoriza el tratamiento de datos personales por parte de TCT como entidad encargada de verificar la identidad del solicitante, y a trasladar dicha verificación a UANATACA para la emisión del certificado, y a DEH para la prestación de servicios de la seguridad en torno a la identidad digital y gestión documental.

El detective manifiesta en su informe que se accede indebidamente a los datos ya que le han comunicado una notificación de la AEAT, que además constaba como notificada con anterioridad a la contratación. Manifiesta que sólo solicitó el certificado digital y que en ningún caso contrató el servicio de recogida de notificaciones electrónicas ni autorizó a utilizar el certificado para acceder a sedes de la administración pública y consultar sus buzones. El detective manifiesta en su informe que el 23 de febrero de 2022 a las 19:32h recibió de DEH un correo electrónico y un mensaje SMS comunicándole que había recibido una notificación administrativa. Manifiesta que el 24 de febrero a las 08:41h se recibió de TCT el reenvió de la notificación administrativa recibida el día anterior. Indica que puede observarse que la notificación recibida desde DEH y TCT es una notificación que ya le fue notificada el 8 de febrero (según impresión de pantalla de la AEAT que aporta), es decir, antes de la contratación, por lo que manifiesta como conclusión que se ha accedido indebidamente a sus datos personales.

Indica que se ha realizado todo ello utilizando un certificado electrónico cualificado que ha sido expedido sin que se haya utilizado un método de identificación válido, ya que TCT solo le pidió remitir copia del DNI y un *selfie* (autofoto), no realizándose identificación presencial.

Fecha en la que tuvieron lugar los hechos reclamados el día 23 de febrero 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 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.

Se constatan los siguientes extremos:

Sobre la emisión de certificados digitales y la identificación de los solicitantes.

Los representantes de DEH han manifestado lo siguiente:

El artículo 24 del 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, prevé expresamente que las Autoridades de Certificación deleguen en otras entidades el proceso de verificación de la identidad de los solicitantes de certificados digitales, y es en virtud de esta

posibilidad expresa de delegación por la que se produce la intervención de DEH en el proceso de emisión de certificados.

Esta delegación es doble: la Autoridad de Certificación delega en DEH algunas de sus facultades en orden a la verificación de la identidad de los solicitantes para que actúe como Autoridad de Registro y DEH, según permiten expresamente sus acuerdos con las Autoridades de Certificación con las que trabaja, delega a su vez parte de estas facultades en los denominados Puntos de Verificación Presencial o PVP.

Esta doble delegación es lo que permite a los solicitantes de certificados digitales, distribuidos por todo el territorio nacional, obtener tales certificados sin necesidad de desplazarse a la sede de la Autoridad de Certificación, que es quien va a emitir el certificado solicitado.

Precisión adicional: el proceso que a continuación se va a describir no se aplica en todas las emisiones de certificados digitales. Algunos de ellos se emiten a través del proceso de vídeo identificación, regulado por 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, en el que DEH no interviene como Autoridad de Registro, porque la propia naturaleza del sistema de video identificación no lo hace necesario.

No obstante, el proceso de emisión de certificados digitales, en la mayoría de los casos, sigue los requisitos impuestos de modo general por el artículo 7.1 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza:

- El PVP recibe del interesado su solicitud de emisión de un certificado digital y debe verificar presencialmente la identidad del solicitante mediante la exhibición de su DNI u otro documento válido acreditativo de su identidad en vigor.

- El PVP rellena y firma un documento, denominado IDT, mediante el que traslada a DEH dicha solicitud y en el que manifiesta haber verificado presencialmente la identidad del solicitante remitiéndolo a DEH junto con copia del DNI del solicitante (u otro documento identificativo válido en vigor).

- A la recepción de esta IDT, DEH, actuando como Autoridad de Registro de la Autoridad de Certificación, comprueba la validez de la documentación recibida.

- Efectuada y superada esta verificación, DEH remite a la Autoridad de Certificación la solicitud, para que se proceda a la emisión del certificado digital.

- La Autoridad de Certificación, tras efectuar sus propias comprobaciones acerca de la solicitud recibida, procede a emitir el certificado digital y a facilitar al solicitante un enlace para que, por una sola vez, el solicitante pueda descargarse el certificado obtenido.

El proceso que se acaba de describir se formaliza mediante tres documentos distintos:

- La IDT firmada por el PVP.

- La aceptación por el solicitante de las condiciones de servicio, porque DEH participa en el proceso de emisión debido a que el solicitante está interesado en contratar el servicio de vigilancia de notificaciones CERTIBOX. En virtud de esta aceptación, el solicitante acepta que el certificado que solicita se active en la plataforma CERTIBOX para que el servicio de vigilancia pueda tener lugar.

- La aceptación por el solicitante del contrato de emisión con la Autoridad de Certificación.

El flujo de datos en el proceso de emisión es, por tanto, la transmisión desde el PVP a la Autoridad de Certificación, a través de DEH, de los datos personales necesarios para la emisión del certificado digital y que son: el nombre y apellidos del solicitante; su número de DNI (o documento identificativo alternativo); copia de dicho DNI o documento identificativo alternativo; correo electrónico, en el que el solicitante recibirá el mensaje que le permitirá descargarse el certificado; y su número de móvil, ya que el proceso de formalización de la solicitud del certificado digital requiere del envío de un mensaje con una clave a dicho móvil.

Con relación a este flujo de datos, y como medidas adicionales de seguridad que garanticen la perfecta identidad entre quién afirma solicitar un certificado y la persona a quien se emite dicho certificado, el proceso de emisión debe cumplir dos requisitos adicionales:

- El móvil designado por el solicitante y en el que recibirá las claves que le permitirán completar el proceso de emisión del certificado debe ser único. Es decir, el sistema CERTIBOX no acepta que se designe un móvil que ya ha sido utilizado para emitir otro certificado digital.

- Recientemente, DEH exige además al solicitante que envíe una transferencia de un céntimo de euro a DEH bajo el concepto *“Emisión de certificado digital para el NIF xxxxx”*. Solo si el NIF del titular de la cuenta desde la que DEH recibe la transferencia coincide con el NIF del certificado solicitado se procede a la emisión del certificado.

Sobre el rol de TCT y las obligaciones contractuales.

De las manifestaciones de los representantes de DEH y de la documentación aportada se desprende lo siguiente:
TCT, como asesor fiscal que atiende los encargos que les hacen sus clientes, tiene un contrato firmado con DEH para la utilización de la plataforma CERTIBOX, contrato cuya copia aportan. Se verifica que en el contrato figura que TCT actúa para el servicio de CERTIBOX como responsable del tratamiento y DEH como encargado. En este documento figuran, entre otras estipulaciones, el objeto y la duración del contrato, la naturaleza de los tratamientos, el tipo de datos, las categorías de los interesados, que los datos se tratarán siguiendo instrucciones del responsable y que no se utilizarán para finalidades distintas, que únicamente se accederá a los datos cuando sea imprescindible para el servicio, garantías sobre el compromiso de confidencialidad de las personas involucradas, referencias a las medidas de seguridad, garantías sobre la posible subcontratación y que a la finalización se devuelven o destruyen los datos.

Por otra parte, el personal de TCT actúa como PVP de conformidad con lo previsto en los artículos 24 del reglamento 910/2014 y 7.1 de la Ley 6/2020, actuando en nombre

y por cuenta de DEH en su calidad de Autoridad de Registro. Para ello, TCT y DEH mantienen firmado un acuerdo de prestación de servicio de PVP.

Se verifica que en la estipulación Sexta de este acuerdo consta que a los efectos de la identificación DEH se establece como responsable del tratamiento y TCT actúa en calidad de encargado de tratamiento. En el acuerdo entre otras obligaciones del encargado consta que los datos se tratarán siguiendo instrucciones del responsable y que no se utilizarán para fines distintos, que únicamente se accederá a los datos cuando sea imprescindible para el buen desarrollo de los servicios, garantías sobre el compromiso de confidencialidad de las personas autorizadas para tratar los datos, referencias a las medidas de seguridad, garantías sobre la posible subcontratación y que a la finalización se devuelven o destruyen los datos.

De las manifestaciones de los representantes de DEH se desprende que, en resumen, el procedimiento que TCT sigue para el alta de los clientes en la plataforma CERTI-BOX, y que integra la emisión del certificado digital es el siguiente:

- TCT da de alta a sus clientes en la plataforma CERTIBOX y remite a DEH la IDT en la que manifiesta que ha verificado presencialmente la identidad de su cliente junto con la documentación necesaria para la emisión del certificado. Esta alta no implica que se inicie la vigilancia de las notificaciones de ese cliente, sino que la plataforma CERTIBOX envía automáticamente al correo electrónico del cliente de TCT un mensaje informándole que su asesor ha solicitado su alta en el servicio de vigilancia de notificaciones.

- El cliente de TCT debe aceptar esta alta, efectuar la transferencia del céntimo desde una cuenta cuyo NIF coincida con el del certificado que se solicita, aceptar las condiciones de servicio de DEH, que implican que quien va a gestionar sus notificaciones es el asesor que ha solicitado su alta, y completar el proceso de solicitud del certificado digital. Manifiestan que solo entonces se inicia la vigilancia de las notificaciones de ese cliente en particular, por su aceptación expresa, que solo él puede realizar. El cliente del asesor puede comunicar en cualquier momento su baja en el servicio de vigilancia.

Los representantes de DEH informan que los certificados y sus claves se almacenan cifrados y de forma separada utilizando dos servicios de almacenamiento, uno para certificados y otro específico para claves, y que el servicio de vigilancia de notificaciones, de forma totalmente automatizada, accede a ambos servicios de forma individual por cada certificado digital sometido a vigilancia, y solicita aisladamente el descifrado de la contraseña y acceso al certificado digital cifrado.

Indican que el servicio utilizado para las operaciones de cifrado y descifrado sólo es accesible desde los sistemas automatizados de la entidad y que con el resultado de las operaciones automáticas anteriores, el servicio de vigilancia accede a las distintas sedes electrónicas. Manifiestan que toda esta operación descrita se realiza en espacios temporales volátiles por lo que, al terminar la actividad, el servicio automatizado de vigilancia desecha la información y dichos datos volátiles desaparecen, permaneciendo, cifrados y custodiados en los servicios específicos.

DEH aporta un correo electrónico de fecha 23 de febrero de 2022 11:48h dirigido al detective con el Asunto: Notificación de contraseña de certificado digital, con el texto "Estimado usuario, La contraseña de instalación de su certificado digital es: "[…]". Requerida información sobre dicho correo los representantes de la entidad contestan que se trata de un recordatorio de la contraseña o PIN de instalación del certificado digital que se envía al titular con objeto de facilitar la instalación y uso del mismo. Es la contraseña que fue elegida por el titular en el proceso de alta y que puede utilizarla para realizar la instalación del certificado digital en su equipo, para el caso que desee utilizarlo por su cuenta. Viene acompañada por el PIN de revocación del certificado.

Se verifica que tanto la contraseña/PIN de instalación como el PIN de revocación se encuentran en claro (sin cifrar) en este correo electrónico. Aportan también copia de un correo de fecha 22 de febrero de 2022 remitido al detective en el que se comprueba figura el PIN de revocación en claro.

Se ha requerido a DEH que aporte información sobre el motivo por el cual se accedió y reenvió la notificación procedente de la AEAT, que ya había sido notificada en fecha 08/02/2022 (antes de la contratación de los servicios), relatada en informe del detective.

TERCERO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad DEH es una pequeña empresa constituida en el año 2011, y con un volumen de negocios de ***XXX*** euros en el año 2021.

CUARTO: Con fecha 14 de abril de 2023**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del Artículo 32 del RGPD y Artículo 6.1 del RGPD, tipificada en el Artículo 83.4 del RGPD y Artículo 83.5 del RGPD.

QUINTO: Notificado el citado acuerdo de inicio 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), la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba: << c*onformidad con la propuesta de sanción por infracción del artículo 32 RGPD. Esta parte, al amparo del artículo 85 de la Ley 39/2015 y aceptando la oferta efectuada en el acuerdo de iniciación, se conforma con la propuesta de sanción efectuada por infracción del artículo 32 RGPD, al haber remitido al detective denunciante la contraseña de su* certificado *digital sin encriptar, desistiendo expresamente de interponer recurso alguno frente a dicha sanción, asumiendo su responsabilidad, y procederá al pago de la misma en la cuenta corriente que se indica en el acuerdo de iniciación antes de la finalización del presente procedimiento. Este reconocimiento de responsabilidad se basa en un principio de lealtad hacia la Administración actuante, pues aun discrepando de los criterios que la han llevado a individualizar la sanción propuesta, que no han tenido en cuenta el carácter provocado de la infracción denunciada y la inexistencia de perjuicio efectivo alguno en materia de protección de datos, por cuanto no se ha podido señalar un solo caso en que la práctica, abandonada por mi representada hace más de un año, de remitir en claro a los solicitantes de certificados digitales la contraseña de su certificado, con la finalidad de facilitarles la descarga del mismo, se haya concretado*

en la producción de daño alguno; lo cierto es que dicha práctica, ya abandonada, generaba un riesgo potencial, que es el que lleva a mi representada a asumir su responsabilidad y conformarse con la sanción propuesta.

Disconformidad con la propuesta de sanción por infracción del artículo 6.1 RGPD. Aun no existiendo disconformidad con los hechos que, sobre esta supuesta infracción, se narran en el acuerdo de iniciación, esta parte no puede conformarse con la sanción propuesta, por entender que: - Los hechos narrados en el acuerdo de iniciación no son típicos. - La sanción propuesta vulnera la prohibición del non bis in idem. - No cabe exigir responsabilidad administrativa por unos hechos que la propia propuesta solo ha sido capaz de detectar que ocurrieron una vez, cuando tales hechos fueron intencionadamente provocados por el propio denunciante.

Posibilidad de acogerse a las reducciones previstas por el artículo 85 de la Ley 39/2015 respecto de uno solo de los hechos imputados.

Aceptar el reconocimiento de responsabilidad de mi representada respecto a la infracción del artículo 32 RGPD >>.

SEXTO: DEH procedió en fecha 26 de mayo de 2023 al pago anticipado de la sanción fijada en el acuerdo de apertura para la infracción del artículo 32 del RGPD con una reducción del cuarenta por ciento.

SÉPTIMO: Con fecha 8 de mayo de 2023, el instructor del procedimiento acordó practicar las siguientes pruebas: *<<1. Se dan por reproducidos a efectos probatorios las comunicaciones efectuadas por ASSOCIACIO DEFENSIO ADMINISTRAT I CONTRIBUENT y ANF AUTORIDAD DE CERTIFICACIÓN y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones previas de investigación que forman parte del procedimiento AI/00269/2022. 2.Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado, presentadas por DEH NOTIFICACION ELECTRONICA HABILITADA S.L., y la documentación que a ellas acompaña>>.*

OCTAVO: Con fecha 19 de octubre de 2023 se formuló propuesta de resolución, proponiendo que por la Directora de la Agencia Española de Protección de Datos**:**

<<PRIMERO: DECLARE la terminación del procedimiento EXP202207027, respecto del artículo 32 del RGPD, tipificada en el art. 83.4.a) del RGPD, de conformidad con lo establecido en el artículo 85 de la LPACAP, tras reconocer expresamente su responsabilidad y haber procedido al pago de la sanción en la cuantía de 30.000 € (treinta mil euros) haciendo uso de las reducciones previstas en el Acuerdo de inicio, lo cual conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad.

*SEGUNDO: ARCHIVE el procedimiento sancionador EXP202207027**,** respecto del artículo 6.1 del RGPD instruido a DEH NOTIFICACION ELECTRONICA HABILITADA S.L. con NIF B86198306, por falta del hecho infractor>>*

NOVENO: Notificada la propuesta de resolución, el día 19 de octubre de 2023, DEH no formuló alegaciones a la anterior.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO. - Con fecha 30 de marzo de 2022, esta Agencia tuvo conocimiento a través de la comunicación efectuada por SEDIA, de las prácticas llevadas a cabo por DEH consistentes en la instrumentalización de certificados electrónicos cualificados para el acceso no autorizado a sedes de las Administraciones Públicas con el objetivo de la gestión de las notificaciones provenientes de las mismas.

SEGUNDO. - Obra en el expediente que DEH ha expedido certificados de firma electrónica sin que se hubiera realizado la verificación presencial. Se realiza la emisión del certificado electrónico prescindiendo de la identificación del solicitante.

TERCERO. - Consta probado haber remitido DEH al detective la contraseña de su certificado digital en correo electrónico sin encriptar.

CUARTO. - Se constata en el correo electrónico de fecha 23 de febrero de 2022 11:48h dirigido al detective con el Asunto: Notificación de contraseña de certificado digital, con el texto *"Estimado usuario, La contraseña de instalación de su certificado digital es: "[…]"*, se verifica que tanto la contraseña/PIN de instalación como el PIN de revocación se encuentran en claro (sin cifrar).

QUINTO. - Obra en el expediente que para cumplir su encargo profesional el detective simuló una situación de extrema urgencia y remitiendo un DNI alterado por él, engañando a TCT para que alterara el proceso establecido de verificación presencial.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora 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
Obligación incumplida

Se imputa a la parte reclamada la comisión de dos infracciones por vulneración de los artículos 6.1 y 32 del RGPD.

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".

III

Artículo 85 de la LPACAP e infracción del artículo 32 del RGPD.

El artículo 85 de la LPACAP dispone:

"1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí.
Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.
El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

En el Antecedente sexto de esta resolución se recoge que DEH procedió en fecha 26 de mayo de 2023 al pago anticipado de la sanción fijada en el acuerdo de apertura para la infracción del artículo 32 del RGPD con una reducción del cuarenta por ciento. A tenor del artículo 85.3. de la LPACAP el pago anticipado de la sanción prevista provocó la terminación del procedimiento sancionador respecto a dicha infracción.

IV

Archivo del procedimiento en relación con el artículo artículo 6.1 del RGPD

El artículo 89 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su apartado primero y tercero dispone:

1.*"El órgano instructor resolverá la finalización del procedimiento, con archivo de las actuaciones, sin que sea necesaria la formulación de la propuesta de resolución, cuando en la instrucción procedimiento se ponga de manifiesto que concurre alguna de las siguientes circunstancias:*

a) La inexistencia de los hechos que pudieran constituir la infracción.

b) Cuando los hechos no resulten acreditados.

c)Cuando los hechos probados no constituyan, de modo manifiesto, infracción administrativa.

d)Cuando no exista o no se haya podido identificar a la persona o personas responsables o bien aparezcan exentos de responsabilidad.

e) Cuando se concluyera, en cualquier momento, que ha prescrito la infracción".

3. "*En la propuesta de resolución se fijarán de forma motivada los hechos que se consideren probados y su exacta calificación jurídica, se determinará la infracción que, en su caso, aquéllos constituyan, la persona o personas responsables y la sanción que se proponga, la valoración de las pruebas practicadas, en especial aquellas que constituyan los fundamentos básicos de la decisión, así como las medidas provisionales que, en su caso, se hubieran adoptado. Cuando la instrucción concluya la inexistencia de infracción o responsabilidad y no se haga uso de la facultad prevista en el apartado primero, la propuesta declarará esa circunstancia".*

En el presente caso, DEH alega *"Inexistencia de responsabilidad administrativa derivada de una infracción provocada por el denunciante. Aunque forma parte de la denuncia efectuada por el detective denunciante, no está de más recordar que la falta de verificación presencial de su identidad fue expresamente provocada por él, alegando ante TCT la existencia de una situación de suma urgencia que le hacía imprescindible disponer de un certificado digital de modo inmediato, excusando su falta de personación para que su identidad fuese verificada presencialmente alegando*

hallarse de viaje. Para preconstituir la prueba de la infracción que él mismo provocó, facilitó a TCT una copia alterada de su DNI con la finalidad de acreditar que dicha verificación presencial no se produjo. TCT, fiándose de las razones de urgencia alegadas por el detective denunciante, y confiando igualmente en que la documentación oficial que se le había remitido no había sido intencionadamente alterada, procedió a cursar ante DEH ONLINE su solicitud de certificado digital, ocultando a mi representada que había omitido el trámite de verificación presencial que exige el artículo 7.1 de la Ley 6/2020".

Pues bien, del escrito de la denuncia y de la diferente documentación de los agentes intervinientes en este proceso se desprende que para cumplir su encargo profesional el detective falseó su actividad, alegando razones de extrema urgencia y remitiendo un DNI alterado por él, engañando a TCT para que alterara el proceso establecido de verificación presencial.

Es de señalar que en el Auto de aclaración de la AN (sala de lo contencioso) de 22/12/2015, de complemento de la SAN de 19/10/2015 (Rec. 423/2014), indica que: *"Resulta aplicable a este respecto la doctrina establecida de forma reiterada por la doctrina del Tribunal Supremo, Sala Segunda, cuando trata el tema del delito provocado, teniendo en cuenta que los principios que rigen el proceso penal son de aplicación al procedimiento sancionatorio de infracciones administrativas"*.

Así, la sentencia del Tribunal Supremo de fecha 5 de octubre de 2004, y en relación con aquellas otras que se recogen en la misma, establece la doctrina en el sentido de que, en el delito provocado por los propios agentes, realmente no existe un delito sino la apariencia de tal, si bien es distinto cuando se está cometiendo la conducta delictiva, generalmente de forma continuada, y los agentes únicamente aportan la prueba de la existencia de un delito preexistente.

La actuación del detective privado siempre se enmarcará en aquellos casos en los que lo que se pretende es descubrir situaciones ya existentes. Existiendo sospechas fundadas de la comisión del hecho reprobable, se acudirá a los servicios del detective para constatar los hechos y obtener las pruebas necesarias para su aportación al proceso judicial.

En consecuencia, los mismos límites y requisitos que operan en el ámbito penal para la figura del agente provocador, deberán ser tenidos en cuenta por los detectives privados en sus actuaciones.

El objetivo o fin del investigador es precisamente descubrir situaciones ilícitas ya existentes. No se pretende, por tanto, provocar la comisión del hecho punible, sino poner al descubierto aquel que ya se está produciendo. Por tanto, la conducta del sujeto provocado sí debería ser merecedora de reproche cuando la actuación del tercero interviniente ha sido realizada en aras a descubrir una transgresión que se sabe cometida o en vías de comisión.

Numerosa jurisprudencia ha admitido la actuación del detective privado cuando ésta se ha limitado a interaccionar de manera imparcial, sin ninguna maniobra que supusiera la guía de la conducta del investigado hacia aquellas actuaciones interesadas, y sin influir en la intención ni el ánimo subjetivo del mismo. En esta línea

la Sentencia del Tribunal Superior de Justicia de Aragón, STSJ AR 606/2018, de 16 de mayo, en la que el TSJ declara que la simulación del detective para hacerse pasar por un cliente del investigado que realizaba actividades concurrentes por cuenta propia *"No se trató de una prueba inducida. El detective no provocó una actuación antijurídica del demandante, sino que fue un usuario más de sus servicios médicos, anunciados en internet y que este venía prestando anteriormente, limitándose a constatar cómo el actor estaba atendiendo médicamente a los pacientes que lo solicitaban en la citada consulta pública. Su intervención permitió acreditar que el accionante estaba vulnerando el pacto de no concurrencia que prohibía al demandante prestar servicios de cirugía estética para otras personas físicas o jurídicas durante la vigencia de su contrato con la empresa demandada*". Por lo tanto, de esta sentencia destaca el carácter objetivo de la intervención del detective, quien no provocó la actuación ilícita del investigado, sino que simplemente se limitó a obtener prueba de dichas prácticas.

Otro ejemplo lo encontramos en la sentencia de la Audiencia Provincial de Madrid, SAP Madrid 655/2016, de 29 de noviembre, en la que una empresa fabricante de software contrata los servicios de un detective privado para demostrar la venta de software sin licencia en una tienda de venta de ordenadores. El detective privado simula ser un cliente que adquiere un ordenador, y es el propio vendedor de la tienda el que se ofrece a instalar el programa sin la pertinente licencia de explotación. Confirma el tribunal que no estamos ante un delito provocado, ya que no se genera en el autor la voluntad de realizar el acto prohibido, sino que se trata de la obtención de pruebas de la comisión de un delito por parte de un sujeto que ya tenía el propósito de delinquir, y que ya venía realizando tal actuación con anterioridad a la intervención del investigador.

Este mismo criterio es el que aplica el TSJ Castilla-La Mancha en su STSJ CLM 1437/2019, de 3 de junio de 2019, en la que niega que la actuación del detective haya supuesto un "engaño", y aplica la doctrina establecida por el TS sobre la provocación: *"En cuanto al hecho de que en una de las ocasiones el trabajador se mostrara dispuesto a la prestación de un servicio de reparación previa petición de uno de los detectives, no podemos refrendar el criterio de la instancia de negar virtualidad a tal acontecimiento calificando de «engaño» la actuación investigadora. Por el contrario, ningún reproche cabe realizar a tal actuación, incluso aplicando al caso por su evidente similitud la doctrina penal del delito provocado, a cuyo tenor solo debe desecharse las consecuencias del acto si estas han sido provocadas por el agente investigador de forma tal que sin su intervención el hecho no hubiera tenido lugar".* Concluye pues el TSJ que la actuación del detective no provocó la comisión del ilícito, sino que simplemente se limitó a constatar su realización*: "Aplicando la anterior doctrina al caso que nos ocupa, resulta que el detective no provocó ninguna conducta que el trabajador no hubiera realizado de otro modo, sino que simplemente le planteó una demanda de servicios de las que el propio interesado ofrecía en internet como profesional, y venía realizando en los términos ya relatados. Nada se provocó, sino que se realizó una simple actuación de comprobación, frente a la cual el interesado no manifestó que no se dedicara a tal actividad, sino que «no sabía cuándo podría pasarse», ajustando la cita tras una nueva llamada".*

En conclusión, solamente podrá considerarse la prueba de la detective ilícita si en su actuación se produce un factor coactivo que desencadene el comportamiento transgresor del investigado. Si no existe tal acción provocativa, y la actuación del

detective simplemente ha servido para hacer aflorar, sin intimidación alguna, y con el objetivo de demostrar un comportamiento previamente existente, no nos encontraríamos ante una situación inadmitida sobre la libre determinación individual, que afecte a la validez de la prueba.

Equiparando el caso del detective al del agente provocador, y siguiendo la misma doctrina establecida por el Tribunal Supremo, no habría ningún reproche a la actuación de los Detectives Privados cuando operan con el objetivo de descubrir incumplimientos ya cometidos -o en vías de comisión-, porque en tales casos el detective no trata de provocar la comisión del hecho sancionable, sino de ponerlo al descubierto, y obtener pruebas de una actividad sobre la que se tienen ya fundadas sospechas.

En el presente caso, la intervención del detective es determinante para la comisión de la infracción administrativa (provoca la misma), y no sólo para su constatación (no resulta de la actuación del detective que sea preexistente). Por ello, es aplicable la doctrina de la provocación. y por lo tanto procede al archivo del procedimiento en relación con el artículo artículo 6.1 del RGPD por falta de hecho infractor a consecuencia de la provocación, ilícita obtención de la prueba etc. Se trataría de una actuación “irrelevante” desde la perspectiva del derecho administrativo sancionador.

Cabe concluir que conforme con los hechos y fundamentos de derecho anteriores procede el archivo del procedimiento sancionador por inexistencia de infracción, del artículo 6.1 del RGPD.

A la vista de lo expuesto la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DECLARAR la terminación del procedimiento sancionador respecto a la infracción del artículo 32 del RGPD, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: Respecto a la infracción del artículo 6.1 del RGPD, ACORDAR el ARCHIVO del procedimiento sancionador abierto frente a DEH NOTIFICACION ELECTRONICA HABILITADA S.L. con NIF B86198306, por falta del hecho infractor.

TERCERO: NOTIFICAR la presente resolución a DEH NOTIFICACION ELECTRONICA HABILITADA S.L. con NIF B86198306

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el

día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

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