apdcat
Autoritat Catalana de Protecció de Dades

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 49/2019, referente al Institut Enric Borràs de Badalona, dependiente del Departamento de Educación.

Antecedentes

1. En fecha 02/10/2019 el Área de Inspección de la Autoridad Catalana de Protección de Datos tuvo conocimiento de que, en fecha 19/09/2019, el medio de comunicación Business Insider había publicado la siguiente noticia referente a el Instituto Enric Borràs de Badalona (en adelante, el instituto): *"Un instituto catalán está usando reconocimiento facial para controlar la asistencia a clase, algo por lo que ha sido multado con 19.000 euros un colegio sueco".*

2. La Autoridad abrió una fase de información previa (núm. IP 262/2019), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador, la identificación de la persona o personas que pudieran ser responsables y las circunstancias relevantes que concurrían.

3. En esta fase de información, en fecha 08/10/2019, la Autoridad llevó a cabo un acto de inspección en las dependencias del instituto para verificar determinados aspectos relacionados con el sistema de reconocimiento facial del alumnado. En ese acto de inspección presencial, los representantes del instituto y del Departamento de Educación manifestaron, entre otros, el siguiente:

ÿ Que el sistema de reconocimiento facial estaba instalado desde el curso 2011-2012.

ÿ Que la finalidad perseguida era reducir el absentismo, mediante el control de la asistencia del alumnado, así como también informar de forma inmediata a las familias en caso de ausencia.

ÿ Que el sistema de reconocimiento facial sólo se aplicaba a los alumnos de 1º de ESO. En relación con los alumnos de otros cursos, el control de la asistencia se realizaba manualmente por parte del profesorado.

ÿ Que el sistema se suspendió hasta que la Autoridad se pronunciara. Este curso no se había iniciado el control de asistencia mediante reconocimiento facial. En la aplicación que gestiona el control de asistencia se empezaron a cargar los datos de varios alumnos (se suspendió antes de cargar todo el listado de alumnos), pero no llegaron a captarse los vectores de su cara.

ÿ Que el sistema permitía la identificación unívoca de las personas. El único problema de identificación que se detectó afectaba a dos personas gemelas, pero esto se va

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

resolver mediante la verificación de su identidad a través de su impronta dactilar (el resto de alumnos no debían identificarse a través de la huella).

- ÿ Que en el inicio del curso, el alumno se situaba delante de uno de los terminales, el cual recogía a los vectores de su cara haciendo diversos movimientos. A su vez, se asociaban a estos vectores al código del alumno (era un código aleatorio pero único para cada alumno) y al número de teléfono de los representantes legales.
- ÿ Que para controlar su asistencia, el alumno debía acercarse al terminal a través del cual se reconocía su identidad.
- ÿ Que cuando se detectaba que un alumno no había asistido al instituto, antes de generar el aviso (SMS), se verificaba si su familia había avisado de que no asistiría. De lo contrario, la persona que gestionaba la aplicación de control de asistencia accionaba la opción de enviar el SMS a sus tutores. En caso de que la familia contactara posteriormente con el instituto, indicando que el alumno sí que había ido, se comprobaba si había asistido presencialmente (se iba a buscar al alumno a la clase).
- ÿ Que a los alumnos de 1º de ESO, aparte del control de asistencia mediante reconocimiento facial, también se controlaba su asistencia a clase pasando lista.
- ÿ Que los datos necesarios para permitir el reconocimiento facial sólo se conservaban durante el curso de 1º ESO. En junio, al finalizar el curso, se eliminaban los datos.
- ÿ Que este tratamiento se fundamentaba en el consentimiento de los representantes legales de el alumnado.
- ÿ Que en caso de que el representante legal de algún alumno no otorgara el consentimiento o bien lo retirara con posterioridad, la asistencia de aquel alumno se verificaría manualmente. Ninguna persona se había negado a prestar su consentimiento, ni tampoco lo había retirado.
- ÿ Que con respecto al resto de alumnos del instituto, cuya presencia no se controlaba mediante reconocimiento facial, se avisaba a la familia telefónicamente si no asistía al instituto.
  Se habría actuado de la misma forma en caso de que no se obtuviera el consentimiento de los representantes legales de un alumno de 1º de ESO. Este aviso no era inmediato como en el caso del SMS que se enviaba respecto a los alumnos sujetos a reconocimiento facial.
- ÿ Que el derecho de información se hacía efectivo en la carta de compromiso educativo del instituto. En esta carta, no se habilitaba la posibilidad de que los representantes legales de los menores pudieran manifestar su negativa al tratamiento de datos biométricos con fines de control de la asistencia de sus hijos mediante reconocimiento facial.
- ÿ Que la empresa instaladora del sistema de reconocimiento facial, efectuaba el mantenimiento de este sistema e intervenía al inicio de curso para cargar los datos de los alumnos (asociar el código del alumno con el nombre).
- ÿ Que no se había suscrito con dicha empresa un contrato de encargado del tratamiento.
- ÿ Que este sistema permitió alcanzar la finalidad de reducir el absentismo escolar.
- ÿ Que se está valorando, para el próximo curso, otro sistema para controlar la asistencia sin reconocimiento facial.
- ÿ Que existe la predisposición de actuar conforme lo que prevé la normativa sobre protección de datos.

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Asimismo, en esa misma fecha, el personal inspector de la Autoridad verificó, entre otros, lo siguiente:

ÿ Que en el vestíbulo del instituto (planta baja) había instalados 2 terminales para permitir el control de la asistencia mediante reconocimiento facial. A su vez, se constató que en los pasillos de la 1ª planta también existían 2 terminales más, uno de los cuales también permitía el reconocimiento mediante la huella dactilar.

ÿ Que la aplicación que permitía gestionar el sistema de control horario era *"School Access Attendance Control",* la cual estaba instalada en un equipo informático ubicado en la secretaría del instituto. Se verificó que, en el sistema estaban los datos referentes al nombre y apellidos de varios alumnos, el grupo (clase), el ID de usuario y el móvil de su tutor. Se constató que los alumnos figuraban como ausentes y que todos forman parte de 1º de ESO. Por otra parte, se verificó que para acceder a dicha aplicación era necesario autenticarse mediante contraseña.

Finalmente, el personal inspector recogió la siguiente documentación, que fue entregada por los representantes de la entidad inspeccionada:

ÿ Copia de la carta de compromiso firmada por 2 representantes legales de alumnos de 1º de ESO (1 correspondiente al curso 2018-2019 y el otro 1 correspondiente 2019-2020).
ÿ Copia de la hoja de autorización de derechos de imagen firmada por 2 representantes legales (1 correspondiente al curso 2018-2019 y la otra 1 correspondiente 2019-2020).
ÿ Copia de las especificaciones técnicas del control de accesos mediante sistemas biométricos por reconocimiento facial y de dos presupuestos.
ÿ Diversa documentación relativa a los terminales de reconocimiento facial.

4. En fecha 29/11/2019, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el instituto, en primer lugar, por una presunta infracción prevista en el artículo 83.5.a), en relación con los artículos 5.1.a) y 9; en segundo lugar, por una presunta infracción prevista en el artículo 83.5.b), en relación con el artículo 13; y, en tercer lugar, por una presunta infracción prevista en el artículo 83.4.a), en relación con el artículo 28; todos ellos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27/4, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD). Este acuerdo de iniciación se notificó a la entidad imputada en fecha 12/12/2019.

5. En fecha 20/12/2019, el instituto formuló alegaciones en el acuerdo de iniciación.

6. En fecha 06/02/2020, la persona instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoridad Catalana de Protección de Datos amonestara al Instituto Enric Borràs de Badalona como responsable, en primer lugar, de una infracción prevista en el artículo 83.5.a) en relación con los artículos 5.1.a) y 9; en segundo lugar, de una

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

infracción prevista en el artículo 83.5.b) en relación con el artículo 13; y en tercer lugar, de una infracción prevista en el artículo 83.4.a) en relación con el artículo 28 todos ellos del RGPD. Esta propuesta de resolución se notificó en fecha 06/02/2020 y se concedía un plazo de 10 días para formular alegaciones.

7. El plazo se ha superado con creces y no se han presentado alegaciones.

Hechos probados

Del conjunto de las actuaciones practicadas en este procedimiento, se considerarán acreditados los hechos que se detallan a continuación.

1. El instituto Enric Borràs de Badalona trataba datos biométricos para controlar la asistencia al centro educativo de los alumnos de 1º de ESO.

A tal efecto, en el curso 2011-2012 instaló un sistema de reconocimiento facial para controlar la asistencia al centro educativo de los alumnos de 1º de ESO. Y, en relación a dos personas alumnas que eran gemelas, también controló su asistencia mediante la huella dactilar, dado que el sistema de reconocimiento facial no garantizaba su identificación unívoca.

Este sistema de control de la asistencia mediante el reconocimiento facial o la impronta dactilar se mantuvo activo hasta finalizar el curso 2018-2019. En fecha 08/10/2019, el personal inspector de la Autoridad verificó que este sistema ya no se utilizaba para controlar la asistencia de los alumnos de 1º de ESO (que constaban como ausentes).

2. En relación al control de la asistencia de los alumnos de 1º de ESO mediante su reconocimiento facial o la huella dactilar, el instituto no ha acreditado haber hecho efectivo el derecho de información a los representantes de los alumnos de 1º de ESO ESO durante el curso 2018-2019.

3. El instituto encargó en 2011 la instalación de dicho sistema de control de la asistencia a los alumnos de 1º de ESO a la empresa Xip Solucions, SL; así como su mantenimiento. El mantenimiento de este sistema implicaba que, al inicio de cada curso, el personal de esa empresa cargara los datos de los alumnos al sistema.

Este encargo no se formalizó en un contrato u otro acto jurídico escrito con el contenido que exige el artículo 28.3 del RGPD, y así lo admitió la persona representante del instituto en el acto de inspección presencial efectuado el 08/10/2019.

Fundamentos de derecho

1. Son de aplicación a este procedimiento lo que prevén la LPAC, y el artículo 15 del Decreto 278/1993, según lo que prevé la DT 2ª de la Ley 32/2010, de 1 de octubre, de la Autoridad

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Catalana de Protección de Datos. De conformidad con los artículos 5 y 8 de la Ley 32/2010, la resolución del procedimiento sancionador corresponde a la directora de la Autoridad Catalana de Protección de Datos.

2. La entidad imputada no ha formulado alegaciones a la propuesta de resolución, pero sí lo hizo en el acuerdo de iniciación. Al respecto, se considera oportuno reiterar a continuación lo más relevante de la respuesta motivada de la persona instructora a estas alegaciones.

2.1. Acerca de la noticia.

En el suyo de su escrito de alegaciones ante el acuerdo de iniciación, la entidad imputada manifestaba que las cifras publicadas en los medios de comunicación sobre el coste de la instalación del sistema de reconocimiento facial no eran precisas; que el sistema de reconocimiento fácil contribuyó a la mejora del absentismo; que no hubo *"mal uso intencionado de los datos de los alumnos";* y que ya se había acordado realizar un cambio de plataforma educativa para gestionar la asistencia.

Con carácter previo, procede dejar patente que el instituto no cuestionaba en su escrito de alegaciones ante el acuerdo de iniciación ni los hechos imputados, ni tampoco su calificación jurídica.

Dicho esto, en lo que se refiere al coste de la implantación o mantenimiento, ésta era una circunstancia irrelevante a efectos de determinar los hechos imputados y su calificación jurídica.

En relación a la falta de intencionalidad que invocaba el instituto, tal y como exponía la persona instructora en la propuesta de resolución, es necesario puntualizar que los tipos infractores imputados en el presente procedimiento sancionador, no exigen que concurra el elemento de la intencionalidad .

En lo referente a la mejora del absentismo, no se discute aquí si el sistema de reconocimiento facial (y dactilar) podía contribuir a alcanzar esta finalidad, sino que ésta podía obtenerse a través de otros medios menos intrusivos para los derechos de el alumnado de 1º de ESO, que no implicaran el tratamiento de categorías especiales de datos (como los datos biométricos).
Prueba de lo anterior es que respecto al resto de alumnos, su asistencia se controlaba por parte del profesorado en el instituto o en el aula; así como que la presencia en el aula del alumnado de 1º de ESO también se verificaba por el profesorado pasando lista (el sistema controvertido verificaba la presencia del alumnado en el instituto, pero no en el aula).

Cabe decir que la Autoridad ya se pronunció en el dictamen CNS 63/2018, en el sentido de considerar que el *"principio de minimización no se manifiesta sólo a la hora de optar por alternativas que no impliquen el tratamiento de datos personales , o de llevar a cabo el tratamiento de datos de forma que se empleen los datos mínimos indispensables, sino que también debe comportar que si se puede alcanzar una determinada finalidad sin tener que tratar datos de categorías especiales, ésta*

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

opción debe prevalecer ante otras opciones que sí impliquen el tratamiento de este tipo de datos."

Al margen de lo anterior, en el presente caso el tratamiento no se sustentaba en ninguna de las excepciones establecidas en el artículo 9.2 del RGPD, que deben concurrir cuando se traten categorías especiales de datos, como sucedía en el presente supuesto .

Por último, la decisión sobre el cambio de plataforma educativa para gestionar la asistencia del alumnado, vendría a corroborar que en el presente caso no era necesario el tratamiento de categorías especiales de datos para controlar la asistencia del alumnado que cursaba 1º de ESO.

2.2. Sobre las actuaciones realizadas.

Seguidamente, la entidad imputada informaba en su escrito de alegaciones ante el acuerdo de iniciación de que la implantación del sistema en este curso se suspendió inmediatamente a raíz de las noticias publicadas en los medios de comunicación; que se habían desmontado los terminales y toda la instalación; así como que el equipo informático de secretaría también estaba inhabilitado.

En este sentido, tal y como manifestaba la persona instructora en la propuesta de resolución, todas las medidas que el instituto informaba haber implementado a raíz de la inspección presencial efectuada en fecha 08/10/2019 por el personal inspector de la Autoridad, deben comportar que sea innecesario requerir ninguna medida correctora para corregir los efectos de las infracciones imputadas, tal y como se expondrá más adelante.

Asimismo, cabe destacar la buena predisposición del instituto para dar cumplimiento a la normativa sobre protección de datos, suspendiendo el sistema de reconocimiento facial/dactilar en cuanto se hizo pública una noticia que cuestionaba su adecuación al régimen de protección de datos datos; así como cuando a raíz de la intervención de la Autoridad en el marco de la fase de información, ha decidido desmantelar dicho sistema.

Por su parte, en su escrito de alegaciones ante el acuerdo de iniciación, el instituto también indicaba que ninguna familia *"ha manifestado formalmente ningún comentario por el uso del reconocimiento".* En este punto, basta con señalar que esta circunstancia no permitiría considerar que el tratamiento de categorías especiales de datos era lícito (artículo 9 RGPD).

3. En relación con los hechos descritos en el punto 1º del apartado de hechos probados, tanto relativos al reconocimiento facial como al reconocimiento a través de la huella dactilar, vulneran los principios de licitud (artículos 5.1.ay 9 RGPD).

El artículo 5.1.a) del RGPD regula el principio de licitud determinante de que los datos serán *"tratados de forma lícita (...)".*

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Por su parte, el artículo 9.2 del RGPD, referente al tratamiento de categorías especiales de datos, dispone que la prohibición de su tratamiento no se aplica si concurren una de las siguientes circunstancias:

"a) el interesado dio su consentimiento explícito para el tratamiento de dichas datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo conforme al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
c) el tratamiento es necesario para protegir intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos oa personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que las datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
g) el tratamiento es necesario por razones de un interés público esencial, en base al Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

e) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, en base al Derecho de la Unión o de los Estados miembros que establezca medidas
adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en base al Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado."

Tal y como indicaba la persona instructora, durante la tramitación de este procedimiento se ha acreditado debidamente la conducta descrita en el punto 1º del apartado de hechos probados (referentes al reconocimiento facial y al reconocimiento a través de la huella), la cual es constitutiva de una infracción prevista en el artículo 83.5.a) en relación con los artículos 5.1.a) y 9; ambos del RGPD.

El artículo 83.5.a) del RGPD, tipifica como infracción, la vulneración de los *"principios básicos del tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9",* entre los que se contempla la licitud del tratamiento de categorías especiales de datos (artículos 5.1.ay 9 RGPD).

Por su parte, esta conducta también se ha recogido como infracción muy grave en el artículo 72.1.e) de la Ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), en la siguiente forma:

"e) El tratamiento de datos personales de las categorías a que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que se dé alguna de las circunstancias previstas en el citado precepto y el artículo 9 de esta ley orgánica."

4. Con respecto al hecho descrito en el punto 2º del apartado de hechos probados, en lo referente a la vulneración del derecho de información, se debe acudir al artículo 13 del RGPD, que prevé que:

"1.Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que éstos se obtengan, le facilitará toda la información indicada a continuación:
a) la identidad y las datos de contacto del responsable y, en su caso, de su representante;

b) las datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento al que se destinan las datos personales y la base jurídica del tratamiento;

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de las datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país o organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y al medio para obtener una copia de las mismas o al hecho de que se hayan prestado.
2.Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan las datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:
a) el plazo durante el cual se conservarán las datos personales o, en cuanto no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a las datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, oa oponerse al tratamiento, así como el derecho a la portabilidad de las datos ;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar las datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y consecuencias previstas de dicho tratamiento para el interesado. (...)"

De conformidad con lo expuesto, tal y como indicaba la persona instructora, el hecho recogido en el punto 2 del apartado de hechos probados constituye la infracción prevista en el artículo 83.5.b) del RGPD, que tipifica como a tal efecto la vulneración de *"los derechos de los interesados a tenor de los artículos 12 a 22",* entre los que se encuentra el derecho de información de la persona interesada contemplado en el artículo 13 del RGPD.

A su vez, esta conducta se ha recogido también como infracción muy grave en el artículo 72.1.h) de la LOPDDDD, en la siguiente forma:

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

"h) La omisión del deber de informar al afectado sobre el tratamiento de sus datos personales de conformidad con lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 016/679 y 12 de esta Ley orgánica."

5. Con respecto al hecho descrito en el punto 3º del apartado de hechos probados, en lo referente a la falta de contrato de encargado del tratamiento, se debe acudir al artículo 28.3 del RGPD, que dispone lo siguiente:

"3.El tratamiento por el encargado se regirá por un contrato u otro acto jurídico conforme al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:
a) tratará las datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive respecto a las transferencias de datos personales a un tercer país oa una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b)garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o extienda sujetas a una obligación de confidencialidad de naturaleza estatutaria;
c) tomará todas las medidas necesarias de conformidad con el artículo 32;
d) respetará las condiciones indicadas en los aparta- dos 2 y 4 para recurrir a otro encargado del tratamiento;
e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que éste pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;
g) a elección del responsable, suprimirá o devolverá todas las datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de las datos personales en virtud del Derecho de la Unión o de los Estados miembros;
h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías,

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

> *incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.*
> *En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, a su juicio, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros. "*

De conformidad con lo expuesto, tal y como indicaba la persona instructora, el hecho recogido en el punto 3 del apartado de hechos probados constituye la infracción prevista en el artículo 83.4.a) del RGPD, que tipifica como tal, la vulneración de *"las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43",* entre ellas la prevista en el artículo 28 RGPD.

A su vez, esta conducta se ha recogido también como infracción grave en el artículo 73.k) de la LOPDDDD, en la siguiente forma:

> *"k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido que exige el artículo 28.3 del Reglamento (UE) 2016/679."*

6. El artículo 77.2 LOPDGDD dispone que, en el caso de infracciones cometidas por los responsables o encargados enumerados en el art. 77.1 LOPDGDD, la autoridad de protección de datos competente:

> *"(...) debe dictar una resolución que las sancione con una amonestación. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se haya cometido.*
> *La resolución se notificará al responsable o encargado del tratamiento, a cuyo órgano dependa jerárquicamente, en su caso, ya los afectados que tengan la condición de interesado, en su caso."*

En términos similares a la LOPDDDD, el artículo 21.2 de la Ley 32/2010, determina lo siguiente:

> *"2. En el caso de infracciones cometidas con relación a ficheros de titularidad pública, el director o directora de la Autoridad Catalana de Protección de Datos debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos . Además, puede proponer, en su caso, la iniciación de actuaciones disciplinarias de acuerdo con lo que establece la legislación vigente sobre el régimen disciplinario del personal al servicio de las administraciones públicas. Esta resolución debe notificarse a la persona responsable del fichero o del tratamiento, a la encargada del tratamiento, si procede, al órgano del que dependan ya las personas afectadas, si las hubiere".*

En el presente caso, tal y como exponía la persona instructora en la propuesta de resolución, no procede proponer ningún requerimiento de medidas correctoras para corregir los efectos de las

Calle Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

infracciones imputadas, dado que el instituto ha desmantelado el sistema de reconocimiento facial y dactilar.

Resolución

Por todo esto, resuelvo:

1. Amonestar al Instituto Enric Borràs de Badalona como responsable de tres infracciones: una infracción prevista en el artículo 83.5.a) en relación con los artículos 5.1.a) y 9; otra infracción prevista en el artículo 83.5.b) en relación con el artículo 13; y una tercera infracción prevista en el artículo 83.4.a) en relación con el artículo 28, todos ellos del RGPD.

No es necesario requerir medidas correctoras para corregir los efectos de la infracción, de conformidad con lo expuesto en el fundamento de derecho 6º.

2. Notificar esta resolución en el instituto.

3. Comunicar la resolución que se dicte en el Síndic de Greuges, de conformidad con lo que prevé el artículo 77.5 del LOPDDDD.

4. Ordenar que se publique esta resolución en la web de la Autoridad (apdcat.gencat.cat), de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003 , de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.

La directora,