

Expediente N°: E/04798/2013

### RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante las entidades **AUTOMATICOS SURMATIC SL**, **CODERE APUESTAS S.A.** en virtud de denuncia presentada por la **POLICIA MUNICIPAL DE MADRID** y teniendo como base los siguientes

#### HECHOS

**PRIMERO:** Con fecha de 24 de mayo de 2013 tiene entrada en esta Agencia escrito de la Policía Municipal de (en adelante la Policía) comunicando posible infracción a la Ley Orgánica 15/1999 motivada por cámaras de videovigilancia cuyo titular es la entidad **CODERE APUESTAS S.A.** y **AUTOMATISMOS SURMATIC SL** instaladas en un SALON DE JUEGO ubicado en (C/.....1) - **MADRID**.

En el acta de inspección de la policía municipal consta “se observa sistema de videograbación de 8 cámaras y sistema de archivo de DNI con posible infracción LORTAC ( protección datos)”. En informe ampliatorio indican la existencia de una cámara exterior enfocando a la vía pública y zona de acceso. Se observa la existencia de cartel informativo y de un sistema de lectura de DNI de CODERE. Desconocen si se encuentra inscritos los ficheros correspondientes.

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

Se ha realizado una inspección a **CODERE APUESTAS SA** ( en adelante **CODERE** ) en el espacio que esta entidad utiliza para su uso y que tiene concertado con **AUTOMATICOS SURMATIC SL** (en adelante **SURMATIC**, y no **AUTOMATISMOS SURMATIC SL**) en (C/.....1) - MADRID con los siguientes resultados:

- 1 Los representantes de **CODERE** realizaron las siguientes manifestaciones en respuesta a las cuestiones planteadas por los inspectores:
  - 1.1 “**CODERE** comercializa apuestas en el local inspeccionado para lo cual dispone de un espacio cedido por **SURMATIC**, en el que **CODERE** ha dispuesto diversas máquinas de apuestas a disposición de los clientes.
  - 1.2 No obstante, el titular del local es **SURMATIC**, siendo esta entidad la responsable del sistema de videovigilancia, así como titular del contrato de mantenimiento.
  - 1.3 Las zonas de apuestas de **SURMATIC** y **CODERE** se encuentran separadas.
  - 1.4 El local dispone de acceso al Registro de Interdicciones de acceso al Juego, sistema de la COMUNIDAD DE MADRID destinado a recoger la

*información necesaria para hacer efectivo el derecho de los ciudadanos a que les sea prohibido el acceso a los locales y juegos.*

*La inscripción en este Registro se realiza por la persona que voluntariamente solicita su inclusión, procediendo la inscripción solicitada por terceros en virtud de sentencia judicial firme.*

*Este Registro de Interdicciones es responsabilidad de la Dirección General de Tributos y Ordenación y Gestión del Juego, dependiente de la Consejería de Economía y Hacienda de la Comunidad de Madrid.*

*El Registro se encuentra regulado por el Decreto 23/1995, de 16 de marzo, por el que se aprueba el Reglamento de Organización y Funcionamiento del Registro de Juego y del Registro de Interdicción de acceso al Juego.*

- 1.5 *Así, para el acceso a las máquinas de apuestas, los clientes deben de identificarse previamente facilitando su DNI, existiendo en la zona habilitada para **CODERE** un terminal mediante el cual se comprueba, mediante consulta al Registro de interdicción referido de la COMUNIDAD DE MADRID, que la persona no tiene prohibido el juego.*

*El terminal dispone de un escáner de DNIs que lee los datos del reverso del DNI únicamente a los efectos de realizar la consulta. No quedan datos personales registrados sobre el DNI ni sobre la consulta realizada. Únicamente, una vez comprobada la no prohibición al juego de la persona, se le permite la utilización de los medios de juego puestos a disposición de los clientes, emitiendo la máquina un ticket al efecto que es proporcionado al cliente, y sin el cual no tendrá permitido el juego en las instalaciones.*

*Así mismo, es comprobada la mayoría de edad del cliente.*

- 1.6 *El local objeto de inspección no mantiene ningún sistema de registro de DNIs, teniendo únicamente acceso telemático, en modo consulta, al mencionado Registro de Interdicción.”*

Consta adjunta al acta de inspección copia del documento de autorización de local o zona de apuestas donde se aprecia que el titular del local ubicado en **(C/.....2) de MADRID** es **SURMATIC**, y siendo **CODERE** una empresa comercializadora de apuestas en el local.

- 2 Durante la inspección realizada los inspectores de la Agencia solicitaron al representante de **CODERE** que les permitiera el acceso al sistema de consulta del Registro de Interdicción de acceso al Juego, realizándose las siguientes comprobaciones:
  - 2.1 Se verifica que para acceder al sistema se debe de introducir previamente un nombre de usuario y clave asociada.
  - 2.2 Se realiza una consulta utilizando el DNI de uno de los inspectores, que es pasado por el escáner, verificando que el sistema lee los datos de nombre, apellidos, número de DNI, fecha de nacimiento y sexo. Se verifica que el sistema devuelve un símbolo de OK o verificación correcta. Se adjuntan al acta de inspección impresiones con las

comprobaciones realizadas.

- 2.3 Se procede a la emisión del ticket, que se adjunta al acta de inspección.
- 3 Los inspectores de la Agencia solicitan información al representante de **CODERE** con relación a otros sistemas de almacenamiento de datos personales de clientes de la entidad que puedan existir, ante lo que manifiestan que los únicos datos que se recogen son los de las personas que son premiadas, a los efectos requeridos por las disposiciones legales con relación al blanqueo de capitales y de IRPF. Para ello, la entidad tiene a disposición de los clientes tres formularios de recogida de datos, para la solicitud de abono de los premios. Se verifica que dichos formularios incluyen leyendas informativas sobre protección de datos.

Constan ejemplares de los tres modelos adjuntos al acta de inspección.

- 4 Los representantes de **SURMATIC** realizan las siguientes manifestaciones en respuesta a las cuestiones planteadas por los inspectores:
  - 4.1 **SURMATIC** comercializa apuestas en el local inspeccionado, el cual se encuentra en régimen de alquiler. El local es compartido con **CODERE APUESTAS SA**, empresa también comercializadora de apuestas, tal y como consta en la autorización de local o zona de apuestas, ya en poder de los inspectores, expedido por la Dirección General de Tributos y Ordenación y Gestión del Juego de la Comunidad de Madrid.
  - 4.2 La sala cuenta con un sistema de videovigilancia desde el año 2011. El Sistema ha sido instalado por la empresa **CENTRAL DE ALARMAS PROGRAMADAS SL** con la que se ha suscrito un contrato de arrendamiento de servicios de seguridad, cuya copia se adjunta como **DOC.1**, así como su anexo de acceso a datos por cuenta de terceros.
  - 4.3 La finalidad del sistema es fundamentalmente la seguridad de las instalaciones y las personas, y, en concreto evitar robos en el local.
  - 4.4 El sistema está integrado por un total de cinco cámaras interiores, y si bien una de ellas se encuentra situada en la zona de entrada al local, no existen cámaras exteriores.

Las otras cuatro cámaras se encuentran todas enfocado a las zonas de juego, teniendo una de las cámaras posibilidad de giro en remoto.

- 4.5 Las imágenes captadas por las cámaras se almacenan en un sistema de disco duro que se ubica en una zona de almacén, cerrada con llave.
- 4.6 **SURMATIC** tiene inscrito en el Registro General de Protección de Datos el fichero correspondiente a las imágenes captadas por los Sistemas de Videovigilancia de las salas de juego de la entidad.
- 4.7 Las imágenes de las cámaras pueden ser visualizadas únicamente por el personal de la empresa de seguridad, no teniendo el personal de **SURMATIC** acceso a ellas, de tal forma que cuando se produce una incidencia de seguridad debe de solicitarse a **CENTRAL DE ALARMAS**

**PROGRAMADAS SL** el acceso a las imágenes grabadas por las cámaras.

- 4.8 El sistema graba las imágenes con un tiempo de permanencia de aproximadamente de un mes, borrándose siempre cuando se supera dicho periodo. El sistema funciona 24 horas por 365 días al año.
- 4.9 Existe un cartel informativo sobre la existencia de sistema de videovigilancia en el acceso al local. También existe un folleto informativo con más detalle de los derechos que asisten a los clientes.
- 4.10 El local dispone de acceso al Registro de Interdicciones de acceso al Juego, sistema de la COMUNIDAD DE MADRID destinado a recoger la información necesaria para hacer efectivo el derecho de los ciudadanos a que les sea prohibido el acceso a los locales y juegos.

La inscripción en este Registro se realiza por la persona que voluntariamente solicita su inclusión, procediendo la inscripción solicitada por terceros en virtud de sentencia judicial firme.

Este Registro de Interdicciones es responsabilidad de la Dirección General de Tributos y Ordenación y Gestión del Juego, dependiente de la Consejería de Economía y Hacienda de la Comunidad de Madrid.

El Registro se encuentra regulado por el Decreto 23/1995, de 16 de marzo, por el que se aprueba el Reglamento de Organización y Funcionamiento del Registro de Juego y del Registro de Interdicción de acceso al Juego.

- 4.11 Así, para el acceso a las máquinas de apuestas, los clientes deben de identificarse previamente facilitando su DNI, existiendo en una zona protegida por una mampara de seguridad un terminal compartido con la entidad **CODERE APUESTAS SA**, mediante el cual se comprueba, mediante consulta al Registro de interdicción referido de la COMUNIDAD DE MADRID, que la persona no tiene prohibido el juego.

El terminal dispone de un escáner de DNIs que lee los datos del reverso del DNI únicamente a los efectos de realizar la consulta. No quedan datos personales registrados sobre el DNI ni sobre la consulta realizada. Únicamente, una vez comprobada la no prohibición al juego de la persona, se le permite la utilización de los medios de juego puestos a disposición de los clientes, emitiendo la máquina un ticket al efecto que es proporcionado al cliente, y sin el cual no tendrá permitido el juego en las instalaciones.

Así mismo, es comprobada la mayoría de edad del cliente.

- 4.12 El local objeto de inspección no mantiene ningún sistema de registro de DNIs, teniendo únicamente acceso telemático, en modo consulta, al mencionado Registro de Interdicción.

Realizada también una inspección a **SURMATIC**, se obtienen los siguientes resultados:

- 5 Los representantes de SURMATIC realizaron las siguientes

manifestaciones en respuesta a las cuestiones planteadas por los inspectores:

- 5.1 ***"SURMATIC** comercializa apuestas en el local inspeccionado, el cual se encuentra en régimen de alquiler. El local es compartido con **CODERE APUESTAS SA**, empresa también comercializadora de apuestas, tal y como consta en la autorización de local o zona de apuestas, ya en poder de los inspectores, expedido por la Dirección General de Tributos y Ordenación y Gestión del Juego de la Comunidad de Madrid.*
- 5.2 *La sala cuenta con un sistema de videovigilancia desde el año 2011. El Sistema ha sido instalado por la empresa CENTRAL DE ALARMAS PROGRAMADAS SL con la que se ha suscrito un contrato de arrendamiento de servicios de seguridad [...]*
- 5.3 *La finalidad del sistema es fundamentalmente la seguridad de las instalaciones y las personas, y, en concreto evitar robos en el local.*
- 5.4 *El sistema está integrado por un total de cinco cámaras interiores, y si bien una de ellas se encuentra situada en la zona de entrada al local, no existen cámaras exteriores.*

*Las otras cuatro cámaras se encuentran todas enfocado a las zonas de juego, teniendo una de las cámaras posibilidad de giro en remoto.*

- 5.5 *Las imágenes captadas por las cámaras se almacenan en un sistema de disco duro que se ubica en una zona de almacén, cerrada con llave.*
- 5.6 ***SURMATIC** tiene inscrito en el Registro General de Protección de Datos el fichero correspondiente a las imágenes captadas por los Sistemas de Videovigilancia de las salas de juego de la entidad.*
- 5.7 *Las imágenes de las cámaras pueden ser visualizadas únicamente por el personal de la empresa de seguridad, no teniendo el personal de **SURMATIC** acceso a ellas, de tal forma que cuando se produce una incidencia de seguridad debe de solicitarse a CENTRAL DE ALARMAS PROGRAMADAS SL el acceso a las imágenes grabadas por las cámaras.*
- 5.8 *El sistema graba las imágenes con un tiempo de permanencia de aproximadamente de un mes, borrándose siempre cuando se supera dicho periodo. El sistema funciona 24 horas por 365 días al año.*
- 5.9 *Existe un cartel informativo sobre la existencia de sistema de videovigilancia en el acceso al local. También existe un folleto informativo con más detalle de los derechos que asisten a los clientes.*
- 5.10 *El local dispone de acceso al Registro de Interdicciones de acceso al Juego, sistema de la COMUNIDAD DE MADRID destinado a recoger la información necesaria para hacer efectivo el derecho de los ciudadanos a que les sea prohibido el acceso a los locales y juegos.*

*La inscripción en este Registro se realiza por la persona que voluntariamente solicita su inclusión, procediendo la inscripción solicitada por terceros en virtud de sentencia judicial firme.*

*Este Registro de Interdicciones es responsabilidad de la Dirección General de Tributos y Ordenación y Gestión del Juego, dependiente de la Consejería de Economía y Hacienda de la Comunidad de Madrid.*

*El Registro se encuentra regulado por el Decreto 23/1995, de 16 de marzo, por el que se aprueba el Reglamento de Organización y Funcionamiento del Registro de Juego y del Registro de Interdicción de acceso al Juego.*

- 5.11 *Así, para el acceso a las máquinas de apuestas, los clientes deben de identificarse previamente facilitando su DNI, existiendo en una zona protegida por una mampara de seguridad un terminal compartido con la entidad CODERE APUESTAS SA, mediante el cual se comprueba, mediante consulta al Registro de interdicción referido de la COMUNIDAD DE MADRID, que la persona no tiene prohibido el juego.*

*El terminal dispone de un escáner de DNIs que lee los datos del reverso del DNI únicamente a los efectos de realizar la consulta. No quedan datos personales registrados sobre el DNI ni sobre la consulta realizada. Únicamente, una vez comprobada la no prohibición al juego de la persona, se le permite la utilización de los medios de juego puestos a disposición de los clientes, emitiendo la máquina un ticket al efecto que es proporcionado al cliente, y sin el cual no tendrá permitido el juego en las instalaciones.*

*Así mismo, es comprobada la mayoría de edad del cliente.*

- 5.12 *El local objeto de inspección no mantiene ningún sistema de registro de DNIs, teniendo únicamente acceso telemático, en modo consulta, al mencionado Registro de Interdicción."*

Consta, adjunto al acta de inspección, copia del contrato de arrendamiento de servicios de seguridad suscrito con la empresa **CENTRAL DE ALARMAS PROGRAMADAS SL**, junto con copia de su anexo de acceso a datos por cuenta de terceros.

- 6 Los inspectores de la Agencia solicitaron que el acceso al sistema de videovigilancia realizándose las siguientes comprobaciones:
  - 6.1 Se verifica la existencia de **cinco cámaras interiores**, tres en la zona de **SURMATIC**, una en la de CODERE, y una en el vestíbulo común. Las zonas se encuentran separadas por una mampara con puerta.
  - 6.2 **Una de las cámaras se encuentra en la zona de entrada, enfocando al vestíbulo y recogiendo parte de la puerta de entrada.** Se realiza una fotografía desde la cámara al objeto de recoger la imagen que capta la misma.
  - 6.3 Se verifica así mismo la **existencia de un cartel informativo** de la existencia de un sistema de videovigilancia, situado junto a la puerta de entrada a la sala, realizándose una fotografía. **Se verifica la existencia de un folleto informativo detallado** al que se realiza también una fotografía.
  - 6.4 Se comprueba la existencia de un cuarto de almacén cuya puerta se encuentra cerrada con llave. Un vez abierto se verifica que en él se aloja la electrónica de red y los servidores, entre ellos el sistema de

almacenamiento de imágenes. Se comprueba que no existe espacio físico para el acceso de una persona al objeto de acceder a los sistemas. Se realiza una fotografía a la puerta, así como del equipo de grabación de imágenes.

- 6.5 Consta adjunto al acta de inspección reportaje fotográfico con las comprobaciones realizadas.
- 7 Los inspectores de la Agencia solicitaron al representante información con relación a otros sistemas de almacenamiento de datos personales de clientes de la entidad que pudieran existir, ante lo que manifestaron que no existe ninguno, ni siquiera uno que recoja datos de las personas premiadas, ya que los premios de la zona de **SURMATIC** son inferiores límites legales establecidos a los efectos de blanqueo de capitales e IRPF, al tratarse básicamente de máquinas tragaperras y no de apuestas deportivas como en el caso de **CODERE APUESTAS, SA**, por lo que no existen formularios de recogida de datos de los premiados.

Por último, se ha verificado la inscripción en el RGPD del fichero correspondiente al Sistema de grabación de imágenes, titularidad de **SURMATIC**, fichero con código de inscripción 2111330422. Fue inscrito en fecha 13/05/2011 y consta como encargado de tratamiento **CENTRAL DE ALARMAS PROGRAMADAS SL**.

## **FUNDAMENTOS DE DERECHO**

### **I**

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

### **II**

Con carácter previo, procede situar la materia de videovigilancia en su contexto normativo.

Así el artículo 1 de la LOPD dispone: *“La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”*

En cuanto al ámbito de aplicación de la LOPD, el artículo 2.1 de la misma señala: *“La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”*, definiéndose el concepto de dato de carácter personal en el apartado a) del artículo 3 de la LOPD, como *“Cualquier información concerniente a personas físicas identificadas o identificables”*.

El artículo 3 de la LOPD define en su letra c) el tratamiento de datos como aquellas *“operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”*.

El artículo 5.1. f) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, define datos de carácter personal como: *“Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a personas físicas identificadas o identificables”*.

En este mismo sentido se pronuncia el artículo 2.a) de la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, según el cual, a efectos de dicha Directiva, se entiende por dato personal *“toda información sobre una persona física identificada o identificable; se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social”*. Asimismo, el Considerando 26 de esta Directiva se refiere a esta cuestión señalando que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a aquélla.

La Exposición de Motivos de la Instrucción 1/2006, de 8 de noviembre, de esta Agencia Española de Protección de Datos, relativa al tratamiento de los datos con fines de videovigilancia señala que: *“La seguridad y la vigilancia, elementos presentes en la sociedad actual, no son incompatibles con el derecho fundamental a la protección de la imagen como dato personal, lo que en consecuencia exige respetar la normativa existente en materia de protección de datos, para de esta manera mantener la confianza de la ciudadanía en el sistema democrático”*. Sigue señalando: *“Las imágenes se consideran un dato de carácter personal, en virtud de lo establecido en el artículo 3 de la Ley Orgánica 15/1999...”*.

La garantía del derecho a la protección de datos, conferida por la normativa de referencia, requiere que exista una actuación que constituya un tratamiento de datos personales en el sentido expresado. En otro caso las mencionadas disposiciones no serán de aplicación.

Por su parte, la citada Instrucción 1/2006, dispone en su artículo 1.1 lo siguiente:

*“1. La presente Instrucción se aplica al tratamiento de datos personales de imágenes de personas físicas identificadas o identificables, con fines de vigilancia a través de sistemas de cámaras y videocámaras.*

*El tratamiento objeto de esta Instrucción comprende la grabación, captación, transmisión, conservación, y almacenamiento de imágenes, incluida su reproducción o*

*emisión en tiempo real, así como el tratamiento que resulte de los datos personales relacionados con aquéllas.*

*Se considerará identificable una persona cuando su identidad pueda determinarse mediante los tratamientos a los que se refiere la presente instrucción, sin que ello requiera plazos o actividades desproporcionados.*

*Las referencias contenidas en esta Instrucción a videocámaras y cámaras se entenderán hechas también a cualquier medio técnico análogo y, en general, a cualquier sistema que permita los tratamientos previstos en la misma.” (el subrayado es de la Agencia Española de Protección de Datos).*

La Instrucción 1/2006 en su artículo 2 establece lo siguiente:

*“1. Sólo será posible el tratamiento de los datos objeto de la presente instrucción, cuando se encuentre amparado por lo dispuesto en el artículo 6.1 y 2 y el artículo 11.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

*2. Sin perjuicio de lo establecido en el apartado anterior la instalación de cámaras y videocámaras deberá respetar en todo caso los requisitos exigidos por la legislación vigente en la materia.”*

De lo anteriormente expuesto se desprende que el concepto de dato personal, según la definición de la LOPD, requiere la concurrencia de un doble elemento: por una parte, la existencia de una información o dato y, por otra, que dicho dato pueda vincularse a una persona física identificada o identificable, por lo que la imagen de una persona física identificada o identificable constituye un dato de carácter personal.

Así, de conformidad con la normativa y jurisprudencia expuesta, la captación de imágenes a través de videocámaras, como es el caso que nos ocupa, constituye un tratamiento de datos personales, cuyo responsable se identifica, en el presente caso, con el citado establecimiento, toda vez que es ésta la que en primer lugar, ha decidido la instalación de las reseñadas videocámaras con fines de vigilancia, y, en segundo lugar, ha dispuesto sobre la finalidad, contenido y uso del citado tratamiento de imágenes.

### III

En el presente expediente se denuncia a las entidades denunciadas por la existencia de un sistema de videovigilancia que pudieras vulnerar la normativa de protección de datos.

Así, debe entrarse a valorar el cumplimiento del deber de información e inscripción de ficheros.

Primeramente debe clarificarse que **CODERE** comercializa apuestas en el local inspeccionado para lo cual dispone de un espacio cedido por **SURMATIC**, en el que **CODERE** ha dispuesto diversas máquinas de apuestas a disposición de los clientes. **CODERE APUESTAS SA**, es una empresa también comercializadora de apuestas, tal y como consta en la autorización de local o zona de apuestas, expedido por la Dirección

General de Tributos y Ordenación y Gestión del Juego de la Comunidad de Madrid.

La sala cuenta con un sistema de videovigilancia desde el año 2011. El sistema ha sido instalado por la empresa **CENTRAL DE ALARMAS PROGRAMADAS SL** con la que se ha suscrito un contrato de arrendamiento de servicios de seguridad.

El titular del local es **SURMATIC**, siendo esta entidad la responsable del sistema de videovigilancia, así como titular del contrato de mantenimiento.

La finalidad del sistema es fundamentalmente la seguridad de las instalaciones y las personas, y, en concreto evitar robos en el local.

Por los inspectores actuantes se verifica la existencia de cinco cámaras interiores, tres en la zona de **SURMATIC**, una en la de **CODERE**, y una en el vestíbulo común. No existen cámaras exteriores. Las zonas se encuentran separadas por una mampara con puerta. Una de las cámaras se encuentra en la zona de entrada, enfocando al vestíbulo y recogiendo parte de la puerta de entrada.

Así, el tratamiento de las imágenes por parte del responsable, obliga a que se cumpla con el deber de informar a los afectados, en los términos establecidos en el artículo 5.1 de la LOPD el cual reza lo siguiente:

*“1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*

*a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*

*b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*

*c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*

*d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*

*e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante”.*

En cuanto al modo en que hay de facilitarse la información recogida en el artículo 5 de la LOPD, debe tenerse en cuenta el artículo 3 de la Instrucción 1/2006, que establece lo siguiente:

*“Los responsables que cuenten con sistemas de videovigilancia deberán cumplir con el deber de información previsto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre. A tal fin deberán:*

*a) Colocar, en las zonas videovigiladas, al menos un distintivo informativo ubicado en lugar suficientemente visible, tanto en espacios abiertos como cerrados y*

*b) Tener a disposición de los/las interesados/as impresos en los que se detalle la información prevista en el artículo 5.1 de la Ley Orgánica 15/1999.*

*El contenido y el diseño del distintivo informativo se ajustará a lo previsto en el Anexo de esta Instrucción.”*

“ANEXO-

*1. El distintivo informativo a que se refiere el artículo 3.a) de la presente Instrucción deberá de incluir una referencia a la «LEY ORGÁNICA 15/1999, DE PROTECCIÓN DE DATOS», incluirá una mención a la finalidad para la que se tratan los datos («ZONA VIDEOVIGILADA»), y una mención expresa a la identificación del responsable ante quien puedan ejercitarse los derechos a los que se refieren los artículos 15 y siguientes de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.”*

En el caso que nos ocupa, los inspectores actuantes comprobaron la existencia de cartel informativo de la existencia de un sistema de videovigilancia, situado junto a la puerta de entrada a la sala, acorde al que hace referencia el citado artículo 3.a) de la Instrucción 1/2006, en relación al artículo 5 de la LOPD. Asimismo se aporta cláusula informativa a disposición de los interesados, de conformidad con el artículo 3.b) de la citada Instrucción.

Por lo tanto las entidades denunciadas, cumplen el deber de información, en cuanto al sistema de videovigilancia, recogido en el artículo 5 de la LOPD, anteriormente transcrito.

Por otro lado, respecto al cumplimiento de la inscripción de ficheros, el artículo 26.1 de la LOPD, recoge lo siguiente:

*“1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos”*

El responsable del fichero es el titular del fichero que contiene datos de carácter personal. Sobre él van a recaer las obligaciones que establece la LOPD. . El responsable del fichero, antes de disponerse a someter datos personales a tratamiento, deberá cumplir con los requisitos de la normativa de protección de datos, teniendo en cuenta su naturaleza y la naturaleza de los datos que va a someter a tratamiento.

El apartado d) del artículo 3 de la LOPD define al responsable del fichero o tratamiento como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento. El artículo 43 de la LOPD sujeta a su régimen sancionador precisamente al responsable del fichero o tratamiento.

El reglamento de desarrollo de la LOPD, aprobado por RD 1720/2007, de 21 de diciembre, complementa esta definición en el apartado q) del artículo 5, en el que señala lo siguiente:

*“q) Responsable del fichero o del tratamiento: Persona física o jurídica, de*

*naturaleza pública o privada, u órgano administrativo, que solo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.*

*Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados”.*

El responsable del fichero es, en suma, quien debe garantizar el derecho fundamental de protección de datos personales de todas las personas cuyos datos almacena. Por ello, va a estar obligado a llevar a cabo una serie de actuaciones dirigidas a la protección de los datos, a su integridad y a su seguridad.

El responsable debe notificar su fichero a la Agencia Española de Protección de Datos, que dispondrá inscribirlo en el Registro General de Protección de Datos. La notificación de inscripción del fichero facilitará que terceros puedan conocer que se está produciendo un tratamiento con una finalidad determinada y los afectados tendrán la oportunidad de ejercitar sus derechos ante el responsable.

Además este es el criterio que se hace constar en la Instrucción 1/2006 , al señalar en su artículo 7 que *“1-La persona o entidad que prevea la creación de ficheros de videovigilancia deberá notificarlo previamente a la Agencia Española de Protección de Datos, para su inscripción en el Registro General de la misma.*

*Tratándose de ficheros de titularidad pública deberá estarse a lo establecido en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.*

*2.-A estos efectos, no se considerará fichero el tratamiento consistente exclusivamente en la reproducción o emisión de imágenes en tiempo real.”*

En el caso que nos ocupa, consta la inscripción en el Registro General de Protección de Datos del fichero correspondiente al Sistema de grabación de imágenes, titularidad de **SURMATIC**. Fue inscrito en fecha 13/05/2011 y consta como encargado de tratamiento **CENTRAL DE ALARMAS PROGRAMADAS SL**.

#### IV

Por otro lado, hasta la entrada en vigor, el 27 de diciembre de 2009, de la Ley 25/2009, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y sus ejercicio(conocida como “Ley Ómnibus”), la legitimación para el tratamiento por particulares y empresas de imágenes captadas a través de dispositivos de videovigilancia sólo era posible en caso de que dichos sistemas hubieran sido contratados con empresas de seguridad privada, debidamente acreditadas ante el Ministerio del Interior, al que además debía notificarse el contrato que se hubiese celebrado, conforme a lo exigido por la Ley 23/1992, de 30 de julio de Seguridad Privada.

La Ley 25/2009 ha suprimido para la mayor parte de los casos estas exigencias, al liberalizar la comercialización, entrega, instalación y mantenimiento de estos dispositivos, de forma que ya no será necesario acudir para su puesta en funcionamiento a una empresa de seguridad privada ni cumplir las obligaciones de notificación del contrato al Ministerio del Interior..

En concreto el artículo 14 de la nueva Ley modifica el artículo 5.1 e) de la Ley 23/1992, de 30 de julio de Seguridad Privada, añadiendo una Disposición Adicional Sexta a la Ley de Seguridad Privada con la siguiente redacción:

“Disposición Adicional Sexta. Exclusión de las empresas relacionadas con equipos técnicos de seguridad:

*Los prestadores de servicios y las filiales de empresas de seguridad que vendan, entreguen, instalen o mantengan equipos técnicos de seguridad, siempre que no incluyan la prestación de servicios de conexión con centrales de alarma, quedan excluidas de la legislación de seguridad privada, siempre y cuando no se dediquen a ninguno de los otros fines definidos en el artículo 5, sin perjuicio de otras legislaciones específicas que pudieran resultarles de aplicación.”*

La interpretación de la mencionada disposición determina que cualquier particular o empresa cuya actividad no sea la propia de una empresa de seguridad privada podrá; “vender, entregar, instalar y mantener equipos técnicos de seguridad” sin necesidad de cumplir las exigencias previstas en la Ley de Seguridad Privada para tales empresas. De este modo, dado que la Ley permite la instalación y mantenimiento de dichos equipos por empresas distintas a las de seguridad privada, legitima a quienes adquieran de estos dispositivos para tratar los datos personales derivado de la captación de las imágenes sin necesidad de acudir a empresas de seguridad privada, siendo dicho tratamiento conforme a lo previsto en la Ley Orgánica de Protección de Datos de Carácter Personal.

No obstante, la instalación de un sistema de videovigilancia conectado a una central de alarma, sí seguirá requiriendo la concurrencia de los requisitos exigidos hasta ahora; esto es, que el dispositivo sea contratado, instalado y mantenido por una empresa de seguridad privada autorizada por el Ministerio del Interior y que el contrato sea notificado a dicho Departamento.

En todo caso, el tratamiento de las imágenes deberá cumplir los restantes requisitos exigibles en materia de protección de datos de Carácter Personal, recogidos en la Ley Orgánica y, en particular, en la Instrucción 1/2006 de la Agencia Española de Protección de Datos, como son, entre otros, los relativos a que las imágenes que se capten sean las necesarias y no excesivas para la finalidad perseguida; el deber de informar a los interesados, tanto a través de la colocación de carteles informativos como mediante la puesta a disposición de aquéllos de impresos en que se detalle la información; la notificación de la existencia de los ficheros a la Agencia Española de Protección de Datos; o la implantación de medidas de seguridad.

En el caso que nos ocupa, el sistema de videovigilancia ha sido instalado por la empresa de seguridad autorizada **CENTRAL DE ALARMAS PROGRAMADAS SL**, con la que se ha suscrito un contrato de arrendamiento de servicios de seguridad. Las imágenes de las cámaras pueden ser visualizadas únicamente por el personal de la empresa de seguridad, no teniendo el personal de **SURMATIC** acceso a ellas, de tal forma que cuando se produce una incidencia de seguridad debe de solicitarse a **CENTRAL DE ALARMAS PROGRAMADAS SL** el acceso a las imágenes grabadas por las cámaras. Asimismo consta aportado contrato de acceso a datos por cuenta de tercero por parte de **SURMATIC** y **CENTRAL DE ALARMAS PROGRAMADAS S.L.**

Por lo tanto, el sistema de videovigilancia ha sido instalado por empresas de seguridad, debidamente autorizada, por lo que el tratamiento de los datos de las personas que acceden al establecimiento, se encuentra habilitado por la LSP.

## V

Por otro lado, respecto a la posible captación por parte de la entidad denunciada, de imágenes de la vía pública, a través de la cámara instalada en la puerta de acceso, hay que señalar que para entender las especialidades derivadas del tratamiento de las imágenes en vía pública, es preciso conocer la regulación que sobre esta materia se contempla en el artículo 1 de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos que establece: *“La presente Ley regula la utilización por las Fuerzas y Cuerpos de Seguridad de videocámaras para grabar imágenes y sonidos en lugares públicos abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública”*.

Este precepto es preciso ponerlo en relación con lo dispuesto en el artículo 3 e) de la Ley Orgánica 15/1999, donde se prevé que: *“Se regirán por sus disposiciones específicas y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:*

*e) Los procedentes de las imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia”*.

En virtud de todo lo expuesto, podemos destacar que la instalación de videocámaras en lugares públicos es competencia exclusiva de las Fuerzas y Cuerpos de Seguridad, de ahí que la legitimación para el tratamiento de dichas imágenes se complete en la Ley Orgánica 4/1997, señalándose en su artículo 2.2, en lo que hace mención a su ámbito de aplicación que *“2.2. Sin perjuicio de las disposiciones específicas contenidas en la presente Ley, el tratamiento automatizado de las imágenes y sonidos se regirá por lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizados de los Datos de Carácter Personal.”*

Así, la legitimación para el uso de instalaciones de videovigilancia se ciñe a la protección de entornos privados. La prevención del delito y la garantía de la seguridad en las vías públicas corresponden en exclusiva a las Fuerzas y Cuerpos de Seguridad del Estado.

No obstante, en algunas ocasiones la protección de los espacios privados sólo es posible si las cámaras se ubican en espacios como las fachadas. A veces, también resulta necesario captar los accesos, puertas o entradas, de modo que aunque la cámara se encuentre en el interior del edificio, resulta imposible no registrar parte de lo que sucede en la porción de vía pública que inevitablemente se capta. Por otra parte, las videocámaras deberán orientarse de modo tal que su objeto de vigilancia principal sea el entorno privado y la captación de imágenes de la vía pública sea la mínima imprescindible. Así, el artículo 4.1 y 2 de la LOPD, garantiza el cumplimiento del principio de proporcionalidad en todo tratamiento de datos personales, cuando señala que:

*“1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.*

*2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos”.*

En este sentido, se pronuncia la Instrucción 1/2006, cuando señala en el artículo 4, lo siguiente:

*1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.*

*2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.*

*3. Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida”.*

Para que la excepción recogida en el artículo 4.3 de la Instrucción 1/2006 resulte aplicable no deberá existir una posibilidad de instalación alternativa, sin poder interpretarse que dicho precepto constituye una habilitación para captar imágenes en espacios públicos, puesto que en ningún caso puede admitirse el uso de prácticas de

vigilancia más allá del entorno objeto de la instalación y en particular en lo que se refiere a los espacios públicos circundantes, edificios contiguos y vehículos distintos de los que accedan al espacio vigilado.

Pues bien, una vez explicada esta cuestión, cabe decir que los inspectores actuantes comprobaron la existencia de cinco cámaras interiores, tres en la zona de **SURMATIC**, una en la de **CODERE**, y una en el vestíbulo común. No existen cámaras exteriores. Una de las cámaras se encuentra en la zona de entrada, enfocando al vestíbulo y recogiendo parte de la puerta de entrada. Por tanto, las imágenes captadas no infringirían el principio de proporcionalidad de los datos previsto en el artículo 4.1 de la Ley Orgánica de Protección de Datos, cuando se habla de que los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Por tanto, siguiendo el criterio de la citada Instrucción 1/2006, no puede considerarse, en el presente caso, que la instalación de las videocámaras en los términos expuestos vulnere los principios de calidad, proporcionalidad y finalidad del tratamiento.

## VI

Por último, **SURMATIC** dispone de acceso al Registro de Interdicciones de acceso al Juego, sistema de la COMUNIDAD DE MADRID destinado a recoger la información necesaria para hacer efectivo el derecho de los ciudadanos a que les sea prohibido el acceso a los locales y juegos.

La inscripción en este Registro se realiza por la persona que voluntariamente solicita su inclusión, procediendo la inscripción solicitada por terceros en virtud de sentencia judicial firme.

Este Registro de Interdicciones es responsabilidad de la Dirección General de Tributos y Ordenación y Gestión del Juego, dependiente de la Consejería de Economía y Hacienda de la Comunidad de Madrid.

El Registro se encuentra regulado por el Decreto 23/1995, de 16 de marzo, por el que se aprueba el Reglamento de Organización y Funcionamiento del Registro de Juego y del Registro de Interdicción de acceso al Juego.

Así, para el acceso a las máquinas de apuestas, los clientes deben de identificarse previamente facilitando su DNI, existiendo en una zona protegida por una mampara de seguridad un terminal compartido con la entidad **CODERE APUESTAS SA**, mediante el cual se comprueba, mediante consulta al Registro de interdicción referido de la COMUNIDAD DE MADRID, que la persona no tiene prohibido el juego.

El terminal dispone de un escáner de DNIs que lee los datos del reverso del DNI únicamente a los efectos de realizar la consulta. No quedan datos personales registrados sobre el DNI ni sobre la consulta realizada. Únicamente, una vez comprobada la no prohibición al juego de la persona, se le permite la utilización de los

medios de juego puestos a disposición de los clientes, emitiendo la máquina un ticket al efecto que es proporcionado al cliente, y sin el cual no tendrá permitido el juego en las instalaciones. Asimismo, es comprobada la mayoría de edad del cliente.

El local objeto de inspección no mantiene ningún sistema de registro de DNIs, teniendo únicamente acceso telemático, en modo consulta, al mencionado Registro de Interdicción.

Los inspectores de la Agencia solicitaron al representante información con relación a otros sistemas de almacenamiento de datos personales de clientes de la entidad que pudieran existir, ante lo que manifestaron que no existe ninguno, ni siquiera uno que recoja datos de las personas premiadas, ya que los premios de la zona de **SURMATIC** son inferiores límites legales establecidos a los efectos de blanqueo de capitales e IRPF, al tratarse básicamente de máquinas tragaperras y no de apuestas deportivas como en el caso de **CODERE APUESTAS, SA**, por lo que no existen formularios de recogida de datos de los premiados.

Los inspectores de la Agencia solicitan al representante de **CODERE** información con relación a otros sistemas de almacenamiento de datos personales de clientes de la entidad que pudieran existir, ante lo que manifiestan que los únicos datos que se recogen son los de las personas que son premiadas, a los efectos requeridos por las disposiciones legales con relación al blanqueo de capitales y de IRPF. Para ello, la entidad tiene a disposición de los clientes tres formularios de recogida de datos, para la solicitud de abono de los premios, verificando los inspectores actuantes que en dichos formularios se incluyen las leyendas informativas sobre protección de datos.

A la vista de todo lo expuesto, se procede al archivo del presente expediente de actuaciones previas al no apreciarse vulneración a la actual normativa en materia de protección de datos.

Por lo tanto, de acuerdo con lo señalado,

**Por el Director de la Agencia Española de Protección de Datos,**

**SE ACUERDA:**

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a **AUTOMATICOS SURMATIC SL**, **CODERE APUESTAS S.A.** y a **POLICIA MUNICIPAL DE MADRID**.

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

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de

Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

José Luis Rodríguez Álvarez  
Director de la Agencia Española de Protección de Datos