LA GESTION Y PROTECIÓN DE LOS DATOS PERSONALES CONTENIDOS EN SOPORTES INFORMÁTICOS EN EL CENTRO DE ATENCIÓN DE URGENCIAS Y EMERGENCIAS DE EXTREMADURA 1.1.2 .

Víctor García Vega
Asesor de la Consejera de Presidencia
Junta de Extremadura

1. PLANTEAMIENTO.

Prescindiendo de cualquier ánimo de exhaustividad, como no podía ser de otro modo dado el riguroso marco expositivo que nos concede una comunicación, se pretende con esta exposición el acercamiento a un aspecto endémicamente soslayado en los Servicios de Atención de Urgencias y Emergencias de nuestro entorno, y al que la Consejería de Presidencia de la Junta de Extremadura ha prestado una atención preferente desde la creación del Centro de Atención Urgencias y Emergencias de Extremadura 1.1.2. Ese ámbito no es otro que el de la gestión y seguridad de los datos personales que, en el curso de la atención de los incidentes, se puedan recabar desde el Servicio.

La especial idiosincrasia del Centro de atención de urgencias y emergencias de Extremadura 1.1.2 que, al contrario de lo que sucede en la mayor parte de las Comunidades Autónomas donde se presta la atención a través de empresas concesionarias, se presta de una manera directa por la Administración Autonómica como si se tratase de una unidad administrativa más, hace que la exigencia no sólo de una eficaz atención sino de una especial garantía

Como consecuencia de lo anterior es fácilmente asumible que la grandeza del Centro de Atención Urgencias y Emergencias se cifra en la doble exigencia que constituye su *leit motiv*. Por una parte, su actividad consiste en la atención de las urgencias y emergencias que se produzcan en la Comunidad ofreciendo la respuesta adecuada a través de los servicios de seguridad o sanidad pública que se estimen necesarios. Por otra, y he aquí la dificultad, ha de resolverse esa situación protegiendo los derechos al honor e intimidad de los alertantes e implicados, esto es, no recabando más datos personales de los estrictamente necesarios para la resolución de la crisis, y garantizando la protección y absoluta privacidad en el tratamiento de los mismos.

Los riesgos son variados. La respuesta debe ser unívoca.

2. RÉGIMEN JURÍDICO DE REFERENCIA Y SU APLICACIÓN AL CENTRO.

No por usual resulta innecesario comenzar a analizar el régimen jurídico de la protección que en España se da a los datos personales en poder de las Administraciones Públicas invocando el artículo 18.4 de la Constitución Española, que exige la existencia de una ley orgánica que regule el uso de la informática, estableciendo: "La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Siguiendo este mandato constitucional se promulga la nueva Ley Orgánica de Protección de Datos de Carácter Personal (LO 15/1999, de 13 de diciembre, en adelante LOPD) para adaptar nuestro derecho interno a la Directiva Comunitaria sobre la materia.

La LOPD tiene por objeto (art.1) 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. Siendo su *ámbito de aplicación (art.2 LOPD)* 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.

El a*rtículo 3* LOPD define como datos personales cualquier información concerniente a personas físicas identificadas o identificables.

.

Hay que advertir de modo previo que los datos que se recaban desde el Servicio no se encuentran entre los denominados por la LOPD *Datos Especialmente Protegidos* en tanto se trata de los estrictamente necesarios para conocer la identidad de la persona que reclama el auxilio, con un elemento que aporta una cierta trascendencia, la grabación de la voz.

En cualquier caso, la recopilación de estos datos se realiza exclusivamente con la finalidad de prestar una adecuada atención a los incidentes o emergencias, por lo

que no se ha creado lo que propiamente se podría denominar fichero de datos personales. Se trata, tan sólo, de una simple acumulación de incidentes, cronológicamente almacenados para su gestión, parte de cuyo relato está formado por los datos personales rigurosamente necesarios para la resolución del incidente.

Por tanto, entendemos que la recopilación de datos que realiza el 1.1.2 es absolutamente indirecta y necesaria, finalista, de manera que no se ha estimado de aplicación en nuestro caso el art. 20 LOPD, relativo al procedimiento de *Creación, modificación o supresión* de ficheros de titularidad pública sobre datos personales, y ello porque no existe un fichero de datos personales stricto senso. Existe una recopilación histórica de incidentes atendidos por el Centro en la que constan una serie de datos personales de los usuarios.

No obstante lo anterior, sí se ha querido desde el Centro, y por la propia trascendencia que, por motivos de seguridad y prestación adecuada del servicio, se otorga a los datos personales recabados, observar estrictamente lo dispuesto en el Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal, el RD 994/1999, de 11 de mayo. Entramos en su análisis en epígrafes sucesivos.

3. EL PROCESO DE RECOPILACIÓN DE DATOS PERSONALES Y LA GESTIÓN DE SU PROTECCIÓN Y SEGURIDAD.

Cuando se produce una situación de urgencia o emergencia y un alertante pulsa en su terminal telefónico los dígitos 1.1.2, el operador de demanda que atienda la llamada le planteará un cuestionario que ha de contener un mínimo de información. Por el hecho de serle requerida y puesto en su conocimiento que esos datos que se proporcionan facilitarán la resolución del incidente, el consentimiento del alertante al prestarlos se sobnreentiende. Los Datos mínimos a recabar son:

- Nombre y apellidos del alertante, su edad. Es necesario destacar aquí que la identidad del alertante no se facilita a ninguno de los profesionales que prestan servicio en el Centro, salvo requerimiento judicial o necesidades urgentes de represión de un delito flagrante.
- Lugar desde el que se encuentra realizando la llamada (existe en el Centro un localizador automático del origen de las llamadas) .

- Número de teléfono desde el que la realiza (como comprobación de seguridad, porque se refleja en la pantalla del terminal informático del operador de respuesta) .
- Lugar donde se ha producido el incidente (calle, carretera) .
- Descripción del incidente y número de afectados. Consiste este momento del proceso de gestión del incidente en un interrogatorio guiado para la clasificación de la urgencia.
- Otras circunstancias del incidente que puedan resultar de interés a juicio del alertante.

Tras la clasificación (esto es, identificada la emergencia como sanitaria, de tráfico, seguridad pública o multisectorial) de la llamada realizada por el operador de demanda, ésta se traspasa a un Técnico Sectorial (policía nacional, guardia civil, técnico de extinción de incendios, policía local, cruz roja o personal médico) que ya dispone en la pantalla de su terminal de la información recabada por el operador de demanda. El Técnico Sectorial goza de la capacidad de profundizar en el interrogatorio. Después asignará los recursos necesarios para la resolución de los incidentes.

La atención telefónica del incidente es grabada digitalmente y los Jefes de Sala son los encargados de gestionar la información, controlar el acceso a la misma y procurar su seguridad, siendo los únicos autorizados para la consulta de datos históricos del archivo del Centro junto con su Director.

La grabación digital obedece a dos finalidades:

1. Garantizar una adecuada prestación del servicio por los profesionales, quienes siempre contarán con soporte material que pruebe su correcta actuación profesional.
2. Establecer una medida disuasoria de eventuales llamadas jocosas o con finalidades delictivas que hagan movilizar recursos materiales y humanos hacia lugares donde no son necesarios, en detrimento de incidentes efectivamente producidos y que sí requieren de esos medios.

Una vez concluido el incidente y cerrado su seguimiento, los datos personales recabados en el proceso de atención de la urgencia o emergencia son almacenados en soporte

4. LAS MEDIDAS DE SEGURIDAD DEL CENTRO 1.1.2 .

El *Art. 9 de la LOPD, al referirse a la Seguridad de los datos,* establece que el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garantice la seguridad de los datos de carácter personal y evite su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana del medio físico o natural.

Ya adelantamos antes que pese a no existir un fichero de datos personales en sentido estricto, el hecho de manejar unos datos mínimos de carácter personal de los alertantes, implica una responsabilidad que desde el Centro se ha asumido mediante la asunción de las prescripciones que establece al respecto el Reglamento de Medidas de seguridad de los ficheros que contengan datos de carácter personal (RD 994/1999, de 11 de junio), según el cual todos los ficheros (entendamos el término lato sensu) que contengan datos de carácter personal deberán, como mínimo, adoptar las medidas de seguridad calificadas como de nivel básico. Tales medidas son (art. 8 y ss. del Reglamento) las siguientes.

1. *. Documento de seguridad: U*n documento de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información. El documento contiene estos extremos:

a) Ambito de aplicación del documento con especificación detallada de los recursos protegidos. Esto es, el Centro y los Datos personales recabados.
b) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
c) Funciones y obligaciones del personal.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

2.- *Funciones y obligaciones del personal*: Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, en la persona del Jefe de Sala. El responsable del fichero, que es el Director del Centro 112, ha adoptado las medidas necesarias para que el personal conozca las normas de seguridad que

afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

3.- Registro de incidencias.

El procedimiento de notificación y gestión de incidencias contiene un registro en el que se hace constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

4.- Identificación y autenticación de usuarios.

El Director del Centro se encarga de estar al corriente del acceso de los Jefes de Sala, únicos autorizados con él, al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso. El mecanismo de autenticación se basa en la existencia de contraseñas, para lo que existe procedimiento de asignación, distribución y almacenamiento que garantiza su confidencialidad e integridad. Las contraseñas se cambian con la periodicidad que determina el documento de seguridad y mientras estén vigentes se almacenan de forma ininteligible.

5.- Control de acceso.

Los usuarios (los Jefes de Sala) tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. El Director del Centro ha establecido mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

6.- Gestión de soportes.

Los soportes informáticos que contienen datos de carácter personal permiten identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad. Además se encuentran protegidos en cajas de seguridad dada la trascendencia que pudieran tener como material probatorio.

7.- Copias de respaldo y recuperación.

El Director del Centro y, por delegación, los Jefes de Sala, verifican la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

En cualquier caso, el principio de calidad de los datos en poder del Centro ha de conformar su funcionamiento, siendo aquel definido por exclusión en el art. 4 LOPD:”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. 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. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Al elenco de medidas descritas se ha de añadir, además, el Secreto Profesional que conforma la prestación que todos los profesionales realizan en el Centro, desde los Jefes de Sala, hasta los miembros de los Cuerpos y Fuerzas de Seguridad allí destacados. Este genérico derecho-deber se ve especialmente recogido en la LOPD, cuyo *artículo 10.* (bajo la rúbrica *Deber de secreto*), establece que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

5. LOS DERECHOS DE LOS CIUDADANOS.

Por afectado o interesado entiende la LOPD la persona física titular de los datos que sean objeto del tratamiento o recogida de datos personales [art. 3. E) LOPD].

La Comunidad Autónoma de Madrid aprobó recientemente un Decálogo de Derechos del Ciudadano ante la Administración de su Comunidad en el que recoge el “derecho a acceder a los registros y archivos públicos con las limitaciones legalmente establecidas”. Esa prescripción genérica, si bien goza del mérito de dar a conocer al usuario un derecho que le asiste, al cabo no resulta sino una reiteración de lo dispuesto en el artículo 37 de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las administraciones públicas y del procedimiento administrativo común.

Más en concreto la LOPD regula en su a*rtículo 15 (del Derecho de acceso*) establece que el interesado o afectado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. Esta información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible o inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Del mismo modo le asiste un d*erecho de rectificación y cancelación (Artículo 16)*, según el cual el responsable del tratamiento, es decir, la persona encargada de dirigir el Centro 1.1.2, tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la LOPD y, en particular, cuando tales datos resulten inexactos o incompletos. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

Cuando por disposiciones legales especiales se hayan de proporcionar datos personales a fuerzas y cuerpos de seguridad u órganos jurisdiccionales, se notificará convenientemente esta cesión a los interesados (artículo 11 LOPD).

El máximo responsable de la seguridad de los soportes físicos del Centro es su Director, el definido en la LOPD como Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.. Él será el primer órgano administrativo encargado de resolver en el procedimiento de acceso, eventual rectificación y cancelación de los datos.

CONCLUSIONES.

Consecuencia de la reciente puesta en funcionamiento del Centro, aun está en fase de promulgación el pertinente Reglamento de Régimen Interior del Centro de Atención de Urgencias y Emergencias de Extremadura 1.1.2. Este acogerá en su redacción las extremos que el RD 994/1999 prescribe para los ficheros de seguridad de nivel básico y que ya hemos anotado. Hasta tanto, y hasta la pronta publicación del mismo rige a modo de instrucciones de régimen interno dictadas por el Director del Centro como expresión de su potestad organizativa del servicio.

No es en modo alguno descartable la posibilidad de que en el futuro se constituya una Agencia de Protección de Datos Extremeña. Hasta que ese futurible adquiera carta de naturaleza es la Agencia de Protección de Datos nacional la encargada de velar por el cumplimiento de la legalidad vigente en materia de protección de datos personales en nuestra comunidad. Desde esta Administración autonómica ofrecemos, desde la actividad preventiva que aquí he descrito someramente, nuestra más sincera colaboración.

-Título de la comunicación: **LA GESTION Y PROTECIÓN DE LOS DATOS PERSONALES CONTENIDOS EN SOPORTES INFORMÁTICOS EN EL CENTRO DE ATENCIÓN DE URGENCIAS Y EMERGENCIAS DE EXTREMADURA 1.1.2 .**

- **Autor: Víctor García Vega.**
  Asesor de la Consejera de Presidencia de la Junta de Extremadura.
  Ex Becario del MEC en el Departamento de Derecho Público de la Universidad de Extremadura.
  Abogado.

- **Resumen de la Comunicación:**

El Centro de Atención de Urgencias y Emergencias 112 de Extremadura dependiente de la Consejería de Presidencia de la Junta de Extremadura, realiza una labor de atención de los incidentes que puedan requerir los servicios de seguridad pública, entendida ésta lato sensu.

Mediante una simple llamada de teléfono, el usuario del servicio recibe la ayuda que cada emergencia requiera por su naturaleza. Ahora bien, en la gestión del proceso de atención son recabados una serie de datos personales de alertante , e incluso, víctimas de la situación de urgencia.

El tratamiento informático que se da a esos datos personales y los parámetros de seguridad en los cuales se fundamenta el trabajo con los mismos en el Centro a la luz de la reciente Ley Orgánica de Protección de Datos Personales, constituyen el objeto del presente trabajo.