- **Expediente nº.: EXP202100603**

RESOLUCIÓN DE RECURSO DE REPOSICIÓN

Examinado el recurso de reposición interpuesto por **GSMC EVENT PROJECT MANAGEMENT, S.L.** NIF ***B64828973*** (en lo sucesivo, la parte recurrente) en nombre de **GSMA LIMITED**, NIF ***N4004237F***, contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos de fecha 24/02/2023, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 24/02/2023, se dictó resolución por la Directora de la Agencia Española de Protección de Datos en el expediente EXP202100603, en virtud de la cual se imponía a **GSMA LIMITED**, con NIF ***N4004237F****:*

"*Por una infracción del artículo 35 del RGPD, de conformidad con el artículo 83.4.a) del RGPD, y a efectos de prescripción, considerada como grave en el artículo 73.t) la LOPDGDD, una multa de 200.000 euros*."

Dicha resolución, que fue notificada a la parte recurrente en fecha 24/03/2023, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), y supletoriamente en la Ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), en materia de tramitación de procedimientos sancionadores.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00553/2021, quedó constancia de los siguientes:

1) "*En los términos y condiciones de asistencia para el MOBILE WORLD CONGRESS (MWC) de Barcelona 2021, figura que GSMA Ltd. ('GSMA') es la entidad organizadora del MOBILE WORLD CONGRESS (MWC) de Barcelona 2021, a celebrar entre el 28/06 y el 1/07/2021, y realiza entre otros, tratamientos de datos de los asistentes. La web www.mwcbarcelona.com/legal contiene información sobre el Congreso de Barcelona 2022, indica que "GSMA LTD con su principal lugar de negocio localizado en Atlanta, USA, subsidiaria de propiedad entera de la asociación GSM, y con respecto a 4yfn 2022, GSMA 4fyn EVENT MANAGEMENT S.L., una subsidiaria de GSMA LTD., le da la bienvenida al MWC BARCELONA 2022.", y que "GSMA LTD y sus afiliados le proporcionan el evento…" Según información de internet, GSMA (Global System for Mobile Communications, "Sistema Global para Comunicaciones Móviles), es una organización de la industria del móvil que agrupa a operadores de todo el mundo, más de 750 operadores de telefonía móvil y más de 400 Compañías están asociadas como miembros.*
De acuerdo con la reclamada: GSMA EVENT PROJECT MANAGEMENT, S.L. (EPM) es una filial española de GSMA. EPM se ha creado específicamente para prestar servicios relacionados con la gestión del MWC en Barcelona. Las actividades de tratamiento de datos personales de la GSMA están inextricablemente vinculadas a las actividades de EPM.

Por lo tanto, la GSMA trata datos personales en el contexto de las actividades de un establecimiento de la UE y está sujeto al RGPD con arreglo al artículo 3, apartado 1 del RGPD, de modo que no se requiere ningún representante de la UE de conformidad con el artículo 27 del RGPD."

La citada entidad no figura inscrita en el Registro mercantil, si figurando: GSMC EVENT PROJECT MANAGEMENT, S.L., cif ***B64828973*** *y como objeto social:" la prestación de servicios de gestión de proyectos, y de servicios de apoyo en relación con las conferencias congresos, espectáculos y reuniones organizados por cualquier de las sociedades pertenecientes al grupo de las sociedades pertenecientes al grupo"*

Por otro lado, la entidad GSMA 4YFN EVENT MANAGEMENT S.L, CIF ***B67299297****, domicilio Av. de la Reina Maria Cristina S/N Hall 1, Barcelona, tiene objeto social "prestación de servicios de conferencias y eventos. organización de eventos empresariales, sociales, culturales, recreativos o tecnológicos, incluyendo puesta en marcha de ferias de muestras, etc.". En la consulta a la aplicación AXESOR, figura como socio único GSMA LIMITED. A GSMA LIMITED le figura en la aplicación AXESOR como entidad no residente, el NIF* ***N4004237F***

2) *En los términos y condiciones de asistencia, se prevé el proceso de registro que posibilitaría el acceso presencial de los asistentes para el evento para ese 2021, se ha de crear una cuenta en su sitio web, y registrarse para la asistencia, de modo que al llegar a la sede física ya se debía estar registrado. En la sede no habría áreas de apoyo en el registro ni se proporcionarían credenciales impresas. El sistema pretendía tener una verificación de la identidad recogida antes de la llegada de cada persona a la sede. Para el año 2021, el MWC disponía como obligatorio en modalidad de asistencia presencial a su sede, el registro del DNI/ pasaporte, tarjeta de identidad, subiéndolo a su web. Solamente no era exigible subir los documentos identitarios a los que optaran por modalidad "virtual". Estos requisitos se contemplan en el Clausulado de "términos y condiciones generales para la asistencia" MWC 2021, Barcelona" en el que los asistentes tienen que aceptar dichas condiciones.*

En los términos y condiciones de asistencia, se prevé "Identificación: Usted acepta llevar una identificación con foto emitida por su gobierno en forma de pasaporte o tarjeta de identificación nacional de la UE con usted en todo momento durante el Evento. Se le pedirá que presente dicha identificación. Usted es el único responsable de la exactitud de todos los datos personales proporcionados al registrarse para el Evento…"
Además, se recogen en el registro de los usuarios, datos como "nombre, cargo, nombre de la empresa, dirección trabajo, email de trabajo, funciones laborales, número de teléfono, área de interés y fotografía. Si eres un ponente, como información adicional, tu perfil profesional"

3) *La reclamada indicó a la reclamante que el pasaporte y los datos de identificación se requieren y son exigidos por los Mossos d`Esquadra, que la base legitimadora para el tratamiento de la subida de los pasaportes y tarjetas de identidad es el artículo 6.1 c) del RGPD por cuanto se les exigió que facilitarán determinada información a los Mossos: nombre apellidos nacionalidad fecha de nacimiento documento de identidad facilitados fecha de expedición y número de documento, siendo esta manera de*

proporcionarlo novedosa, por ser electrónica y "que ha cambiado para 2021, debido a que los negocios necesitan entorno sin contacto". La reclamada no acredita esta exigencia ni que lo deba ser a través de una web, de su propia titularidad privada, donde se recogen y almacenan. Señaló la reclamada que, en las anteriores ediciones del Congreso, los asistentes llevaban sus tarjetas identificativas en una credencial.

4) *En términos y condiciones generales para los asistentes se indica en privacidad y Protección de Datos que se recogen datos "sobre ti en relación con la provisión de los servicios y para la administración de la cuenta" y que más detalles sobre la política de práctica sobre el tratamiento de datos personales está disponible en Política de Privacidad. En Política de Privacidad se indica que se obtiene información sobre los datos recabados de diversos colectivos, entre otros, los asistentes, a través del sistema de registro de asistentes, la app del evento, tarjetas credenciales digitales y/o impresas, o el sistema de escaneo de reconocimiento facial (en los puntos de acceso, para sesiones o para participar en reuniones de espacios cerrados). Se indica: "información que proporciona voluntariamente: "cuando… creas una cuenta con nosotros, te registras para el evento, ...requieres un servicio…"" La información recogida incluye, pero no se limita a: tu nombre, cargo, nombre de la empresa, dirección trabajo, email de trabajo, funciones laborales, número de teléfono, área de interés y fotografía. Si eres un ponente, como información adicional, tu perfil profesional"*

5) La reclamada explica que, a partir de la toma de los citados documentos identitarios, existe la posibilidad cuando se registra en la web, para el acceso presencial, de dos modos, y uno más residual:

a) *<u>Reconocimiento de verificación automático, se denomina también validación de identidad automática</u>: Junto a los documentos identitarios ya subidos, el programa de la web de la reclamada solicita el consentimiento expreso para usar BREEZ (siglas de entrada fácil con reconocimiento biométrico) que utiliza el reconocimiento facial biométrico. En esta modalidad se puede inscribir tanto durante el registro como después de haberse registrado para el evento. El sistema BREEZ supone que el software de SCANVIS -encargada del tratamiento de la reclamada- realiza una foto de la persona hace coincidir automáticamente la imagen "que nos proporciona con la fotografía en su pasaporte/tarjeta nacional de identidad", "a los que atribuirá unas puntuaciones de coincidencia", "la tecnología analiza los rasgos faciales, tomando medidas de los puntos de datos que componen la cara, como distancia entre ojos, o de la frente a la barbilla, se procesan una serie de puntos de datos para crear un mapa de su cara en tiempo real, esto se convierte en un patrón de datos utilizando un algoritmo para crear el que la reclamada llama "token biométrico", (ficha biométrica, identificador). Ese token es el que posibilita que en los accesos su imagen captada por el lector de FR coincida y se acceda al evento en colas propias diferenciadas, para sesiones o para participar en reuniones de espacios cerrados o incluso áreas restringidas.*

En los accesos sin contacto con BREEZ, se indica que "verificará su imagen capturada por las cámaras contra su token biométrico para finalidades de validación de identificación".

En la información del consentimiento en BREEZ se indica que "Usted consiente para GSMA usando sus datos biométricos obtenidos de las fotografías proporcionadas por

usted para finalidades de validación de identificación en el contexto del registro online y para el MWC Barcelona con finalidades de acceso a la sede", precedido por una casilla que indica" Si, consiento el uso de mis datos biométricos para la validación automática de identidad".

Fundamenta la finalidad en un doble sentido, verificar la identidad cuando asiste al evento, y seguridad en el acceso al recinto. La base jurídica de este tratamiento según indican sería el consentimiento expreso, pudiendo retirar su consentimiento con lo que su validación pasaría a ser manual.

La información sobre el sistema BREEZZ se amplía en la sección BREEZ FAQS -FR
El consentimiento otorgado para la validación automática de la identidad se puede retirar en cualquier momento

a) *Reconocimiento de verificación manual, o validación manual de la identidad: Junto a los documentos identitarios ya subidos, el programa de la web de la reclamada realiza una foto de la persona asistente. Implica que el acceso se va a producir con control a través de presencia humana, que efectúa la verificación cuando el asistente al acercarse escanea su credencial digital en forma de QR de lectura, mostrando la foto tomada que ve la presencia humana al mismo tiempo que a la persona.*

b) *Excepcionalmente, la validación de identificación en papel, presencial in situ*

2) *El denominado por la reclamada: "token biométrico" creado para el proceso de comparación de imágenes se eliminará cuatro (4) semanas después de la finalización del evento. Señala el apartado ¿cómo se utiliza y almacena en mis datos biométricos? que cada token biométrico se cifra y almacena en una base de datos separada de los datos sin procesar utilizados en su creación*

No obstante, en las FAQS de BREEZ se indica que a pesar de que no tiene contacto, todos los asistentes deben tener su credencial digital disponible para ingresar al perímetro externo del lugar y que la credencial digital también será la única forma de acceder a conferencias y sus sesiones de socios.

3) *De acuerdo con la reclamada, la entidad SCANVIS con la que tiene un encargo de tratamiento del sistema de reconocimiento facial para el acceso a la sede, se encuentra en un país fuera de la UE, y GSMA ha suscrito cláusulas contractuales estándar con SCANVIS. Añade que los datos del MWC FR están alojados por Amazon Web Services («AWS») en Alemania.*

4) La reclamada manifestó que en el MWC 2019, permitió que las copias en papel de los documentos de identificación se verificarán manualmente al acceder a la sede de MWC, opción que en 2021 se suprimió-salvo excepciones- por razones de salud y seguridad, con el fin de minimizar el riesgo de propagación de la COVID-19, reduciendo colas y las multitudes en los puntos de acceso. Esto está en consonancia con el "plan de acción de congresos de la Generalitat de Cataluña" al que está sujeto a la GSMA y que exige expresamente la sustitución de procesos manuales por procesos digitales.

5) Según la reclamada al MWC 2021, asistieron aproximadamente 20.000 personas.

10) *Antes del MWC de 2021, la reclamada disponía de un documento de EVALUACION DE IMPACTO que es aportado en alegaciones, titulado: "MWC20 Facial recognition process", creado el 17/12/2019. Tiene nueve apartados con respuesta si/no, relacionados con los principios de protección de datos, figurando cero en toda clase de riesgos, riesgo residual, ninguno. En varias cuestiones reproduce el artículo del RGPD, y la respuesta: Si (ejemplo 4.5, 4.4, 4.6 entre otros) En el primer apartado: "general", se indica que "es una nueva versión del proceso de reconocimiento facial actualizado para el 2020" (en él se mencionan eventos fechados en el Congreso de 2020, ninguno de 2021), y que el "termino BREEZ es el término orientado al cliente para nuestro proceso de reconocimiento facial". Es una revisión del proyecto de 2019, en la que se incluyen sus cambios desde entonces, refiriendo el funcionamiento de BREEZ. En el apartado de ¿Cómo valorarías la importancia de la necesidad de las operaciones de tratamiento? (5.2) no se indica la actividad de tratamiento del reconocimiento facial, indicando: "Con el fin de satisfacer las medidas de seguridad en el evento, hemos sido instruidos por el Formulario de la Policía Española para poner en marcha procesos estrictos para garantizar que todos los asistentes sean examinados a través de una verificación de pasaporte/documento de identidad de la UE antes de que puedan ingresar en el recinto, y recoger sus credenciales. Los procesos heredados se basan en verificaciones manuales que pueden ser lentas y brindar una experiencia negativa en el evento. A través del uso de la tecnología descrita en este DPIA, podemos automatizarlos para permitir un uso mucho más proceso eficiente, así como un evento más preciso y seguro."*

En el apartado 5.3 sobre la proporcionalidad de las operaciones de tratamiento solo se indica que sí, "para satisfacer los requerimientos, es necesario crear tokens biométricos basados en las fotografías". El documento carece de evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; el uso del reconocimiento facial para el acceso a los eventos, de su evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, del artículo 35 del RGPD y de las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. Igualmente, relaciona los datos de los pasaportes y tarjetas de identidad que manifiesta son exigidos por los Mossos d`Esquadra que presuntamente tienen una finalidad, para conectarlo con la foto que se hacen con el software, que inicia el proceso de reconocimiento facial, emparejando su identidad para facilitar el acceso."

TERCERO: La parte recurrente ha presentado en fecha 24/03/2023, en esta Agencia Española de Protección de Datos, recurso de reposición, fundamentándolo, básicamente, en:

El incumplimiento del artículo 35 del RGPD que sanciona la resolución se refiere a la "falta de diligencia" en la elaboración de una evaluación de impacto de protección de datos (EIPD) para el tratamiento de datos biométricos del reconocimiento facial ("RF")

utilizado para el acceso al MOBILE WORLD CONGRESS (“MWC”) en su edición de 2021. Concretamente se indica que GSMA: “*ha aportado una evaluación de impacto que fue meramente nominal, por cuanto no ha examinado sus aspectos sustantivos, ni valorado los riesgos ni la proporcionalidad y necesidad de la implantación del sistema, su afectación a los derechos y libertades de los interesados y sus garantías*”

En la graduación de la infracción se estimó, aplicando el artículo 83.2.a) del RGPD, que el uso del RF afectaba a la totalidad de los asistentes, 20 mil personas, sin discriminar los que de entre ellos utilizaron el sistema, que ascendió a 7.585 personas y que ya se manifestó durante la tramitación del expediente.

Solicita que en función de que los datos reales para tener en cuenta en la agravación son de casi un tercio menos de personas de las consignadas, debería tenerse en cuenta para ajustar proporcionalmente la sanción a la baja.

Aporta en un anexo, especificación en detalle de la cifra de personas que usaron el sistema de RF con detalle de accesos realizados.

En el certificado, indica específicamente, que, de los 17.462 asistentes registrados, utilizan el RF para acceder al recinto 7.585 personas.

Junto al certificado aporta unas 240 páginas en formato Excel, de registro de datos, que bajo el indicativo “*Scan Date*” van del 28 al 1/07/2021, (cuatro días), con un total de 7.585 registros asociados cada uno contiene su serie de identificador formado por letras y números, que se correspondería según lo alegado, con las personas registradas, se deduce que todas distintas, correspondientes a los asistentes, figurando: “ *registros completados*”, así como la hora de acceso “*Scan Time*” y la puerta por la que acceden.

FUNDAMENTOS DE DERECHO

I
Competencia

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 123 de la Ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP) y el artículo 48.1 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD).

II
Contestación a las alegaciones presentadas

Analizada la alegación de las personas afectadas en el alcance del tratamiento en relación con la circunstancia contenida en la resolución dentro del articulo 83.2 a) del RGPD, se observa que, en el cuadro aportado, no se indica de esas personas, 7.585, una vez completado el registro, cuantas ocasiones accedían al día, o durante los cuatro días que duró el Congreso.

En la resolución recurrida no se llega a considerar como hecho probado más que fueron 20.000 los asistentes, ahora certificado a 17 mil, tampoco que estuvieran directamente afectados por el tratamiento, esto es, que utilizaran el sistema RF. Por el contrario, se estimaba que, partiendo del hecho de tratarse de un evento de asistencia masiva, el número de registrados reales de 7.585 usuarios del RF, no desmiente ese factor. Esto es, se consideró como agravante el tipo de evento de asistencia masiva que se trataba, no el número exacto de afectados directos por este tipo de tratamiento.

Además, dentro del tanto por ciento alto que representan los 7.585 asistentes que optaron por este sistema del RF, sobre el total de los 17.462, superaría el 40%, un grado elevado para entrar en consideración. Por lo demás, no se tiene estimación de la intensidad del uso del RF por días, por lo que se conviene aún con estos datos, que afecta a una gran masa de asistentes y que han de usar intensivamente el sistema, en cada ocasión que acceden a la sede. Este elemento agravatorio, junto con los no discutidos "*intencionalidad o negligencia en la infracción*" y especialmente la vinculación de la actividad profesional del tratamiento habitual de datos personales, no pude disminuir la antijuridicidad agravada que supone naturaleza del tratamiento y las personas afectadas sobre las que recae la infracción imputada, ausencia de una EIPD. Así pues, se estima que las circunstancias consideradas en la resolución se ajustan en su graduación.

En cuanto a la alegación de la recurrente que considera se le sancionó por "*falta de diligencia*" en la EIPD, no se indicó tal extremo en la resolución, sino como referente a la conducta, para agravarla, no a la calificación de la EIPD. Lo que concluye la resolución es que una EIPD que no contempla sus elementos esenciales no es efectiva ni cumple objetivo alguno.

III
Conclusión

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

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

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por **GSMC EVENT PROJECT MANAGEMENT, S.L.** en nombre de **GSMA LIMITED** NIF ***N4004237F*** **contra** la resolución de esta Agencia Española de Protección de Datos dictada con fecha 24/03/2023, en el expediente EXP202100603.

SEGUNDO: NOTIFICAR la presente resolución a **GSMC EVENT PROJECT MANAGEMENT, S.L.**

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea ejecutiva la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el artículo 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17/12, mediante su ingreso en

la cuenta restringida nº ES00 0000 0000 0000 0000 0000, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), los interesados podrán interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

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

180-111122

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