CNS 13/2018

Dictamen con relación a la consulta de un ayuntamiento sobre el uso de WhatsApp por parte de una administración local.

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito de un ayuntamiento en el que plantea varias cuestiones respecto a los riesgos y responsabilidades que supone el uso de la aplicación de WhatsApp para determinados fines en el contexto de una administración local.

La consulta plantea el grado de adecuación a la normativa de protección de datos en relación con diferentes casos en los que se estaría planteando la posibilidad de utilizar WhatsApp. Estos casos se refieren a la comunicación con los padres de menores usuarios de la ludoteca municipal; con la comunicación entre miembros del Consejo Municipal de Cultura (concejales, miembros de asociaciones del municipio...); con la comunicación entre miembros del Consejo de la Infancia (concejales, menores de edad representantes de la escuela...); así como en relación con un grupo de WhatsApp que habría creado un grupo de jóvenes del pueblo.

La consulta pregunta, entre otros aspectos, respecto a la responsabilidad que podría tener el Ayuntamiento en relación con la utilización de este canal de comunicación, o respecto al consentimiento que habría que pedir a los participantes del grupo.

Analizada la petición, y visto el informe de la Asesoría Jurídica, se dictamina lo siguiente.

I

(...)

II

El Ayuntamiento pregunta sobre el grado de adecuación a la normativa de protección de datos en relación con diferentes casos en los que, según la consulta, el Ayuntamiento estaría planteando la posibilidad de utilizar WhatsApp, en concreto, en los siguientes supuestos:

Caso 1: Grupo de WhatsApp municipal en el que se incluiría a los padres de niños usuarios de la ludoteca municipal, cuyo administrador sería un trabajador municipal que utilizaría un teléfono de propiedad municipal. Según la consulta, la finalidad es la divulgación de actos que se realizan en la ludoteca, modificaciones de horarios, cancelaciones de actos, etc.

Caso 2: Grupo de WhatsApp del Consejo de Cultura, cuyos integrantes serían sus miembros (concejales, miembros de asociaciones del pueblo...) y personal municipal, y el administrador del grupo sería el Ayuntamiento. La finalidad sería, según la consulta, el envío de convocatorias, cancelaciones, etc.

Caso 3: Grupo de WhatsApp del Consejo de Infancia, cuyos integrantes serían los miembros del Consejo (concejales, menores de edad representantes de la escuela...) y personal municipal, y el administrador del grupo sería el Ayuntamiento. La finalidad sería, según la consulta, el envío de convocatorias, cancelaciones, etc. En este caso, la consulta remarca la peculiaridad de que se incluiría a menores de edad en el grupo.

En cuanto a los casos 1, 2 y 3, el Ayuntamiento plantea las mismas dudas, referidas, en síntesis, al consentimiento de las personas participantes en los grupos, o a la responsabilidad del Ayuntamiento respecto a los comentarios o datos que los participantes pudieran difundir.

Caso 4: Grupo de WhatsApp que, según la consulta, habrían creado jóvenes del pueblo. La consulta no aporta información sobre la finalidad del grupo. La consulta puntualiza que el Ayuntamiento no es el administrador del grupo, y que se habría añadido a este un trabajador municipal que utiliza un número de teléfono del propio Ayuntamiento. La consulta plantea si, al no ser administrador del grupo, el Ayuntamiento tendría alguna responsabilidad como administración pública, y si debería realizar alguna gestión en relación con la LOPD (Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal).

Situada la consulta en estos términos, nos referiremos de forma conjunta a los casos 1, 2 y 3 que plantea el Ayuntamiento, ya que son sustancialmente coincidentes en cuanto a sus características (son grupos creados por el propio Ayuntamiento para comunicar información sobre servicios o actividades municipales) y en cuanto a las dudas que plantean; de forma separada se hará referencia al caso 4, citado.

III

A modo de introducción, hay que hacer notar que los medios o servicios de comunicación que pueden utilizar las administraciones públicas (en este caso, un ayuntamiento), ya sea para relacionarse con los ciudadanos o con otras administraciones públicas, o como canal de comunicación interno dentro de su propia estructura, pueden ser muchos y de naturaleza muy variada, medios de comunicación tradicionales (prensa, radio o televisión), internet, webs propias de los organismos y entes públicos, intranets corporativas, correo ordinario, comunicación por vía telefónica, comunicación presencial, etc.

En la medida en que el uso de cualquier medio, canal o servicio de comunicación por parte del Ayuntamiento comporte un tratamiento de información personal, este tratamiento deberá someterse a los principios y garantías de la protección de datos, es decir, el RGPD, que entró en vigor el 25 de mayo de 2016, y que será aplicable a partir del 25 de mayo de 2018 (artículo 99 del RGPD). También hay que tener en cuenta, hasta la plena entrada en vigor del RGPD en la fecha indicada, las previsiones de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y el Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (RLOPD).

Desde el momento en que el Ayuntamiento habilite un canal de comunicación con los ciudadanos o sus trabajadores o concejales, el tratamiento de datos de los afectados o interesados (artículo 4.1 del RGPD y artículo 3.e de la LOPD) que se derive deberá estar sometido a los principios y garantías de la normativa de protección de datos, en los términos de la normativa mencionada.

En concreto, el Ayuntamiento se refiere a la utilización del sistema de mensajería instantánea (SMI) de WhatsApp. Los SMI son canales de comunicación en tiempo real entre dos o más personas, basada principalmente en texto, que se envía mediante dispositivos conectados a una red como internet. Estas aplicaciones, como la de WhatsApp o similares, permiten adjuntar mensajes de texto, y archivos de imágenes, vídeo y audio, es decir, otros contenidos aparte del propio mensaje de texto. Además de utilizar la mensajería básica, los usuarios de estos sistemas pueden hacer videoconferencias, crear grupos más o menos numerosos (como sería el caso de los grupos a los que se refiere la consulta), chats y compartir información, archivos o contactos.

En cualquier caso, está claro que el hecho de crear un grupo de WhatsApp —o, por extensión, de otros SMI similares, de los muchos disponibles actualmente en el mercado— implica un tratamiento de datos de carácter personal. Por un lado, los datos personales identificativos de los miembros del grupo (nombres, seudónimos utilizados, número de móvil, fotografía de perfil, etc.) y, por otro, la información personal que puedan contener los mensajes que se envían, ya sean por escrito, mensajes de voz, imágenes, etc.

Desde el momento en que esta información se refiere a personas físicas se trata de información personal sometida a la protección de la normativa correspondiente (LOPD y RLOPD, hasta el 25 de mayo de 2018, y RGPD, a partir del 25 de mayo de 2018).

El Parlamento de Cataluña ha dictado la Resolución 280/XI, del Parlamento de Cataluña (BOPC 220, de 27 de septiembre de 2016), sobre el uso de servicios de comunicaciones por el Gobierno, según la cual se insta al Gobierno a fomentar el uso de SMI, por parte de las administraciones públicas, que tengan determinadas características, entre otras, una política de privacidad de acuerdo con la legislación vigente en materia de protección de datos, que practiquen la transparencia, y que incorporen las medidas que establece el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de acuerdo con los términos establecidos.

Recordamos que esta Autoridad ha analizado la utilización de SMI desde la perspectiva de la protección de datos en ocasiones anteriores, así como, específicamente, el contenido de la Resolución 280/XI, citada (dictámenes CNS 24/2013, CNS 55/2016, o CNS 54/2017, a los que nos remitimos).

IV

Según el artículo 4.7 del RGPD (y artículo 3.b de la LOPD), es responsable del tratamiento: "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros";

El responsable del fichero o tratamiento es quien, en primera instancia, está obligado a dar cumplimiento a los principios y garantías de la protección de datos personales.

Cuando una administración pública, como un ayuntamiento, tiene que tratar información personal de los afectados para el cumplimiento de sus funciones y competencias, esta administración es la primera responsable de los ficheros o del

tratamiento de datos que lleva a cabo. Así, cuando el Ayuntamiento ejerce sus funciones en relación con la gestión de espacios municipales (como una ludoteca) o en relación con competencias municipales en el ámbito de la cultura o de la infancia, entre otras, el tratamiento de datos que se genera en cumplimiento de estas competencias municipales conlleva que el Ayuntamiento tenga que velar por el cumplimiento de la normativa de protección de datos.

Por lo tanto, el Ayuntamiento será responsable de la información personal que trate mediante cualquier SMI o que recoja por esta vía.

Al margen de esto, la utilización de SMI por parte de las administraciones públicas presenta una singularidad, ya que es el propio usuario (la persona física) quien decide instalarse una determinada aplicación de mensajería instantánea, mediante la cual puede relacionarse con terceros, incluidas, si es el caso, las administraciones públicas.

Como ha recordado esta Autoridad, las empresas titulares de los SMI (como WhatsApp) deciden qué tratamiento hacen de los datos de los usuarios que deciden utilizar su servicio de mensajería, y las que establecen las condiciones de uso correspondientes. En la información que, habitualmente, se pone a disposición de los usuarios a través de los respectivos sitios web (a los efectos que interesan, www.whatsapp.com), estas empresas determinan qué información utilizarán y cuál no, incluyendo datos personales del usuario y los contactos del usuario, y para qué fines.

A partir de ahí, cualquier empresa de SMI que trate datos de sus usuarios también tendrá que cumplir los principios y garantías de la normativa de protección de datos, en los términos que corresponda.

Ciertamente, es la empresa responsable del SMI la que debe garantizar que cumple la normativa de protección de datos, pero esta es una cuestión que también debe tener presente el Ayuntamiento a la hora de decidir prestar sus servicios mediante un determinado canal de comunicación. El Ayuntamiento debe asegurarse de que el canal de comunicación se ajusta a las exigencias de la normativa.

El Ayuntamiento es responsable de tratar datos personales en relación con el uso de la ludoteca o en relación con la actividad de los consejos de Cultura o de Infancia, entre otros, y como tal es responsable de la información personal que recoge de los propios afectados (padres de la ludoteca, representantes vecinales, alumnos de escuela, o de sus propios concejales y trabajadores municipales) y del tratamiento posterior que se haga con esa información.

A los efectos que interesan, desde el momento en que el Ayuntamiento valora la posibilidad de crear un grupo o un chat de SMI (WhatsApp u otros similares) para comunicarse con los afectados que integrarán el grupo (ciudadanos, concejales, trabajadores municipales, etc.) y gestionar así determinada actividad o servicio municipal, deberá tener en cuenta que eso generará un flujo informativo (de datos identificativos y de contacto del resto de los miembros de cada grupo, y de la información que se comparta en el grupo, como, por ejemplo, mensajes de texto o de sonido, imágenes…), entre los participantes, que debe ajustarse a las exigencias de la normativa de protección de datos.

En este sentido, recordamos que hay una diferencia sustancial entre las diferentes comunicaciones que puede establecer el Ayuntamiento, en el caso que nos ocupa.

Por un lado, nada impide que el Ayuntamiento trate los datos de los que dispone como responsable (por ejemplo, de los padres de la ludoteca) para establecer con ellos una

comunicación de forma directa y bidireccional, para el cumplimiento de fines legítimos; en este caso no hay acceso de terceros a la información que se pueda compartir entre el Ayuntamiento y el afectado.

Ahora bien, si el Ayuntamiento, como responsable de los datos personales de los afectados, trata los datos de contacto para crear una lista de participantes para crear un grupo de SMI, deberá tener una base legal adecuada para llevar a cabo este tratamiento, teniendo en cuenta que en este caso el flujo informativo se multiplica, ya que tanto los datos de contacto como el contenido de los mensajes estarán al alcance de todos los participantes del grupo.

Esto obliga al Ayuntamiento, a la hora de crear grupos de SMI, a ser especialmente cuidadoso y a analizar una serie de cuestiones, como la base legal del tratamiento y la información que dará a los miembros del grupo, con el fin de que el flujo informativo mencionado (entre todos los participantes del grupo) se ajuste a las exigencias de la normativa de protección de datos.

Hecha esta consideración general, hay que decir que WhatsApp, al que se refiere la consulta, es una empresa radicada fuera de la Unión Europea. Ahora bien, según dispone el artículo 2.2 del RGPD:

> "2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:
> a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o
> (...)".

Por lo tanto, cuando WhatsApp se utiliza en dispositivos de usuarios que, como en el caso que nos ocupa, se encuentran en España, es indubitada la aplicación de los principios y garantías de la normativa de protección de datos personales (LOPD, RLOPD y RGPD) a los casos objeto de consulta.

Esta Autoridad ha puesto de manifiesto en ocasiones anteriores varias problemáticas que presenta el tratamiento de datos por algunas empresas de mensajería instantánea, entre otras —aunque no exclusivamente—, WhatsApp, desde la perspectiva de la protección de datos.

Son varias las actuaciones llevadas a cabo en los últimos años por autoridades europeas de protección de datos en relación con el tratamiento de datos de usuarios en la UE por parte de WhatsApp, como, por ejemplo, los informes e investigaciones de varias autoridades de protección de datos (Autoridad de Protección de Datos de Holanda y Autoridad Federal de Canadá, de enero de 2013). También hay que recordar la intervención del GT29, mediante varios escritos dirigidos a Facebook y WhatsApp (27 de octubre de 2016, 16 de diciembre de 2016 y 24 de octubre de 2017), en los que se han puesto de manifiesto varias deficiencias en el mecanismo de prestación del consentimiento de los usuarios a raíz de la previsión de comunicación de datos a Facebook, ("Facebook family of companies"), para un conjunto de finalidades que incluyen el marketing y la publicidad.

Entre otras cuestiones, hay que tener en cuenta el principio de consentimiento (artículo 4 de la LOPD y artículo 4.11 del RGPD). Es notorio que varias empresas de SMI, entre otras, WhatsApp, incluyen condiciones generales o estándares, fijadas y modificadas unilateralmente por la empresa, sin dejar margen de opción al usuario. Aunque puede

ser razonable que el usuario tenga que aceptar necesariamente un cierto nivel de tratamiento de sus datos en la medida en que eso pueda ser necesario desde un punto de vista técnico para la prestación del servicio de mensajería, ello no implica que resulte adecuada la prestación de un consentimiento general y, podríamos decir, "indiscriminado", en el sentido de una aceptación incondicionada, para utilizar los datos del usuario o de terceras personas para fines que no resultan estrictamente necesarios para la prestación del servicio.

En este sentido, el RGPD (considerandos 32 y 43) establece la relevancia de la granularidad en la prestación del consentimiento, elemento que no resulta nuevo en el ámbito que nos ocupa, pues ya había sido expresamente citado y recomendado por el GT29, en su Dictamen 2/2013, sobre aplicaciones en dispositivos inteligentes ("Opinion 2/2013, on apps on smart devices"), de 27 de febrero de 2013, y reiterado por el GT29 en el documento "Guidelines on Consent under Regulation 2016/679", de 28 de noviembre de 2017.

Como se desprende de la información disponible en la web de WhatsApp ("Términos de Servicio de WhatsApp": "Libreta de direcciones. Nos proporcionas regularmente los números de teléfono de los usuarios de WhatsApp y los demás contactos que tienes en la libreta de direcciones de tu teléfono móvil [...]"), se puede apuntar que WhatsApp no aplica un consentimiento granular que permita al usuario seleccionar los contactos a los que tendrá acceso.

Por otra parte, como se desprende de las consideraciones y advertencias provenientes de las autoridades de protección de datos europeas en los últimos años y, más recientemente, de la Resolución R/00259/2018, de la Agencia Española de Protección de Datos, en la que se sanciona a WhatsApp por ceder a Facebook datos personales sin el consentimiento adecuado de los afectados, WhatsApp no aplicaría el consentimiento parcelado en relación con las cesiones de datos de los usuarios a terceros, y no habría permitido a los afectados excluir determinada información personal de dichas cesiones a Facebook, que, a tenor de las recientes opiniones y resoluciones de diversas autoridades de protección de datos, serían cesiones claramente innecesarias y, por tanto, habrían tenido que estar sujetas al consentimiento de los usuarios.

También debe tenerse en cuenta que el RGPD da carta de naturaleza al principio de transparencia (considerandos 39 y 58 del RGPD). Según dispone el artículo 5.1.a) del RGPD, los datos deben ser tratados de manera lícita, leal y transparente con relación al interesado. El principio de transparencia, vinculado en el RGPD a los principios de licitud y de lealtad, engloba específicamente el derecho de informar a los afectados sobre una serie de cuestiones, en los términos del artículo 13 del RGPD (que en algunos aspectos va más allá de lo dispuesto en el artículo 5 de la LOPD), que recoge la información que el responsable, en este caso la empresa responsable de un SMI, en este caso, WhatsApp, debería dar al afectado, también de manera granular y por capas ("layered and granular information"). Como ha hecho saber esta Autoridad, no solo WhatsApp, sino también otros SMI de utilización bastante habitual podrían presentar carencias en cuanto al cumplimiento de las exigencias del artículo 13 del RGPD, en definitiva, de la información que proporcionan a sus usuarios.

Finalmente, la tercera consideración que, sin ánimo de exhaustividad, debería tenerse en cuenta respecto al tratamiento de los datos de los usuarios por parte de WhatsApp (a la que específicamente se refiere la consulta y a la que, por tanto, nos referimos) se sitúa en el ámbito de la seguridad aplicable.

Entre otras cuestiones, como ha hecho saber esta Autoridad (fundamento jurídico VIII del Dictamen CNS 24/2013 y fundamento jurídico X del Dictamen CNS 55/2016), las previsiones que puedan explicitar las empresas responsables (en este caso, WhatsApp) respecto a la confidencialidad con la que tratan los datos de los usuarios (medidas de encriptación de la información, etc.) son especialmente relevantes. En cualquier caso, hacemos notar que el RGPD, aplicable a partir del 25 de mayo de 2018, configura un sistema de seguridad que no se basa en los niveles de seguridad básico, medio y alto (según el esquema de la LOPD y el RLOPD), sino en determinar, a raíz de una previa valoración de los riesgos, qué medidas de seguridad son necesarias en cada caso, teniendo en cuenta el tipo de información tratada (considerando 83 y artículos 24.1 y 32.1 del RGPD). En el artículo "WhatsApp rolls out end-to-end encryption to its over one billion users", de la organización EFF (disponible en traducción al castellano: https://www.eff.org/es/deeplinks/2016/04/whatsapp-estrena-cifrado-de-fin-fin-para mas-de-un-billon-de-usuarios), se analiza el sistema de cifrado de WhatsApp, que se califica como un sistema fuerte.

Por la información disponible (incluida su web), WhatsApp incorpora el cifrado de extremo a extremo, de manera que solo el emisor y el receptor (y no WhatsApp) pueden leer el mensaje. Este tipo de cifrado estaría activado por defecto para todos los usuarios que utilizan las últimas versiones de la aplicación, y no se podría desactivar. Ahora bien, según otra información disponible, si bien el cifrado de extremo a extremo de WhatsApp ofrece garantías, también se detectan ciertas carencias que podrían llevar a que estas medidas no fueran suficientemente operativas. En concreto, el informe de Amnistía Internacional (AI) "For your eyes only? Ranking 11 technology companies on encryption and human rights" (https://www.amnesty.org/download/Documents/POL4049852016ENGLISH.PDF) habría detectado que WhatsApp no informa a los usuarios de que, si se hacen copias de seguridad en la nube, esta información no estaría cifrada. En definitiva, existen vulnerabilidades detectadas —no solo en WhatsApp sino también en otros SMI disponibles en el mercado— que deberían tener en cuenta no únicamente los propios usuarios que se instalan aplicaciones de mensajería instantánea, sino, lógicamente, las administraciones públicas que quieren utilizarlas.

Por todo lo expuesto, y sin perjuicio de algunas carencias, desde la perspectiva de la protección de datos, en relación con los principios de protección de datos y la problemática específica que puede representar un determinado SMI (en este caso, WhatsApp) con respecto al tratamiento de datos de los usuarios de estos SMI, que las administraciones deben tener en cuenta, en el caso objeto de consulta resulta clave contextualizar la posibilidad de crear y utilizar los grupos de WhatsApp en los supuestos planteados, en atención al tipo de información que, presumiblemente, y dada la información disponible, se podría tratar, y a la finalidad prevista.

V

Cuando un ayuntamiento, como responsable (artículo 4.7 del RGPD), quiere utilizar un SMI para sus comunicaciones con los ciudadanos, debe tener en cuenta, de entrada, qué tipo de comunicación quiere establecer, en relación con qué servicio o prestación, a qué personas o colectivos va dirigida la información o el servicio en cuestión, qué tipo de información se verá afectada, etc.

Desde la perspectiva de la protección de datos no tiene las mismas implicaciones utilizar canales de comunicación con los ciudadanos con el fin de dar información o recibir consultas sobre cuestiones diversas (información sobre el estado del tráfico o sobre determinados servicios municipales, sobre actividades lúdicas o culturales, etc.),

que implica un flujo de información que podríamos calificar como de general o "inocua", que la utilización de los SMI para comunicar un posible hecho delictivo, un accidente (comunicaciones a cuerpos policiales, a servicios sanitarios, ambulancias, servicios a personas dependientes que requieren atención domiciliaria, etc.) o cuando se trata de comunicaciones relacionadas con personas menores de edad o colectivos vulnerables, que pueden ser objeto de especial protección y atención por parte de las administraciones públicas y, en lógica consecuencia, titulares de información especialmente sensible (artículo 99 del RGPD y artículo de la LOPD).

Son varios los ejemplos de utilización de SMI por parte de administraciones públicas y de entidades públicas y privadas, y hay que apuntar que, en muchas de estas comunicaciones, no se da un flujo de información especialmente protegida o sensible. En otros casos, por ejemplo, si se emplea un SMI para la transmisión de datos de salud a servicios asistenciales o para la comunicación entre una víctima de una agresión y los cuerpos de seguridad, sí podría darse un flujo informativo de datos que la normativa protege especialmente. Nos remitimos, en este sentido, a las consideraciones hechas en el fundamento jurídico VIII del Dictamen 55/2016, en lo relativo a la problemática que, desde la perspectiva de la protección de datos personales, presenta la utilización de SMI en casos en los que no solo es previsible, sino que es habitual que se comunique información sensible, en los que incluso puede ser desaconsejable la utilización de determinados SMI.

Ahora bien, por la información disponible, el tipo de información personal que podría ser objeto de comunicación en el contexto de los grupos 1, 2 y 3 (divulgación de actividades, convocatoria o cancelación de actos, de la ludoteca municipal, del Consejo de Cultura o del Consejo de Infancia) no sería información merecedora de especial protección a los efectos de la normativa de protección de datos.

Por lo tanto, teniendo en cuenta el flujo informativo y la finalidad de los grupos que crearía el Ayuntamiento, que no comportan, por la información disponible, tratamiento de información especialmente protegida, no se puede descartar la utilización de un SMI ampliamente conocido y utilizado por la ciudadanía, como podría ser WhatsApp, al que se refiere específicamente el Ayuntamiento, o de otros SMI de prestaciones y características similares, aunque habrá que tener en cuenta las consideraciones que se harán a continuación.

VI

Dicho esto, la consulta se refiere al consentimiento de los padres (en relación con el caso 1, aunque se plantea la misma duda para los casos 2 y 3) para que su número de teléfono sea incluido en el grupo de WhatsApp. Aparte de esto, la consulta pregunta qué otros parámetros habría que tener en cuenta para dar cumplimiento a la normativa de protección de datos. En concreto, el Ayuntamiento pregunta si sería correcto (además de acotar al máximo la finalidad del grupo) incluir una cláusula de políticas de buen uso por parte de los usuarios (ciudadanos) del grupo, de compromiso de que no cederán a terceros ni teléfonos del grupo, ni la fotografía del perfil, ni siquiera las imágenes que se puedan compartir en el grupo (la consulta cita como ejemplo "que algún padre colgara en el grupo una foto en la que se identificara a los asistentes al evento, adultos y menores"). La consulta también expone la duda de hasta qué punto el Ayuntamiento sería responsable de los comentarios que los miembros puedan hacer o de los datos que puedan mostrar en el grupo, y sobre la potestad de expulsar a alguien del grupo en el caso de que no lo utilizara de un modo responsable. La consulta explicita que estas dudas son extensibles a los casos 2 y 3.

De entrada, formar parte de un grupo de WhatsApp supone que todos los participantes del grupo tendrán acceso a la información de contacto de los demás miembros (nombre, número de teléfono, estado, foto o imagen de perfil, si es el caso...), en definitiva, que habrá una comunicación de datos personales entre los participantes del grupo, no solo en lo relativo a los mensajes transmitidos por el Ayuntamiento sino también a los datos de contacto que utiliza WhatsApp y que son visibles para los diferentes miembros de un grupo de WhatsApp (nos remitimos, para mayor detalle, a las informaciones disponibles en el apartado de preguntas frecuentes de la web de WhatsApp). También tendrán acceso al contenido de los mensajes que puedan enviar los ciudadanos mediante este SMI.

Uno de los principios fundamentales en que se basa el tratamiento de datos personales es el principio de licitud. Según dispone el artículo 6 del RGPD:

> "1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
>
> a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
>
> (...)".

Según el artículo 4.11 del RGPD, el consentimiento del interesado es: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen";

La finalidad de crear los grupos objeto de consulta es la de informar a las personas participantes de diferentes cuestiones e informaciones de interés, finalidad que, de entrada, se puede lograr por otros medios. Esto lleva a considerar que la base legal sobre la que debería fundamentarse la participación de las personas afectadas en los grupos de WhatsApp (casos 1, 2 y 3 de la consulta) debería ser el consentimiento de estas personas afectadas, que voluntariamente accedan a formar parte del grupo mediante una declaración o acción afirmativa clara.

Quizá el Ayuntamiento disponga del teléfono u otros datos personales identificativos y de contacto de las personas que se prevé que puedan participar en los grupos (padres de menores que asisten a la ludoteca, representantes de asociaciones del municipio y, obviamente, de los concejales o personal del propio ayuntamiento) para determinados fines (cobro de cuotas de la ludoteca, gestión de la relación laboral de los trabajadores municipales, ejercicio de las funciones de los concejales, etc.).

Ahora bien, en atención al principio de finalidad, para tratar los datos de contacto de las personas afectadas con el fin de crear grupos de SMI para la gestión de determinadas actividades, el Ayuntamiento debería disponer del consentimiento de todos los afectados, no solo de las personas externas al Ayuntamiento (ciudadanos), como parece apuntar la consulta.

Esto es así porque, por ejemplo, el Ayuntamiento dispone de datos personales de sus trabajadores para diferentes finalidades —como las derivadas de la propia relación laboral—, por lo que el tratamiento de estos datos por parte del Ayuntamiento puede ser lícito (ej. artículo 6.1.b del RGPD), sin que sea necesario el consentimiento del trabajador. Ahora bien, no parece que la pertenencia de un trabajador municipal a uno de los grupos de mensajería instantánea objeto de consulta resulte exigible al trabajador por el mero hecho de su vinculación laboral con el Ayuntamiento.

Por lo tanto, el Ayuntamiento debería solicitar el consentimiento (una "clara acción afirmativa", en los términos del artículo 4.11 del RGPD) no solo a los "ciudadanos" (padres de los menores que asisten a la ludoteca —caso 1—, miembros de asociaciones del pueblo —caso 2— o alumnos de escuela —caso 3—), sino también a los trabajadores municipales o concejales que, si es el caso, puedan participar en el respectivo grupo, consentimiento que habría que recoger, en cualquiera de los casos, de forma previa a la creación de los grupos de mensajería instantánea.

Ahora bien, hay que recordar que, para que la base del tratamiento sea el consentimiento, es necesario que las personas participantes en los grupos tengan otros canales alternativos de comunicación con el Ayuntamiento para las finalidades previstas, es decir, que no se les imponga como única vía de comunicación el tener que formar parte del grupo de WhatsApp. De ser así, y si no existieran otros canales alternativos, no parece que el consentimiento pueda ser considerado como "libre", en los términos del artículo 4.11 del RGPD.

Hay que añadir que el caso 3, referido al grupo de WhatsApp del Consejo de Infancia, presenta la particularidad de que formarían parte de él, entre otros, menores de edad representantes de la escuela. La consulta no aporta más información sobre la edad de estos menores, o sobre los centros escolares que podrían formar parte del grupo.

Hay que tener en cuenta que, en relación con las condiciones aplicables al consentimiento de los menores, el artículo 8 del RGPD dispone que:

> "1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años".

También hay que añadir que en el caso de España existe normativa que rebaja esa edad. Así, el artículo 13 del RLOPD, de momento aún vigente, prevé la posibilidad de que los menores de edad que sean mayores de 14 años puedan prestar por sí mismos el consentimiento para el tratamiento de sus datos, en los siguientes términos:

> "1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.
> (...)
> 4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado, en su caso, por los padres, tutores o representantes legales".
>
> (...)".

En relación con esto, recordamos que el Proyecto de ley orgánica de protección de datos personales (BOCCGG, de 24.11.2017), que se encuentra en fase de tramitación parlamentaria, dispone, en su artículo 7, lo siguiente:

"Artículo 7. Consentimiento de los menores de edad.

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de trece años.
Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

(...)".

Dado que, como se ha apuntado, la licitud del tratamiento de los datos de estos alumnos estaría fundamentada en el consentimiento previo, el Ayuntamiento deberá pedir el consentimiento a los propios alumnos, en el caso de que sean menores mayores de 14 años, o, en el caso de que se trate de menores que no tienen todavía 14 años, el Ayuntamiento deberá disponer del consentimiento de sus padres o representantes legales. Esto sin perjuicio de las condiciones específicas que haya establecido el SMI para darse de alta en la aplicación.

En conclusión, el hecho de que el Ayuntamiento disponga del consentimiento de todos los participantes de los grupos 1, 2 y 3 legitimaría no solo la creación de los grupos, sino, en lógica consecuencia, el acceso por parte de los participantes de cada grupo a los datos del resto de los usuarios del grupo (número de teléfono, foto o imagen de perfil, etc.) y a la información que estos compartan (mensajes de texto, mensajes de voz, fotografías, etc.), para dar cumplimiento a la finalidad específica de los diferentes grupos.

VII

Dicho esto, el Ayuntamiento pregunta si sería correcto (además de acotar al máximo la finalidad del grupo) incluir una cláusula de políticas de buen uso por parte de los usuarios (ciudadanos) del grupo, de compromiso de que no cederán a terceros ni teléfonos del grupo, ni la fotografía del perfil, ni siquiera las imágenes que se puedan compartir en el grupo (la consulta cita como *ejemplo* "que algún padre colgara en el grupo una foto en el que se identificara a los asistentes al evento, adultos y menores").

De entrada, como se ha apuntado, la creación de los grupos de SMI (casos 1, 2 y 3) tiene una finalidad clara y específica, que la propia consulta explica. Por aplicación del principio de finalidad (artículo 4.2 de la LOPD), y teniendo en cuenta que la normativa exige que los datos se traten con licitud, lealtad y transparencia (artículo 5.1.a del RGPD), está claro que los datos serán recogidos con finalidades determinadas, explícitas y legítimas, y que no serán tratados ulteriormente de manera incompatible con estas finalidades (artículo 5.1.b del RGPD).

El Ayuntamiento, como responsable y administrador de los grupos, preverá y explicará de forma adecuada a las personas que serán participantes del grupo cuál es la finalidad de la comunicación del grupo, con el máximo detalle posible y de forma comprensible, como, de hecho, apunta la propia consulta.

Recordamos que el RGPD da carta de naturaleza al principio de transparencia (considerandos 39 y 58 del RGPD). Según dispone el artículo 5.1.a) del RGPD, los datos deben ser tratados de manera lícita, leal y transparente con relación al interesado.

El principio de transparencia, vinculado a los principios de licitud y de lealtad (artículo 5.1.a del RGPD), engloba específicamente el deber del responsable de informar a los afectados sobre una serie de cuestiones, en los términos del artículo 13 del RGPD, al que nos remitimos, y que en algunos aspectos va más allá de lo dispuesto el artículo 5 de la LOPD. Por lo tanto, el Ayuntamiento, como responsable del tratamiento de datos de determinadas personas físicas —a los efectos que interesan, las personas que pueden participar en los diferentes grupos de SMI que cree el Ayuntamiento—, las informará sobre dicho tratamiento, entre otras cuestiones, sobre su finalidad y su base jurídica (artículo 13.1.c del RGPD).

A partir de la fecha de aplicación del RGPD, se informará de los siguientes aspectos (artículo 13 del RGPD): los datos de contacto del delegado de protección de datos; la base jurídica del tratamiento; los intereses legítimos perseguidos en los que se funde el tratamiento; la intención de transferir los datos a un país tercero u organización internacional y la base para hacerlo; el plazo durante el cual se conservarán los datos; la existencia del derecho a pedir la portabilidad; el derecho a retirar en cualquier momento el consentimiento que se haya prestado; si la comunicación de datos es un requisito legal o contractual o un requisito necesario para suscribir un contrato; el derecho a presentar una reclamación ante una autoridad de control; la existencia de decisiones automatizadas, incluyendo la lógica aplicada y sus consecuencias.

Las cláusulas que no tienen en cuenta el grado de comprensión del ciudadano medio, sino que incluso abusan de terminología legal, no serían admisibles, según afirma el GT29, en el documento de Directrices sobre el consentimiento ("Guidelines on Consent under Regulation 2016/679", de 28 de noviembre de 2017): "Al solicitar el consentimiento, los controladores deben garantizar que utilicen un lenguaje claro y sencillo en todos los casos. Esto significa que un mensaje debe ser fácilmente comprensible para la persona promedio y no solo para los abogados. Los controladores no pueden usar largas políticas de privacidad ilegibles o declaraciones llenas de jerga legal".

A los efectos que interesan en este dictamen, el Ayuntamiento tendrá que poner especial énfasis en informar de forma comprensible a los participantes de los grupos, y previamente a la puesta en funcionamiento de estos grupos, por un lado, sobre el hecho de que los participantes en el grupo podrán acceder a los datos de contacto del resto de los participantes y, por otro lado, sobre el hecho de que los participantes podrán acceder a la información que contengan los mensajes (escritos, de voz, archivos adjuntos, fotografías...) que se comuniquen mediante el grupo.

En cuanto al cumplimiento del deber de información en relación con los menores de edad que puedan formar parte del grupo del Consejo de Infancia (caso 3), hacemos notar que, según el artículo 13.3 del RLOPD: "Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquellos, con expresa indicación de lo dispuesto en este artículo". Según el considerando 58 del RGPD "(...). Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender".

Por tanto, en relación con los menores de edad que puedan dar el consentimiento por sí mismos (menores mayores de 14 años, sin perjuicio de las previsiones que pueda contener el Proyecto de ley orgánica de protección de datos, al que nos hemos referido, que se encuentra en sede parlamentaria), la información que se les facilite deberá estar especialmente adaptada a su nivel de comprensión.

VIII

La consulta pregunta sobre la responsabilidad que podría tener el Ayuntamiento respecto a la cesión que puedan hacer los participantes de los grupos a terceros. Hay que decir que la consulta se refiere, en este punto, a los padres o ciudadanos que participan en los grupos.

En cualquier caso, como cuestión previa, conviene distinguir el tratamiento de datos por parte de concejales o trabajadores del propio Ayuntamiento que formen parte de los grupos, del tratamiento que puedan hacer los ciudadanos (padres, alumnos o miembros de asociaciones), que no tienen, en principio, y por la información de que se dispone, ninguna vinculación laboral u orgánica con el consistorio.

Como ha hecho saber esta Autoridad en dictámenes anteriores, hay que tener en cuenta que, si el acceso de los concejales a datos personales se produce por razón de las funciones que como tales tienen encomendadas (como podría ser el caso, por la información disponible, de los concejales a que se refiere la consulta), estos se regirán por el deber de reserva impuesto por la normativa de régimen local (artículo 164.6 del texto refundido de la Ley municipal y de régimen local de Cataluña, aprobado por el Decreto legislativo 2/2003, de 28 de abril [TRLMRLC]), según el cual "los miembros de la corporación tienen que respetar la confidencialidad de la información a que tienen acceso en razón del cargo si el hecho de publicarlo puede perjudicar los intereses del ente local o de terceros".

Aparte de esta previsión específica que afectaría a los concejales, los trabajadores municipales que, según la consulta, podrían formar parte de los grupos están vinculados por el deber de confidencialidad que les impone la normativa como trabajadores públicos (artículo 52 del Estatuto básico del empleado público, aprobado por el Real decreto legislativo 5/2015, de 30 octubre [EBEP]), así como al deber general de secreto que impone el artículo 10 de la LOPD, según el cual: "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".

Además, según dispone el Código penal (artículos 197 y 198), la autoridad o funcionario público que, fuera de los casos permitidos en la ley, y prevaliéndose de su cargo, difunda, revele o ceda a terceros determinados datos estaría realizando una conducta que podría ser constitutiva del delito de descubrimiento y revelación de secretos.

Esto, junto con la exigencia derivada del principio de finalidad, conlleva que los concejales y los trabajadores del Ayuntamiento que, por razón de su cargo, puedan formar parte de los grupos objeto de consulta, en caso de difundir a terceros o tratar la información (ya sean datos de contacto de otros miembros del grupo u otra información personal) sin consentimiento de los afectados y para otras finalidades distintas de la propia del grupo, podrían contravenir la normativa de protección de datos personales. Incluso puede derivarse una responsabilidad disciplinaria en determinados casos (artículo 83 del RGPD y artículo de la 46.2 de la LOPD).

Por lo tanto, el Ayuntamiento sí podría tener responsabilidad sobre un tratamiento inadecuado que, por ejemplo, lleve a cabo un trabajador municipal que forma parte del grupo y que interviene en este por razón de su cargo.

En cuanto a los padres de niños que acuden a la ludoteca, a los miembros de asociaciones del pueblo o a los menores de edad de las escuelas, aunque la creación de los grupos 1, 2 y 3 sea a iniciativa del Ayuntamiento, difícilmente este tendría responsabilidad directa (a los efectos del artículo 46 de la LOPD) sobre el uso posterior que personas ajenas al Ayuntamiento hagan de datos personales (comentarios, números de contacto, fotos...) a los que habrán accedido legítimamente, en los términos apuntados.

Dicho esto, hay que tener en cuenta que, en principio, cualquier persona que accede a datos personales de otros para una finalidad legítima debería tratar los datos personales a los que haya podido acceder conforme a los principios y garantías de la normativa de protección de datos, citados.

Así, en principio, los ciudadanos que participan en los grupos deberían tratar los datos personales a los que tengan acceso en el marco de la finalidad propia del grupo. Los miembros del grupo deberían disponer del consentimiento u otra habilitación legal para comunicar a personas ajenas al grupo la información personal que se trata en este. El deber general de secreto (artículo 5.1.f del RGPD y artículo 10 de la LOPD) también resultaría de aplicación en este caso. A modo de ejemplo, para comunicar el número de teléfono de otro miembro del grupo a una tercera persona ajena a este, se necesitaría el consentimiento de aquel.

En el caso concreto de la imagen de las personas, que es un dato personal (artículo 5.1.f del RLOPD), como ha hecho saber esta Autoridad en ocasiones anteriores (dictámenes CNS 9/2016 o CNS 64/2015, entre otros), la captación y difusión de la imagen gráfica de personas identificadas o identificables afecta al derecho a la propia imagen (artículo 18.1 de la CE) y, por tanto, hay que tener en cuenta la Ley orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (LO 1/1982). Las previsiones de la LO 1/1982 (artículos 7.5 y 8.2) podrían habilitar la captación y difusión de imágenes de personas identificables (por ejemplo, mediante fotografías) en un acto público y en el cual la imagen de estas personas aparezca como meramente accesoria. De ser así, no sería estrictamente necesario, desde el punto de vista de la normativa estudiada, disponer del consentimiento previo de los afectados para que los miembros de los grupos pudieran ceder a terceros imágenes de este tipo. En cambio, en otros tipos de imágenes en los que no se den estos elementos habría que disponer del consentimiento de los afectados.

En cualquier caso, y sin perjuicio de esta puntualización, no resultaría contrario a la normativa de protección de datos, y hasta podría ser recomendable, que el Ayuntamiento establezca, como política de buen uso, que los miembros de los grupos no compartan imágenes con terceros ajenos al grupo, salvo que dispongan de los consentimientos que puedan ser necesarios, dada la normativa citada.

Dejando de lado las fotografías, y en referencia a otros tipos de informaciones que puedan compartirse en los grupos, es conveniente que el Ayuntamiento advierta a los participantes de los grupos que compartir con terceros información especialmente protegida (como podrían ser datos de salud, posibilidad que apunta la consulta) podría contravenir las previsiones de la normativa de protección de datos personales. En este punto, a efectos ilustrativos, y por su relevancia, nos remitimos a la Sentencia B.

Lindqvist, del Tribunal de Justicia de la UE, de 6 de noviembre de 2003. Esto, sin perjuicio de que, por la información de que se dispone, no parece que la finalidad de los grupos 1, 2 y 3 haga probable el tratamiento de información especialmente protegida.

Por todo lo expuesto, dada la problemática que plantea la consulta (posible difusión de fotografías, comentarios, etc., por parte de los participantes), hay que valorar positivamente que el Ayuntamiento elabore una "cláusula de políticas de buen uso" (un código de buenas prácticas, en definitiva), para que todos los participantes de los grupos (independientemente de su vinculación o no con el Ayuntamiento) traten los datos personales objeto de consulta de forma ajustada a las previsiones de la normativa citada.

Finalmente, en cuanto a la posibilidad de expulsar a algún miembro del grupo, a que se refiere la consulta, desde la perspectiva de la protección de datos no corresponde a esta Autoridad determinar en qué casos el Ayuntamiento tomará la decisión de expulsar a un miembro de alguno de los grupos 1, 2 y 3.

Ahora bien, el mero hecho de haber expulsado a un miembro del grupo de SMI no desvirtúa la obligación del Ayuntamiento de dar cumplimiento de los principios y obligaciones, en materia de protección de datos, que le puedan corresponder como responsable, ni tampoco las consecuencias que un tratamiento inadecuado de los datos personales pueda conllevar.

IX

El caso 4 hace referencia a un grupo de WhatsApp que, según la información de que se dispone, no crearía el Ayuntamiento, sino "los jóvenes del pueblo", aunque, según la consulta, se habría añadido a este grupo un trabajador municipal, que utiliza un número de teléfono del propio Ayuntamiento. El Ayuntamiento pregunta si, al no ser administrador del grupo, el Ayuntamiento tendría alguna responsabilidad como administración pública y si debería realizar alguna gestión con relación a la LOPD.

Dada la información disponible, hay que recordar que se desconoce la finalidad del grupo en cuestión, es decir, si este podría tener alguna relación, directa o indirecta, con alguna actividad o servicio que presta u organiza el Ayuntamiento. Se desconoce si en el marco de este grupo se podría tratar determinada información personal de la que sea responsable el Ayuntamiento. También se desconoce si el trabajador municipal que, según la consulta, se ha añadido al grupo forma parte de este en su condición de trabajador del Ayuntamiento y por razón de su trabajo o bien a título particular.

En relación con esta cuestión, el RGPD dispone que este reglamento no se aplica al tratamiento de datos personales efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas (considerando 18 y artículo 2.2.c del RGPD). Se mantiene así la exclusión que ya contenía la LOPD respecto a los tratamientos mantenidos por personas físicas en ejercicio de actividades exclusivamente personales o domésticas (artículo 2.2.a de la LOPD), entendiendo como tales las que se inscriben en el marco de la vida privada o familiar de los particulares (artículo 4.a del RLOPD) o, como precisó la Audiencia Nacional en Sentencia de 15 de junio de 2006: "(...) Será personal cuando los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos".

Por tanto, dada la información de que se dispone, esta Autoridad no puede determinar si el grupo referido (caso 4) tiene una finalidad exclusivamente personal o doméstica y, en consecuencia, si el tratamiento de datos que se pueda hacer en él se encuentra o no sujeto a la normativa de protección de datos personales.

Por otra parte, por la información aportada, parece claro que no se trataría de un tratamiento responsabilidad del Ayuntamiento, con independencia de que un determinado trabajador de la corporación se haya añadido al grupo a título particular.

En cualquier caso, el trabajador, dada su vinculación laboral con el Ayuntamiento, tiene la obligación de tratar la información personal de que pueda ser conocedor por razón de su cargo con pleno respeto de los principios y garantías de la normativa de protección de datos, dada la normativa citada.

De acuerdo con las consideraciones hechas en este dictamen, se hacen las siguientes

Conclusiones

A la hora de establecer la utilización de un determinado canal de comunicación en los servicios municipales, el Ayuntamiento tendrá en cuenta las garantías que ofrece el canal para el tratamiento de la información de las personas afectadas y la existencia o no de otros canales alternativos.

Casos 1, 2 y 3: El Ayuntamiento dará cumplimiento a los principios y garantías de la normativa de protección de datos, entre otros, dispondrá del consentimiento de todos los participantes de los grupos, salvo que cuente con otra base jurídica y les dará información sobre el tratamiento de los datos (artículo 13 del RGPD) y las consecuencias que se pueden derivar de la utilización de este canal.

Aunque la creación de los grupos sea a iniciativa del Ayuntamiento, difícilmente este tendría responsabilidad directa (a los efectos del artículo 46 de la LOPD) sobre el uso posterior que personas ajenas al Ayuntamiento hagan de datos personales. Sin perjuicio de ello, se valora positivamente la elaboración de una "cláusula de políticas de buen uso", para que todos los participantes de los grupos traten los datos personales de forma ajustada a las previsiones de la normativa.

Caso 4: Dada la información disponible, no puede determinarse si el grupo tiene una finalidad exclusivamente personal o doméstica y, en consecuencia, si se encuentra o no sujeto a la normativa de protección de datos personales. En cualquier caso, por la información facilitada, no sería responsabilidad del Ayuntamiento.

Barcelona, 26 de abril de 2018