InDret

2.2020

Comentario a las «Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications».

Idoia Elizalde Salazar
Universitat Pompeu Fabra
idoia.elizalde@upf.edu

Cada vez es más habitual que proporcionemos datos personales a terceros. Sin embargo, y a pesar de lo cotidiano de la comunicación, no siempre somos conscientes de estar dando a terceros datos sobre nuestra actividad que, al final, permiten identificarnos e identificar nuestras preferencias. Desconocemos qué datos estamos facilitando, a quién, con qué finalidad pueden estos utilizarlos, durante cuánto tiempo y si pueden estos traspasarlos a terceros, entre otras muchas cuestiones relevantes.

Es perentoria, por tanto, la necesidad de mejorar las normas legales que tienen por objeto la protección de los datos de las personas. En el año 2015, el legislador europeo aprobó el Reglamento 2016/679[1] 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 y por el que se deroga la Directiva 95/46/CE , conocido como "Reglamento general de protección de datos" o GDPR por las siglas de su título en inglés (General Data Protection Regulation). Reglamento que derogó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos vigente hasta el momento.

La generación y cesión de datos personales es más intensa cuanto mayor sea el grado de tecnología que involucra una actividad. A la vez, cuando eso sucede, más probable es que el usuario carezca de control sobre los datos que proporciona o que no pueda evitar su cesión a terceros. Todo ello sucede, con una intensidad especial, en el vehículo conectado.

Un grupo de expertos en materia de protección de datos publicó el pasado mes de enero una guía sobre el tratamiento de los datos personales obtenidos por las aplicaciones de las que disponen los vehículos conectados y de los datos que el propio vehículo conectado puede generar. La "*Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications*"[2] (en adelante, "la guía") fue adoptada el pasado 28 de enero por el *European Data Protection Board*. Y desde el 7 de febrero hasta el 4 de mayo se ha abierto un plazo de

[1] DO L 119/1, de 4 de mayo de 2016.

Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES.

[2] European Data Protection Board, "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", 2020. Disponible en https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf.

audiencia[3]. Durante este período han sido numerosas organizaciones las que han presentado comentarios a la guía[4] y en este trabajo doy razón a aquellas observaciones más relevantes que se han hecho a la propuesta de documento.

1. GDPR y Directiva e-Privacy

El GDPR es aplicable para cualquier dato personal procesado por el uso de un vehículo conectado (párrafo 9 de la guía). Es importante no confundir el GDPR con la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, conocida como "ePrivacy Directive", que regula el tratamiento de los datos personales en el sector de las comunicaciones electrónicas. Según la guía la Directiva ePrivacy también es aplicable a los vehículos conectados y los dispositivos conectados a estos, por tener ambos la consideración de "equipo terminal" (párrafo 13). El art.5.3. de la Directiva ePrivacy exige el consentimiento del individuo cuando se pretende almacenar o acceder a información almacenada en el equipo terminal de dicho individuo, salvo que dicho almacenamiento o acceso se realice con el único fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas o para la prestación de un servicio expresamente solicitado por el individuo. Para el resto de tratamiento de datos, el GDPR es aplicable.

No obstante, algunas entidades solicitan que se aclare la compatibilidad de la aplicación de estas dos normas. En especial sobre el tratamiento posterior de los datos obtenidos. La guía prevé que cuando los datos se recopilan sobre la base del consentimiento como lo requiere el art. 5.3 de la Directiva ePrivacy, solo puede procesarse si el controlador busca un consentimiento adicional para este otro propósito o si el controlador de datos puede demostrar que se basa en una ley de la Unión o del Estado miembro para salvaguardar los objetivos mencionados en el art. 23.1 GDPR. La guía considera que el procesamiento adicional, de acuerdo con el art. 6.4 GDPR, no es posible en estos casos ya que socavaría el estándar de protección de datos de la Directiva ePrivacy (párrafo 50). La GERMAN INSURANCE ASSOCIATION, sin embargo, ha considerado que este planteamiento es incorrecto y que no es evidente hasta qué punto se socavaría el nivel de protección de la directiva de ePrivacy[5].

2. Ámbito de aplicación

La guía tiene por objeto aplicarse a aquellos datos personales obtenidos por vehículos conectados siempre que no sean para el uso profesional. Concretamente, a los datos procesados dentro del vehículo, los intercambiados entre el vehículo y dispositivos personales conectados al mismo como los teléfonos móviles y los recogidos dentro del vehículo y exportados a entidades externas

---

[3] Pueden realizarse comentarios mediante el formulario disponible en https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.

[4] *Ídem*. En la misma página web pueden consultarse los comentarios y valoraciones realizados por distintas entidades.

[5] GERMAN INSURANCE ASSOCIATION (DIE DEUTSCHEN VERSICHERER, GDV), "Comment of the German Insurance Association (GDV) on the EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", 2020. Tambien, sobre la confusion de los párrafos 13-14, EUROPEAN AUTOMOTIVE AND TELECOMS ALLIANCE, "EATA response to EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", 2020, pp. 1-3, p. 2.

como pueden ser los fabricantes de los mismos, las compañías aseguradoras o los servicios de reparación y mantenimiento (párrafo 19).

La guía define "vehículo conectado" de una manera amplía: vehículo equipado con unidades de control electrónico unidas entre sí mediante una red dentro del vehículo, así como instalaciones de conectividad que le permiten compartir información con otros dispositivos tanto dentro como fuera del vehículo (párrafo 20). Ejemplifica como aplicaciones de vehículos conectadas las aplicaciones de gestión de movilidad (párrafo 21), gestión del vehículo (párrafo 22), de seguridad vial (párrafo 23), de entretenimiento (párrafo 24), de asistencia al conductor (párrafo 25) o las aplicaciones para mejorar el bienestar del conductor (párrafo 26).

La guía remarca que solamente las aplicaciones de los móviles de los usuarios de los vehículos que aporten datos relacionados con la conducción están dentro de su ámbito de aplicación. Incluye, por tanto, el sistema de navegación GPS y excluye a las aplicaciones que sugieren sitios de interés como restaurantes, monumentos históricos, etc. (párrafo 27). Este punto no ha quedado exento de críticas. HERE TECHNOLOGIES, que desarrolla el servicio de mapas y geolocalización, considera que esta distinción podría provocar la incorrecta aplicación de las recomendaciones de la guía puesto que, muchas aplicaciones móviles recopilan datos de ubicación para sugerir puntos de interés y al mismo tiempo estas aplicaciones ofrecen la funcionalidad de navegación GPS para llegar allí. Consideran que únicamente las aplicaciones que den apoyo al funcionamiento del vehículo mediante datos aportados o recibidos por el vehículo conectado deberían estar dentro del ámbito de aplicación de la guía. Y, por ello, los servicios independientes de navegación GPS que usan los datos de un dispositivo móvil independiente al vehículo (posición GPS del móvil) deberían quedar fuera del ámbito de aplicación de la guía[6].

La guía añade que gran parte de los datos generados por un vehículo conectado hacen referencia a una persona física identificada o identificable y, por lo tanto, constituyen datos personales (párrafo 28). Diferencia entre los datos que incluyen datos directamente identificables de los datos identificables indirectamente como los detalles de los viajes realizados, los datos de uso del vehículo o los datos técnicos del vehículo que, al hacer referencia cruzada con otros datos y especialmente con la matrícula del vehículo, pueden relacionarse con una persona física. Este párrafo 28, ha sido uno de los más criticados de la guía en relación al trato que debería darse a la matrícula del vehículo. Son varias las organizaciones que han considerado que la matrícula, por si misma, no identifica y no que no tiene por qué conducir a la identificación del individuo. BELRON, una compañía de reparación y mantenimiento de vehículos para la cual la matrícula de los vehículos es de gran utilidad, expresa que la matrícula les permite obtener piezas para los vehículos y para realizar verificaciones de calidad[7]. Y que al no conducir a la identificación del individuo no debería de tratarse la matrícula como dato personal en todos los casos. En la misma línea, WEJO LDT., una empresa especializada en la conectividad de vehículos insiste en que existen herramientas, como "squish", para impedir identificar al usuario final de un vehículo mediante la matrícula. Consiste en facilitar únicamente parte de la matrícula e impedir, de esta

[6] HERE TECHNOLOGIES, "Comments on EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", 2020, pp 1-6, p.6.

[7] BELRON, "Submission to the EDBP guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", 2020, pp. 1-4, p.1-2.

manera, que el vehículo o el conductor sean identificados[8]. O HERE TECHNOLOGIES plantea la posibilidad de anonimizar o pseudoanonimizar datos como la matrícula del vehículo[9].

La guía afirma también que cualquier información que pueda asociarse con una persona física entra en el alcance de este documento (párrafo 28). Afirmación que también ha sido criticada porque existen datos asociados a una persona física que pueden incluir datos que no son expresa o indirectamente a cerca de ellos. Es por ello por lo que RSA INSURANCE GROUP recomienda en sus comentarios a la guía que la definición de datos personales tenga el alcance restringido establecido en el art. 4 GDPR[10]. Todas estas organizaciones comparten la idea de que no todos los datos generados en o por un vehículo conectado, aunque sí la mayoría, son datos personales y agradecen que la guía así lo haya considerado. La FÉDÉRATION INTERNATIONALE DE L'AUTOMOBILE y las organizaciones que forman parte de ella van incluso un poco más lejos. No es que la mayoría de los datos son personales, sino que todos lo son a excepción de que sean anonimizados, en cuyo caso la regulación europea sobre protección de datos ya no es aplicable ("not most, but all data in connected vehicles qualify as personal data unless anonymized")[11].

Finalmente, añadir que la FEDERATION OF EUROPEAN MOTORCYCLISTS' ASSOCIATIONS ha considerado que el ámbito de aplicación no es suficiente claro en relación a los vehículos de dos ruedas, entre otros[12]. Exponen que en ocasiones la guía utiliza el término "vehículo conectado" y en otras "coche conectado". Solicitan que en el próximo borrador se aclare si solamente los vehículos de categoría M1 están dentro del ámbito de aplicación de la guía o también los vehículos del resto de categorías como L, N1, M2, N2. Remarcan que ya existen motocicletas conectadas. Sugieren que se incluya explícitamente en el ámbito de aplicación de la guía a las motocicletas y al resto de vehículos de categoría L.

2.1. Exclusiones

La guía ha excluido del ámbito de aplicación los datos que se obtienen por el uso de vehículos conectados por los empleados de una empresa que los pone a disposición de sus trabajadores para el desarrollo de la actividad empresarial (párrafo 31). Datos que permiten al empleador supervisar la actividad de sus empleados como la verificación del tiempo de trabajo. El procesamiento de estos datos tendría que resolverse mediante leyes nacionales de carácter laboral.

---

[8] WEJO LTD., "Submissions to the European Data Protection Board in connection with Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", 2020, pp.1-4, p. 2.

[9] HERE TECHNOLOGIES, *ob cit.,* p. 2.

[10] RSA INSURANCE GROUP, "EDPB Draft Guidelines on the Processing of Personal Data in the Context of Connected Vehicles", 2020, pp. 1-5, p.3.

[11] FÉDÉRATION INTERNATIONALE DE L'AUTOMOBILE, "European Data Protection Board consultation on the Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications, 2020, pp.1-3, p. 1; GENERAL GERMAN AUTOMOBILE CLUB (ALLGEMEINER DEUTSCHER AUTOMOBIL-CLUB E.V.; ADAC) , p.1; FEDERATION OF DANISH MOTORISTS (FORENEDE DANSKE MOTOREJERE; FDM), P.1; AUSTRIAN AUTOMOBILE, MOTORCYCLE, AND TOURING CLUB (ÖSTERREICHISCHER AUTOMOBIL-, MOTORRAD- UND TOURINGSCLUB; ÖAMTC) , p. 1.

[12] FEDERATION OF EUROPEAN MOTORCYCLISTS' ASSOCIATIONS, "View of FEMA on the EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", 2020, p.1.

La guía ha excluido también vehículos sujetos a sistemas que incorporan información digital por trasmisiones de radio FM convencionales (*radio-enabled system*) mediante Wifi o Bluetooth. Excluye, a gran escala, también, el tratamiento de los datos obtenidos mediante una extensa red Wifi a la que muchos transeúntes hacen uso de servicios de localización (párrafo 32). Comparto con la SWEDISH TRANSPORT AGENCY que el contenido de este párrafo no es sencillo de entender y que debería ser reescrito[13]. De hecho, la SWEDISH TRANSPORT AGENCY considera que todo este apartado ("*Out of scope of this document*"), y no solamente el párrafo 32, es confuso y que debería volver a redactarse[14]. Otras organizaciones, como la EUROPEAN AUTOMOTIVE AND TELECOMS ALLIANCE, también han considerado que sería preciso aclarar algunos aspectos de este apartado[15].

La guía excluye también aquellos sistemas que recopilan datos mediante imágenes como los sistemas de cámara para aparcar o las cámaras interiores del vehículo que graban continuamente el exterior del vehículo mientras este circula (conocidas como *dashcam*). La exclusión se justifica en que estas filmaciones se producen en lugares públicos y que la regulación sobre protección de datos obtenidos en espacios públicos compete a cada estado miembro (párrafo 33).

Finalmente, excluye los datos obtenidos por sistemas cooperativos de transporte inteligentes (conocidos como C-ITS por sus siglas en inglés *Cooperative Intelligent Transport Systems*) (párrafo 34). Sin embargo, la SWEDISH TRANSPORT AGENCY apunta que otros párrafos de la guía sí son aplicables a los C-ITS. Insiste, por ello, que el apartado de exclusiones de la guía debería ser revisado[16].

3. Definiciones

La guía define los conceptos de tratamiento de datos (párrafo 36), persona interesada (párrafo 37), controlador de datos (párrafo 38), procesador de datos (párrafo 39) y receptor (párrafo 40) y hace especial mención a las autoridades públicas que actúan como receptoras (párrafo 41).

De estas, la más criticada ha sido la que define al interesado. En su tenor literal:

> "The data subject is the natural person to whom the data covered by the processing relate. In the context of connected vehicles, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle".

La FEDERACIÓN AUTOMOVILÍSTICA DANESA propone añadir como persona interesada al usuario del vehículo[17]. Sin embargo, otras organizaciones han considerado que la definición de persona es demasiado amplia. RSA INSURANCE GROUP sugiere eliminar al pasajero de la definición por considerar difícil obtener el consentimiento de este[18]. O WEIJO LTD. sugiere, incluso, eliminar de la definición al propietario del vehículo, por considerar que en la mayoría de los casos los datos personales que se generarán por el uso del vehículo conectado serán referentes al conductor o al

[13] SWEDISH TRANSPORT AGENCY, "Comments on Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", 2020, p.1.

[14] *Ídem*.

[15] European Automotive and Telecoms Alliance, *ob cit.*, p. 2.

[16] Swedish Transport Agency, *op.cit,* p.1.

[17] Federation of Danish Motorists, *op cit.,* p. 1.

[18] RSA INSURANCE GROUP, *op. cit.,* p. 4.

pasajero y que el propietario, en la mayoría de los supuestos, coincidirá con uno de estos[19]. WEIJO LDT. añade que para los casos en los que el propietario no sea conductor o pasajero, como sucede con las compañías de flotas, no supondría problema porque estas tienen mejor cabida bajo la definición de controlador de datos.

Otras han sugerido que la guía debería remarcar más la diferencia entre controlador y procesador de datos[20].

4. Principales riesgos como resultado de la conectividad de los vehículos

La guía identifica principalmente cinco tipos de riesgos derivados de:

1. La falta de control y la información asimétrica entre los distintos sujetos afectados
2. La calidad del consentimiento de los usuarios
3. El uso de los datos para tratamientos ulteriores
4. La recogida de datos en exceso
5. La seguridad de los datos

4.1. Información asimétrica

Los conductores y pasajeros del vehículo no siempre están bien informados sobre el tratamiento de los datos proporcionados en o mediante el vehículo conectado. Es destacable que según la guía la información se puede proporcionar solo al propietario del vehículo, que puede no ser el conductor. Existe, por lo tanto, el riesgo de que no se ofrezcan opciones suficientes para que todas las personas afectadas puedan ejercer sus derechos de protección de datos y privacidad. Téngase en cuenta que los vehículos conectados pueden permanecer a distintos propietarios a lo largo de su vida útil (párrafo 44).

Añade que la comunicación en el vehículo se puede activar automáticamente, por defecto, sin que el individuo lo sepa. Y que en ausencia de poder controlar eficazmente cómo interactúan el vehículo y su equipo conectado es muy difícil que el usuario controle el flujo de datos (párrafo 45).

INSURANCE EUROPE, de acuerdo con que estos riesgos existen en los casos de dispositivos integrados en el vehículo, sugiere que en el próximo borrador se especifique que, por el contrario, no existe asimetría de información o falta de control sobre los datos cuando se haya contratado un seguro basado en el uso (*built-in systems vs. usage-based insurance*). En estos casos, el cliente instala un dongle en el automóvil o en su dispositivo móvil y consecuentemente, el cliente sabe si su asegurador está recopilando datos o no. Además, si el vehículo se vendiera no se crearía una situación de falta de control, ya que la póliza de seguro del propietario anterior se rescinde automáticamente[21].

---

[19] WEJO LTD., *op cit.,* p. 2.

[20] HERE TECHNOLOGIES, *op.cit.,* p.5.

[21] INSURANCE EUROPE, "Response to EDPB draft guidelines on processing personal data in the context of connected vehicles and mobility related Applications", 2020, pp.1-7, p. 1.

4.2. Consentimiento como base legal

Según la guía el consentimiento (párrafo 46-49):

- Tiene que ser libre, específico e informado
- Los controladores de datos deben prestar especial atención a las modalidades para obtener el consentimiento válido de diferentes participantes, como los propietarios o usuarios de automóviles.
  Los mecanismos clásicos utilizados para obtener el consentimiento de las personas pueden ser difíciles de aplicar en el contexto de los vehículos conectados, lo que resulta en un consentimiento de "baja calidad" basado en la falta de información o en la imposibilidad fáctica de proporcionar un consentimiento ajustado de acuerdo con las preferencias expresadas por los individuos. En la práctica, el consentimiento también puede ser difícil de obtener para los conductores y pasajeros que no están relacionados con el propietario del vehículo en el caso de vehículos de segunda mano, arrendados, alquilados o prestados.
- Debe proporcionarse por separado, para fines específicos. No puede incluirse en el contrato para comprar o arrendar un auto nuevo.
- El consentimiento debe retirarse tan fácilmente como se da.

Algunas entidades como la GERMAN INSURANCE ASSOCIATION o TELEFÓNICA S.A. consideran que la guía centra demasiada atención al consentimiento como base legal y que quizás debería centrar más atención a otros fundamentos legales como el contrato o el legítimo interés[22].

También la GERMAN INSURANCE ASSOCIATION y otras como la EUROPEAN AUTOMOTIVE AND TELECOMS ALLIANCE consideran que obtener el consentimiento de cada uno de los participantes del uso del vehículo no seria práctico. Así como que el principio de poder retirar el consentimiento tan fácil como se da podría ser de difícil o imposible implementación en el vehículo conectado en muchos casos[23].

4.3. Tratamientos ulteriores

La guía recuerda que el consentimiento inicial nunca legitimará un procesamiento posterior ya que el consentimiento debe ser informado y específico para ser válido (párrafo 51).

4.4. Datos en exceso

Cada vez se implementan más en los vehículos conectados y consecuentemente existe un riesgo muy alto de recopilación de datos excesiva en comparación con lo que es necesario para lograr el propósito (párrafo 54).

El desarrollo de nuevas funcionalidades y más específicamente las basadas en algoritmos de aprendizaje automático pueden requerir una gran cantidad de datos recopilados durante un largo período de tiempo (párrafo 55).

---

[22] GERMAN INSURANCE ASSOCIATION, *ob cit.,* p. 6; TELEFÓNICA S.A., "Comments on EDPB Guidelines 1/2020 on processing personal data in the context of connected vehicles", 2020, pp. 1-5, pp. 1-2.

[23] German Insurance Association, *ob cit.,* p.6 ; European Automotive and Telecoms Alliance, *ob cit.,* p.2.

4.5. Seguridad de los datos

La pluralidad de funcionalidades, servicios e interfaces que ofrecen los vehículos conectados aumenta la superficie de ataque y, por lo tanto, la cantidad de vulnerabilidades potenciales a través de las cuales los datos personales podrían verse comprometidos. A diferencia de la mayoría de los dispositivos con internet de las cosas (IoT), los vehículos conectados son sistemas críticos donde una violación de seguridad puede poner en peligro la vida de sus usuarios y la gente de alrededor. Por ello, la importancia de abordar el riesgo de que los "piratas informáticos" intenten explotar las vulnerabilidades de los vehículos conectados (párrafo 56).

Además, los datos personales almacenados en vehículos y / o en ubicaciones externas pueden no estar adecuadamente protegidos contra el acceso no autorizado. La guía pone como ejemplo, la posibilidad de que un técnico que requiere de acceso a algunos datos durante el mantenimiento de vehículo pueda intentar acceder a todos los datos almacenados en el vehículo (párrafo 57). Este ejemplo preocupa a BELRON[24], una empresa de reparaciones, por considerar que este riesgo también existe en el mundo analógico y no solo en el conectado.

5. Tipos de datos

La guía ha identificado tres categorías de datos personales que requieren atención especial:

1. Datos de ubicación
2. Datos biométricos
3. Datos que pueden revelar delitos o infracciones de tráfico.

5.1. Datos de ubicación (localización, geolocalización)

Al recopilar datos personales, los fabricantes de vehículos y equipos, los proveedores de servicios y otros controladores de datos deben tener en cuenta que los datos de geolocalización revelan particularmente los hábitos de vida de los interesados (lugar de trabajo y residencia, centros de interés del conductor, la religión a través del lugar de culto, o orientación sexual a través de los lugares visitados…). En consecuencia, estos deben estar particularmente atentos para no recopilar datos de ubicación, excepto si es absolutamente necesario para el procesamiento. Pone como ejemplo que estos prescindan de recopilar datos de ubicación cuando su objetivo sea detectar el movimiento del vehículo, puesto que mediante un giroscopio ya pueden cumplir esa función (párrafo 60).

Este apartado de la guía (*2.1.1. Geolocation data*) ha sido uno de los más criticados, o sugeridos a reformular, en los comentarios que las distintas organizaciones han presentado durante el período de consultas públicas.

WEJO LTD. sugiere que se introduzca en la Sección Segunda de la guía, sobre definiciones, una para "Geolocation data"[25]. Añade que sería preciso también que en la guía se explicara cual es la diferencia entre el término "geolocation data" y "location data" que incorrectamente se usa

[24] BELRON, *op. cit.*, p.2.

[25] WEJO LTD., *op. cit.*, p. 3.

indistintamente en la guía. Sugiere que la guía utilice el término "location data" en las líneas definidas en Privacy and Electronic Communications Regulations. Añade, incluso, que la guía debería especificar que los datos de ubicación no son *per ser* datos personales.

Por otra parte, el asesor de protección de datos de HUAWEI BELGIUM, el Sr. ZHANG MIAO FRANK, y en la misma línea HERE TECHNOLOGIES, sugieren que la excepción "cuando sea absolutamente necesario" es demasiado amplia y que debería aclararse o detallarse[26].

En general, la recopilación de datos de geolocalización también está sujeta al cumplimiento de los siguientes principios (párrafo 61):

- Configurar adecuadamente la frecuencia de acceso y nivel de detalle de los datos de geolocalización
- Facilitar información detallada sobre la finalidad del tratamiento
- Cuando el procesamiento se basa en el consentimiento, obtener un consentimiento válido y separo de las condiciones generales de uso del vehículo
- Activar la geolocalización únicamente cuando se use la aplicación que la requiere y no por defecto y de forma continua al arrancar el vehículo
- Informar al usuario de que la geolocalización esta activada mediante iconos
- Ofrecer una opción sencilla para desactivar la geolocalización en cualquier momento
- Definir un periodo de conservación limitado

Principios que tampoco han quedado exentos de sugerencias de mejora en los comentarios presentados.

INSURANCE EUROPE, RSA INSURANCE GROUP y la GERMAN INSURANCE ASSOCIATION hacen hincapié en que la guía debería tener en cuenta el funcionamiento de los seguros telemáticos[27]. Para estos, no siempre es necesario procesar datos de geolocalización, pero se recopilarán y usarán en el caso de una consulta relacionada con un accidente o robo, por ejemplo. Añaden que la posibilidad de desconectar en cualquier momento los datos de ubicación dejan sin sentido este tipo de seguros que precisamente se basan en los datos recopilados. Remarcan que este tipo de seguros son elegidos por los propios clientes y que la capacidad de desactivar los datos podría entenderse como un incumplimiento del contrato celebrado con su asegurador. Sugieren una revisión de estos principios para que puedan ser compatibles con este tipo de seguros.

HERE TECHNOLOGIES considera que pretender que únicamente se active solo cuando el usuario inicie una funcionalidad que requiera que se conozca la ubicación del vehículo, y no de manera predeterminada cuando se enciende el automóvil, es inviable en la práctica para determinados servicios como el servicio de advertencias de peligro en la carretera. Considera que estos requisitos demasiado engorrosos harían poco atractivos estos servicios para los clientes, disminuiría sus beneficios e impactaría negativamente en el desarrollo de servicios basados en datos. Expone que la mayoría de los servicios que ellos ofrecen están orientados a brindar servicios en un contexto de ubicación sin identificando al usuario final. Cuando los datos

[26] FRANK, ZhangMiao. DPO Office in Belgium Huawei, p.1; HERE TECHNOLOGIES, *op.cit.*, p.4.

[27] INSURANCE EUROPE, *op.cit.,* p. 3-4; RSA INSURANCE GROUP, *op.cit.*, p.3; GERMAN INSURANCE ASSOCIATION, *op.cit.,* p. 8-9.

personales pueden estar involucrados aplican técnicas de pseudonimización[28] para reducir la identificabilidad directa de los datos relacionados con los individuos. Insiste en que los principios que rigen los datos de geolocalización no deben ser demasiado estrictos si se quiere garantizar la continuidad de determinados servicios al conductor[29].

5.2. Datos biométricos

En el contexto de los vehículos conectados, los datos biométricos se pueden utilizar, entre otras cosas, para permitir el acceso a un vehículo, para autenticar al conductor / propietario y / o para permitir el acceso a las configuraciones y preferencias del perfil del conductor. Para el uso de este tipo de datos es necesario prever una alterativa no biométrica (como una llave física o un código) sin restricciones adicionales (el uso de la biometría no debería ser obligatorio).

En el caso de los datos biométricos, es importante asegurarse de que la solución de autenticación biométrica sea lo suficientemente confiable, en particular cumpliendo con los siguientes principios (párrafo 63):

- Adecuar e implementar medidas de seguridad necesarias en base a las características de la aplicación o sensor
- Asegurarse de que la aplicación o sensor utilizado es resistente a ataques de terceros
- Limitar el número de intentos de autenticación
- Almacenar en el vehículo de forma encriptada la plantilla biométrica
- Solamente utilizar en tiempo real, sin ni siquiera almacenar, la información que compone la plantilla biométrica y la autenticación del usuario

5.3. Datos que pueden revelar delitos o infracciones de tráfico

Los datos personales de los vehículos conectados pueden revelar la comisión de un delito u otra infracción. Por ello la guía los sujeta a restricciones especiales. Por ejemplo, la velocidad instantánea de un vehículo combinada con datos precisos de geolocalización podría considerarse información relacionada con el delito. Como resultado, el procesamiento de dichos datos solo puede llevarse a cabo bajo el control de la autoridad oficial o cuando el procesamiento esté autorizado por la legislación de la Unión o del Estado miembro que establezca las garantías adecuadas para los derechos y libertades de los interesados, como se establece en el art. 10 GDPR. La guía considera que la velocidad no es *per se* información relacionada con el delito, ya que no revela por sí sola un delito dado que las restricciones de velocidad varían según la ubicación (párrafo 64).

La recopilación de este tipo de datos de está sujeta al cumplimiento de los siguientes principios (párrafo 65):

- Procesamiento local
- Por regla general, el procesamiento externo de datos que revelan delitos penales u otras infracciones está prohibido.

[28] Sobre la diferencia entre la anonimización y la pseudonimización, véase el apartado "6.3.2. Anonimización y pseudonimización" del presente comentario.

[29] HERE TECHNOLOGIES, *op.cit*, p.4-5.

- Establecer medidas de seguridad estricta para ofrecer protección al interesado.

La RSA INSURANCE GROUP expone, sin embargo, que los vehículos conectados y los dispositivos telemático recopilan datos sobre la velocidad conducida y la contrastan con el límite de velocidad de la carretera[30]. Es una función fundamental para los seguros telemáticos en los que el asegurador tiene en cuenta la conducta del conductor. Y considera que si la guía se publica como está redactada actualmente, podría erosionar la capacidad de las aseguradoras para proporcionar estos tipos de seguros. Sugiere que se amplíe en este sentido la recomendación de la guía para permitir a las aseguradoras procesar este tipo de datos y que puedan cumplir con los propósitos de una póliza de seguro conectada y telemática.

6. Principios generales de protección de datos

6.1. Limitación de la finalidad

Los datos personales pueden procesarse para una amplia variedad de propósitos en relación con los vehículos conectados, incluida la seguridad del conductor, los seguros, el transporte eficiente, el entretenimiento o los servicios de información (párrafo 66).

De acuerdo con el GDPR, los controladores de datos deben asegurarse de que sus propósitos sean "especificados, explícitos y legítimos", que no se procesen de manera incompatible con esos propósitos y que exista una base legal válida para su procesamiento (párrafo 66).

La venta de un vehículo conectado y el consiguiente cambio de propiedad también deberían provocar la eliminación de cualquier dato personal, que ya no es necesario para los fines especificados (párrafo 89).

6.2. Principio de minimización

Para cumplir con los principios de minimización de datos, los fabricantes de vehículos y equipos, los proveedores de servicios y otros controladores de datos deben prestar especial atención a las categorías de datos que necesitan de un vehículo conectado, ya que solo recopilarán datos personales que sean relevantes y necesarios para el procesamiento (párrafo 67).

WEJO LDT., aunque de acuerdo con que se debe prestar especial atención a la categoría de datos recopilados de un vehículo conectado, considera que el ejemplo que utiliza la guía sobre los datos de ubicación ("los datos de ubicación solo deben recopilarse si es absolutamente necesario para el procedimiento") exagera el riesgo asociado a este tipo de datos. Considera que debería de incluirse un ejemplo más genérico vinculado a los campos de uso de la industria y no algo tan específico[31].

[30] RSA Insurance Group, *op.cit.,* p.3.

[31] WEJO LTD, *op.cit.*, pp. 3-4.

6.3. Privacidad desde el diseño y por defecto

Se remite a los requisitos establecidos en el art. 25 GDPR. Las tecnologías deben estar diseñadas para minimizar la recopilación de datos personales, proporcionar configuraciones predeterminadas protectoras de la privacidad y garantizar que los interesados estén bien informados y tengan la opción de modificar fácilmente las configuraciones asociadas con sus datos personales. Plantea que una guía específica sobre cómo los fabricantes y proveedores de servicios pueden cumplir con la protección de datos por diseño y por defecto podría ser beneficiosa para la industria (párrafo 68).

Enumera tres prácticas que podrían ayudar a mitigar los riesgos para los derechos y libertades de las personas físicas asociadas con los vehículos conectados:

- Tratamiento local de los datos personales
- Anonimización y pseudonimización de los datos personales
- Evaluación de impacto

6.3.1. Tratamiento local de los datos personales

En la medida de lo posible se debe evitar la cesión de datos fuera del vehículo. Se remite, en gran parte, al GDPR.

6.3.2. Anonimización y pseudonimización

Si los datos deben abandonar el vehículo, se debe considerar anonimizarlos antes de transmitirlos. La guía recuerda que los principios de protección de datos no se aplican a la información anónima. La información que no se relaciona con una persona física identificada o identificable o con datos personales que se convierten en anónimos de tal manera que el sujeto de datos ya no es identificable. Una vez que un conjunto de datos es verdaderamente anónimo y las personas ya no son identificables, la ley europea de protección de datos ya no se aplica. Como consecuencia, el anonimato, cuando sea relevante, puede ser una buena estrategia para mantener los beneficios y mitigar los riesgos en relación con los vehículos conectados (párrafo 76).

En el dictamen adoptado en abril de 2014 por el Grupo de Trabajo del Artículo 29 sobre técnicas de anonimato, se detallan medios, a veces en combinación, para alcanzar el anonimato de datos. Otras técnicas como la pseudonimización pueden ayudar a minimizar los riesgos generados por el procesamiento de datos, teniendo en cuenta que, en la mayoría de los casos, los datos directamente identificables no son necesarios para lograr el propósito del procesamiento. La pseudonimización consiste en reemplazar directamente los datos personales identificables por un pseudónimo no significativo. La pseudonimización es reversible, a diferencia del anonimato, y por tanto, está protegida por el GDPR (párrafo 77).

6.3.3. Evaluación de impacto

Los participantes de la industria deberán realizar una evaluación de impacto de protección de datos para identificar y mitigar los riesgos como se detalla en los arts. 35 y 36 GDPR (párrafo 79).

7. Derechos del interesado

7. 1. A estar informado

Antes del procesamiento de datos personales, el interesado deberá ser informado de, al menos, (párrafo 80):

- la identidad del controlador de datos
- el propósito del procesamiento,
- los destinatarios de los datos,
- el período durante el cual los datos serán almacenados
- y los derechos del sujeto de datos bajo el GDPR
- Otros que la guía especifica (párrafo 81)

La guía especifica sobre qué tendrá que estar informado el interesado, además de lo anterior, cuando los datos personales no se recopilan directamente de la persona interesada. Por ejemplo, un fabricante de vehículos puede querer utilizar los datos sobre el propietario del vehículo recopilados por el concesionario a fin de ofrecer un servicio de asistencia en carretera de emergencia (párrafo 82). También sobre qué tendrá que estar informado en caso de que los datos sean tratados por un nuevo controlador de datos, por ejemplo, si cruzan fronteras (párrafo 83). Sobre estos apartados, la RSA INSURANCE GROUP, que aunque comparte la importancia de proteger los datos de los interesados, insiste en que estos procedimientos deberían ser prácticos y sencillos puesto que son múltiples controladores de datos los que prestan servicios a los vehículos conectados[32].

Propone la guía distinguir la información dirigida a los interesados en dos capas, separando dos niveles de información. Por un lado, la información de primer nivel, que es la más importante para los interesados y, por otro lado, la información presumiblemente de interés en una etapa posterior (párrafo 84). Añade que se podrían usar íconos estandarizados además de la información necesaria para mejorar la transparencia al reducir potencialmente la necesidad de presentar grandes cantidades de información escrita a un interesado (párrafo 88).

La GERMAN INSURANCE ASSOCIATION, en relación con las dos capas de información, opina que se tiene que proporcionar demasiada información en el primer nivel y no entiende por qué los derechos del interesado deben describirse en este primer nivel[33]. Considera que debería bastar con informar a los interesados sobre la existencia de sus derechos sobre protección de datos y consultar la segunda etapa para obtener más información.

7..2. Derecho a interrumpir o retirar el consentimiento en cualquier momento.

Deben facilitarse mecanismos que permitan al interesado ejercer de forma efectiva sus derechos de protección de datos. En particular, su derecho de acceso, rectificación, eliminación, restricción del procesamiento y, según la base legal del procesamiento, su derecho a la portabilidad de los datos y su derecho a objetar (párrafo 87).

---

[32] RSA Insurance Group, *ob cit.,* p. 4.

[33] German Insurance Association, *ob cit.,* p. 10.

7.3. Sistema de gestión de perfiles

Para facilitar las modificaciones de la configuración, debe implementarse un sistema de gestión de perfiles dentro del vehículo para almacenar las preferencias de los conductores conocidos y ayudarlos a cambiar fácilmente su configuración de privacidad en cualquier momento. El sistema de gestión de perfiles del vehículo debe centralizar todas las configuraciones de datos cada uno de los perfiles para facilitar el acceso, rectificación y eliminación de datos personales de los sistemas del vehículo a solicitud del interesado. Se debe permitir a los conductores detener la recopilación de ciertos tipos de datos, temporal o permanentemente, en cualquier momento, excepto si una legislación específica establece lo contrario o si los datos son esenciales para las funciones críticas del vehículo (párrafo 88).

Sobre este último aspecto, la ha mostrado su disconformidad sobre que los interesados puedan interrumpir la recopilación de datos en cualquier momento[34]. No se ha tenido en cuenta, de nuevo, los seguros telemáticos en el momento de su redacción.

8. Seguridad y confidencialidad

Los fabricantes de vehículos y equipos, los proveedores de servicios y otros controladores de datos deberán establecer medidas que garanticen la seguridad y confidencialidad de los datos procesados y tomar todas las precauciones útiles para evitar que una persona no autorizada tome el control. La guía enumera las medidas que los participantes de la industria deberían considerar (párrafo 90). Y enumera otra lista de medidas destinada específicamente a los fabricantes de vehículos (párrafo 91).

9. Transmisión de datos a terceros

En principio, solo el controlador de datos y el interesado tienen acceso a los datos generados por un vehículo conectado. Sin embargo, el controlador de datos puede transmitir datos personales a un tercero, siempre que dicha transmisión se base en una de las bases legales establecidas en el art. 6 GDPR (párrafo 93).

El fabricante del vehículo, el proveedor de servicios u otro controlador de datos puede transmitir datos personales a un procesador de datos seleccionado para desempeñar un papel en la prestación del servicio al interesado, siempre que el procesador de datos no use esos datos para su propio propósito. Los controladores y procesadores de datos elaborarán un contrato u otro documento legal que especifique las obligaciones de cada parte y establezca las disposiciones del art. 28 GDPR (párrafo 94).

En vista de la posible sensibilidad de los datos de uso del vehículo, la guía recomienda que el consentimiento del interesado se obtenga sistemáticamente antes de que sus datos se transmitan a un tercero que actúe como controlador de datos. El tercero se hace responsable de los datos que recibe y está sujeto a todas las disposiciones del GDPR (párrafo 95).

[34] *Ídem,* p. 11.

Y una última mención especial para cuando los datos personales se transfieren fuera del Espacio Económico Europeo. Se prevé salvaguarda adicional para garantizar la protección de los datos (párrafo 96).

10. Estudio de casos

La guía ha ejemplificado distintos supuestos en los que se podría aplicar y en los que detalla la cual es la finalidad, la categoría de los datos recolectados, el periodo de retención según el tipo de dato, los derechos del sujeto interesado, las medidas de seguridad que deben ser implementadas y los terceros con los que se compartirán los datos personales tratados.

Concretamente ha previsto siete casos prácticos que versan sobre:

a. La modalidad de póliza *"Pay as you drive (PAYD)",*
b. El alquiler y reserva de plazas de aparcamiento,
c. El sistema de llamadas de emergencia "eCall",
d. Accidentología,
e. Medidas antirrobo y
f. La información almacenada en coches de alquiler.

Y aunque los expertos coinciden en que este apartado de la guía es de gran utilidad, muchos coinciden también en que hay algunos errores conceptuales en ellos o echan en falta que se hayan ejemplificado también otros supuestos en los que la guía será de gran aplicación.

EUROPEAN INSURANCE y la GERMAN INURANCE ASSOCIATION sugieren una revisión del primer estudio de caso sobre el tipo de póliza "Pay as you drive (PAYD)"[35]. La definición y el análisis que hace la guía sobre este tipo de pólizas más bien se refiere a una "Pay how you drive (PHYD)". Y afirmaciones como que las pólizas telemáticas no son servicios de la sociedad de la información son incorrectas (párrafo 105)[36].

FRESHFIELDS BRUCKHAUS DERINGER, despacho de abogados que asesora a la empresa de alquiler de vehículos SIXT SE., sugiere una revisión del último estudio de caso sobre la información almacenada en los coches de alquiler[37].

Otras sugieren incorporar un supuesto que afecte a los servicios de reparación y mantenimiento ya que aparecen en varias ocasiones a lo largo de la guía[38]. Y otras proponen añadir algún caso práctico que sea aplicable a los fabricantes de los vehículos conectados[39].

---

[35] EUROPEAN INSURANCE, *ob cit.,* p. 6; GERMAN INSURANCE ASSOCIATION, *ob cit.,* p. 13.

[36] EUROPEAN INSURANCE, ob cit., p. 6; GERMAN INSURANCE ASSOCIATION, *ob cit.,* p. 12; RSA INSURANCE GROUP, *ob cit.,* p.1

[37] FRESHFIELDS BRUCKHAUS DERINGER, "Memorandum The first Draft of the European Data Protection Board (EDPB) of the "Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications", pp. 1-8.

[38] BELRON, *ob cit,* p.3; FEDERATION OF DANISH MOTORISTS, *ob cit.,* p. 4.

[39] GERMAN INSURANCE ASSOCIATION, *ob cit.,* p. 13.

11. Conclusiones

La guía publicada es, sin duda, muy útil. Demuestra claramente un interés por parte de la Unión Europea por proteger los intereses de los consumidores ante el creciente uso de dispositivos conectados.

A lo largo del trabajo he mencionado algunas de las críticas o sugerencias de mejora que algunas entidades han presentado durante el primer periodo de consultas públicas que finaliza el próximo 1 de mayo. Algunas, bajo mi parecer, sencillas de incluir o de reformular y otras, no tanto. No obstante, remarco que en estos comentarios se manifiesta también en muchas ocasiones el apoyo al contenido de la guía. Cabe ahora esperar la reacción del grupo de trabajo a los comentarios recibidos.