Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados y las aplicaciones relacionadas con la movilidad

Versión 2.0

Adoptadas el 9 de marzo de 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historial de versiones

Versión 2.0	9 de marzo de 2021	Adopción de las Directrices después de la consulta pública
Versión 1.0	28 de enero de 2020	Adopción de las Directrices para la consulta pública

Índice

Visto el artículo 70, apartado 1, letra e), del 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 y por el que se deroga la Directiva 95/46/CE (en adelante, «el RGPD»),

Visto el Acuerdo EEE, y en particular su anexo XI y su Protocolo 37, modificado por la Decisión n.º 154/2018 del Comité Mixto del EEE, de 6 de julio de 2018[1],

Vistos los artículos 12 y 22 de su Reglamento interno,

HA ADOPTADO LAS SIGUIENTES DIRECTRICES

1 INTRODUCCIÓN

1. El automóvil, símbolo de la economía del siglo XX, es uno de los productos de consumo masivo que ha repercutido en toda la sociedad. Comúnmente asociados a la noción de libertad, los coches suelen considerarse algo más que un medio de transporte, y representan un espacio privado en el que las personas pueden disfrutar de una forma de autonomía de decisión, sin interferencias externas. Hoy en día, a medida que los vehículos conectados se van imponiendo, esa visión ya no se corresponde con la realidad. La conectividad en el vehículo se está extendiendo rápidamente, desde los modelos de lujo y las marcas de prestigio hasta los modelos de gran volumen del mercado medio, y los vehículos se están convirtiendo en enormes centros de datos. No solo los vehículos, sino también los conductores y los pasajeros están cada vez más conectados. De hecho, muchos modelos introducidos en el mercado en los últimos años integran sensores y equipos conectados a bordo que pueden recoger y registrar, entre otras cosas, el rendimiento del motor, los hábitos de conducción, los lugares visitados y, posiblemente, incluso los movimientos oculares del conductor, su pulso o datos biométricos con el fin de identificar de forma inequívoca a una persona física[2].

2. Este tratamiento de datos se produce en un ecosistema complejo, que no se limita a los actores tradicionales de la industria del automóvil, sino que también está conformado por la aparición de nuevos actores pertenecientes a la economía digital. Estos nuevos actores pueden ofrecer servicios de información y entretenimiento, como música en línea, información sobre el estado de las carreteras y el tráfico, o proporcionar sistemas y servicios de asistencia a la conducción, como el *software* de piloto automático, actualizaciones del estado del vehículo, seguros basados en el uso o cartografía dinámica. Además, dado que los vehículos están conectados a través de redes de comunicación electrónicas, los administradores de infraestructuras viarias y los operadores de telecomunicaciones que intervienen en este proceso también desempeñan un papel importante con respecto a las posibles operaciones de tratamiento aplicadas a los datos personales de los conductores y pasajeros.

3. Es más, los vehículos conectados están generando cantidades de datos cada vez mayores, la mayoría de los cuales pueden considerarse datos personales, ya que estarán relacionados

[1] Las referencias a los «Estados miembros» en el presente documento deben entenderse como referencias a los «Estados miembros del EEE».
[2] Infografía *Data and the connected car* por el Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.

con los conductores o los pasajeros. Aunque los datos recogidos por un coche conectado no estén directamente relacionados con un nombre, sino con aspectos técnicos y características del vehículo, afectarán al conductor o a los pasajeros del coche. A modo de ejemplo, los datos relativos al estilo de conducción o a la distancia recorrida, los relativos al desgaste de las piezas del vehículo, los datos de localización o los recogidos por las cámaras pueden referirse al comportamiento del conductor, así como a información sobre otras personas que puedan estar a bordo o sobre los interesados que pasen por allí. Estos datos técnicos son producidos por una persona física y permiten su identificación directa o indirecta por el responsable del tratamiento o por un tercero. El vehículo puede considerarse como una terminal que puede ser utilizada por diferentes usuarios. Por lo tanto, al igual que en el caso de un ordenador personal, esta potencial pluralidad de usuarios no afecta al carácter personal de los datos.

4. En 2016, la Fédération Internationale de l'Automobile (FIA) llevó a cabo una campaña en toda Europa denominada «My Car My Data» para conocer la opinión de los europeos sobre los vehículos conectados[3]. Aunque reveló el gran interés de los conductores por la conectividad, también puso de manifiesto la atención que debe ejercerse respecto al uso de los datos producidos por los vehículos, así como la importancia de cumplir la legislación sobre la protección de datos personales. Así pues, el reto es, para cada parte interesada, incorporar la dimensión de la «protección de los datos personales» desde la fase de diseño del producto, y garantizar que los usuarios de los automóviles disfruten de transparencia y control en relación con sus datos, de conformidad con el considerando 78 del RGPD. Este enfoque contribuye a reforzar la confianza de los usuarios y, por tanto, el desarrollo a largo plazo de esas tecnologías.

1.1 Trabajos conexos

5. Los vehículos conectados se han convertido en un tema importante para los reguladores durante el último decenio y el interés ha aumentado de manera considerable en los últimos años. Así, se han publicado diversos trabajos a nivel nacional e internacional sobre la seguridad y la privacidad de los vehículos conectados. Estas normativas e iniciativas pretenden complementar los marcos existentes de protección de datos y privacidad con normas sectoriales específicas o proporcionar orientación a los profesionales.

1.1.1 Iniciativas a nivel europeo e internacional

6. Desde el 31 de marzo de 2018, es obligatorio el sistema eCall basado en el número 112 integrado en todos los nuevos tipos de vehículos M1 y N1 (turismos y vehículos ligeros)[4][5]. En 2006, el Grupo de Trabajo del Artículo 29 ya había adoptado un documento de trabajo sobre la protección de datos y las consecuencias para la intimidad en la iniciativa eCall[6]. Además, como se ha comentado anteriormente, el Grupo de Trabajo del Artículo 29 también adoptó, en octubre de 2017, un dictamen sobre el tratamiento de datos personales en el contexto de los sistemas de transporte inteligente y cooperativos (STI-C).

7. En enero de 2017, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) publicó un estudio centrado en la ciberseguridad y la resiliencia de los vehículos inteligentes en el que se enumeran los activos sensibles, así como las amenazas y los riesgos correspondientes, los factores de mitigación y las posibles medidas de seguridad

[3] Campaña «My Car My Data»; http://www.mycarmydata.eu/.
[4] El servicio de llamadas de emergencia interoperable en toda la Unión (eCall)l; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.
[5] Decisión n.º 585/2014/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, sobre la implantación del servicio de llamadas de emergencia interoperable en toda la Unión (eCall) (texto pertinente a efectos del EEE); https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014D0585.
[6] Documento de trabajo sobre la protección de datos y las consecuencias para la intimidad en la iniciativa eCall; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_es.pdf.

a aplicar[7]. En septiembre de 2017, la Conferencia Internacional de Autoridades de Protección de Datos y Protección de la Intimidad adoptó una resolución sobre los vehículos conectados[8]. Por último, en abril de 2018, el Grupo de trabajo internacional sobre protección de datos en las telecomunicaciones también adoptó un documento de trabajo sobre los vehículos conectados[9].

1.1.2 Iniciativas nacionales de los miembros del Comité Europeo de Protección de Datos (CEPD)

8. En enero de 2016, la Conferencia de Autoridades Federales y Estatales de Protección de Datos de Alemania y la Asociación Alemana de la Industria del Automóvil (VDA) publicaron una declaración común sobre los principios de protección de datos en los vehículos conectados y no conectados[10]. En agosto de 2017, el Centro de Vehículos Conectados y Autónomos del Reino Unido publicó una guía en la que se exponen los principios de la ciberseguridad para los vehículos conectados y automatizados, con el fin de concienciar al sector de la automoción sobre esta cuestión[11]. En octubre de 2017, la autoridad francesa de protección de datos (*Commission Nationale de l'Informatique et des Libertés, CNIL*) publicó un paquete de cumplimiento para los vehículos conectados con el fin de proporcionar asistencia a las partes interesadas sobre cómo integrar la protección de datos desde el diseño y por defecto, así como para permitir a los interesados tener un control efectivo sobre sus datos[12].

1.2 Normativa aplicable

9. El marco jurídico pertinente de la UE es el RGPD. Se aplica en cualquier caso en que el tratamiento de datos en el contexto de los vehículos conectados implique el tratamiento de datos personales de personas físicas.

10. Además del RGPD, la Directiva 2002/58/CE, revisada por la Directiva 2009/136/CE (en adelante, la «Directiva sobre la privacidad y las comunicaciones electrónicas»), **establece una norma específica para todos los agentes que deseen almacenar o acceder a la información almacenada en el equipo terminal de un abonado o usuario en el Espacio Económico Europeo (EEE).**

11. De hecho, si bien la mayoría de las disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas (artículo 6, artículo 9, etc.) solo se aplican a los proveedores de servicios de comunicaciones electrónicas disponibles al público y a los proveedores de redes de comunicaciones públicas, el artículo 5, apartado 3, de dicha Directiva es una disposición general. No solo se aplica a los servicios de comunicaciones electrónicas, sino también a toda entidad, privada o pública, que registre o lea información en un equipo terminal sin tener en cuenta la naturaleza de los datos que se almacenan o a los que se accede.

---

[7] *Cyber security and resilience of smart cars*; https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars.
[8] *Resolution on data protection in automated and connected vehicles*; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.
[9] *Working paper on connected vehicles*; https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/.
[10] *Data protection aspects of using connected and non-connected vehicles*; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.
[11] *Principles of cyber security for connected and automated vehicles*; https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles.
[12] *Compliance package for a responsible use of data in connected cars*; https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data.

12. En cuanto al concepto de «equipo terminal», la definición viene dada por la Directiva 2008/63/CE[13]. El artículo 1, letra a), define el equipo terminal como un «el equipo conectado directa o indirectamente a la interfaz de una red pública de telecomunicaciones para transmitir, procesar o recibir información; en ambos casos (conexión directa o indirecta), la conexión podrá realizarse por cable, fibra óptica o vía electromagnética; la conexión será indirecta si se interpone un aparato entre el equipo terminal y la interfaz de la red pública; b) se considerarán también como equipos terminales los equipos de las estaciones terrenas de comunicación por satélite».

13. En consecuencia, siempre que se cumplan los criterios mencionados, el vehículo conectado y el dispositivo conectado a él deben considerarse como un «equipo terminal» (como un ordenador, un teléfono inteligente o una televisión híbrida) y se aplican, en su caso, las disposiciones del artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

14. Como señala el CEPD en su Dictamen 5/2019 sobre la interacción entre la Directiva sobre la privacidad y las comunicaciones electrónicas y el RGPD[14], el artículo 5, apartado 3, de la Directiva establece que, por regla general, y sin perjuicio de las excepciones a dicha norma mencionadas en el apartado 17 del presente documento, se requiere el consentimiento previo para el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario. En la medida en que la información almacenada en el equipo de los usuarios finales constituya datos personales, el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas prevalecerá sobre lo dispuesto en el artículo 6 del RGPD en lo relativo a la actividad de almacenamiento o de acceso a dicha información[15]. Cualquier operación de tratamiento de datos personales posterior a las mencionadas operaciones de tratamiento, incluido el tratamiento de datos personales obtenidos mediante el acceso a la información en el equipo terminal, debe tener una base jurídica en virtud del artículo 6 del RGPD para ser lícita[16].

15. Dado que el responsable del tratamiento, al solicitar el consentimiento para el almacenamiento o la obtención de acceso a la información con arreglo al artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas, deberá informar al interesado sobre los fines del tratamiento de los datos, incluido cualquier tratamiento posterior a las operaciones mencionadas (es decir, el «tratamiento posterior»). El consentimiento en virtud del artículo 6 del RGPD será generalmente la base jurídica más adecuada para regular el tratamiento de los datos personales posterior a dichas operaciones (en la medida en que la finalidad del tratamiento posterior esté comprendida en el consentimiento del interesado, véanse los apartados 53 y 54 del presente documento). Por lo tanto, es probable que el consentimiento constituya la base jurídica tanto para el almacenamiento y el acceso a la información ya almacenada como para el tratamiento posterior de los datos personales[17]. De hecho, al evaluar el cumplimiento del artículo 6 del

[13] Directiva 2008/63/CE de la Comisión, de 20 de junio de 2008, relativa a la competencia en los mercados de equipos terminales de telecomunicaciones (versión codificada) (texto pertinente a efectos del EEE); https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32008L0063.

[14] Comité Europeo de Protección de Datos, Dictamen 5/2019 sobre la interacción entre la Directiva sobre la privacidad y las comunicaciones electrónicas y el Reglamento general de protección de datos, en particular en lo que respecta a la competencia, funciones y poderes de las autoridades de protección de datos, adoptado el 12 de marzo de 2019 (en lo sucesivo, el «Dictamen 5/2019»), apartado 40.

[15] Véase la nota 15, apartado 40.

[16] Véase la nota 15, apartado 41.

[17] El consentimiento requerido por el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas y el consentimiento necesario como base jurídica para el tratamiento de los datos (artículo 6 del RGPD) para el mismo fin específico pueden obtenerse al mismo tiempo (por ejemplo, marcando una casilla que indique claramente a qué da su consentimiento el interesado).

RGPD, hay que tener en cuenta que el tratamiento en su conjunto implica actividades específicas para las que el legislador de la UE ha tratado de proporcionar protección adicional[18]. Además, los responsables del tratamiento deben tener en cuenta el efecto sobre los derechos de los interesados al identificar el fundamento jurídico adecuado que permita respetar el principio de lealtad[19]. La conclusión es que los responsables del tratamiento no pueden invocar el artículo 6 del RGPD para rebajar la protección adicional que ofrece el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

16. El CEPD recuerda que la noción de consentimiento que figura en la Directiva sobre la privacidad y las comunicaciones electrónicas es la misma que la que contempla el RGPD y debe cumplir todos los requisitos del consentimiento según lo dispuesto en el artículo 4, apartado 11, y el artículo 7 del RGPD.

17. Sin embargo, aunque el consentimiento es el principio, el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas permite que el almacenamiento de información o la obtención de acceso a la información que ya está almacenada en el equipo terminal queden exentos del requisito de consentimiento informado si el consentimiento cumple uno de los siguientes criterios:

    - **Exención 1:** al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas.
    - **Exención 2:** cuando sea estrictamente necesario para que el proveedor de una empresa de información proporcione un servicio explícitamente solicitado por el abonado o usuario.

18. En estos casos, el tratamiento de los datos personales, incluidos los obtenidos mediante el acceso a la información en el equipo terminal, se basa en una de las bases jurídicas previstas en el artículo 6 del RGPD. Por ejemplo, no es necesario el consentimiento cuando el tratamiento de datos es necesario para prestar los servicios de navegación por GPS solicitados por el interesado cuando dichos servicios pueden calificarse de servicios de la sociedad de la información.

1.3 Ámbito de aplicación

19. El CEPD desea señalar que las presentes Directrices tienen como objetivo facilitar el cumplimiento del tratamiento de datos personales realizado por una amplia gama de partes interesadas que operan en este entorno. Sin embargo, no aspiran a abarcar todos los casos de uso posibles en este contexto ni a proporcionar orientación para todas las situaciones específicas posibles.

20. El ámbito de aplicación de este documento se centra en particular en el tratamiento de datos personales en relación con el uso no profesional de vehículos conectados por parte de los interesados: por ejemplo, conductores, pasajeros, propietarios de vehículos, otros usuarios de la vía pública, etc. Más concretamente, se centra en los datos personales: i) que se tratan dentro del vehículo, ii) se intercambian entre el vehículo y los dispositivos personales conectados a él (por ejemplo, el teléfono inteligente del usuario) o iii) se recogen localmente en el vehículo y se exportan a entidades externas (por ejemplo, fabricantes de vehículos, administradores de infraestructuras, compañías de seguros, reparadores de automóviles) para su tratamiento ulterior.

21. La definición de vehículo conectado debe entenderse como un concepto amplio en este documento. Se puede definir como un vehículo equipado con numerosas unidades de

[18] Dictamen 5/2019, apartado 41.

[19] Comité Europeo de Protección de Datos, Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del RGPD en el contexto de la prestación de servicios en línea a los interesados, versión 2.0, de 8 de octubre de 2019, apartado 1.

control electrónico (UCE) que están conectadas entre sí a través de una red integrada en el vehículo, así como instalaciones de conectividad que le permiten compartir información con otros dispositivos tanto dentro como fuera del vehículo. De este modo, se pueden intercambiar datos entre el vehículo y los dispositivos personales conectados a él, permitiendo, por ejemplo, replicar las aplicaciones móviles en la unidad de información y entretenimiento del salpicadero del vehículo. Asimismo, el presente documento aborda el desarrollo de aplicaciones móviles autónomas, es decir, independientes del vehículo (por ejemplo, basadas en el uso exclusivo del teléfono inteligente) para asistir a los conductores, ya que contribuyen a las capacidades de conectividad del vehículo, aunque no se basen efectivamente en la transmisión de datos con el vehículo en sí. Las aplicaciones para los vehículos conectados son múltiples y diversas y pueden incluir[20]:

22. *Gestión de la movilidad:* funciones que permiten a los conductores llegar rápidamente y de forma rentable a un destino, proporcionando información oportuna sobre la navegación por GPS, las condiciones ambientales potencialmente peligrosas (por ejemplo, carreteras heladas), la congestión del tráfico u obras en la carretera, la asistencia en aparcamientos o garajes, la optimización del consumo de combustible o la tarificación vial.

23. *Gestión de vehículos:* funciones que supuestamente ayudan a los conductores a reducir los costes operativos y a mejorar la facilidad de uso, como la notificación del estado del vehículo y los recordatorios de servicio, la transferencia de datos de uso (por ejemplo, para los servicios de reparación del vehículo), los seguros personalizados de pago por uso (*Pay As/How You Drive*), las operaciones remotas (por ejemplo, el sistema de calefacción) o las configuraciones de perfiles (por ejemplo, la posición del asiento).

24. *Seguridad vial:* funciones que advierten al conductor de peligros externos y respuestas internas, como la protección contra colisiones, las advertencias de peligro, los avisos de salida de carril, la detección de somnolencia del conductor, la llamada de emergencia (eCall) o las «cajas negras» de investigación de accidentes (registrador de datos de incidentes).

25. *Ocio:* funciones de información y entretenimiento para el conductor y los pasajeros, como interfaces de teléfonos inteligentes (llamadas de manos libres, mensajes de texto generados por voz), puntos de acceso WLAN, música, vídeo, Internet, redes sociales, oficina móvil o servicios «domésticos inteligentes».

26. *Asistencia al conductor:* funciones que implican una conducción parcial o totalmente automatizada, como la asistencia operativa o el piloto automático con tráfico intenso, al aparcar o en autopistas,

27. *Bienestar:* funciones que controlan el confort, la capacidad y la aptitud física del conductor para conducir, como la detección de la fatiga o la asistencia médica.

28. Por lo tanto, los vehículos pueden estar conectados de forma nativa o no y los datos personales pueden recogerse por varios medios, entre ellos: i) sensores del vehículo, ii) cajas telemáticas, o iii) aplicaciones móviles (por ejemplo, a las que se accede desde un dispositivo perteneciente a un conductor). Para que se incluyan en el ámbito de aplicación de este documento, las aplicaciones móviles deben estar relacionadas con el contexto de la conducción. Por ejemplo, las aplicaciones de navegación GPS entran en el ámbito de aplicación. Sin embargo, las aplicaciones cuyas funcionalidades solo sugieren a los conductores lugares de interés (restaurantes, monumentos históricos, etc.) quedan fuera del ámbito de estas Directrices.

29. Muchos de los datos que genera un vehículo conectado se refieren a una persona física identificada o identificable y, por tanto, constituyen datos personales. Estaríamos hablando,

[20] *PwC Strategy 2014. In the fast lane. The bright future of connected cars*: https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

por ejemplo, de datos directamente identificables (la identidad completa del conductor), así como datos indirectamente identificables como la información de los viajes realizados, datos de uso del vehículo (datos relativos al estilo de conducción o la distancia recorrida), o datos técnicos del vehículo (datos relativos al desgaste de las piezas del vehículo) que, mediante referencias cruzadas con otros archivos, y especialmente el número de identificación del vehículo (NIV), pueden relacionarse con una persona física. Los metadatos, tales como el estado de mantenimiento del vehículo, también pueden ser datos personales en los vehículos conectados. En otras palabras, todos los datos que puedan asociarse a una persona física entran, por tanto, en el ámbito de aplicación de este documento.

30. El ecosistema de los vehículos conectados abarca un amplio espectro de partes interesadas, más concretamente los actores tradicionales de la industria del automóvil, así como los actores emergentes de la industria digital. Por lo tanto, estas Directrices están dirigidas a los fabricantes de vehículos, fabricantes de equipos y proveedores de automóviles, reparadores de automóviles, concesionarios, proveedores de servicios para vehículos, gestores de flotas, compañías de seguros de automóviles, proveedores de entretenimiento, operadores de telecomunicaciones, administradores de infraestructuras viales y autoridades públicas, así como a los interesados. El CEPD subraya que las categorías de interesados a las que se refieren los datos difieren de un servicio a otro (por ejemplo, conductores, propietarios, pasajeros, etc.). Se trata de una lista no exhaustiva, ya que el ecosistema conlleva una gran variedad de servicios, incluidos los servicios para los que se necesita una autenticación o identificación directa y los servicios para los que no se necesita.

31. Algunos tratamientos de datos efectuados por personas físicas dentro del vehículo se inscriben «en el ejercicio de actividades exclusivamente personales o domésticas» y, por tanto, quedan fuera del ámbito de aplicación del RGPD[21]. En concreto, se trata del uso de datos personales dentro de los vehículos por parte de los únicos interesados que facilitaron dichos datos al salpicadero del vehículo. No obstante, el CEPD recuerda que, de conformidad con su considerando 18, el RGPD «se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas».

1.3.1 Fuera del ámbito de aplicación de este documento

32. Los empleadores que proporcionan coches de empresa a sus empleados pueden querer controlar sus acciones (por ejemplo, para garantizar la seguridad del empleado, de los bienes o de los vehículos, para asignar recursos, para hacer un seguimiento y facturar un servicio o para comprobar el tiempo de trabajo). El tratamiento de datos realizado por los empleadores en este contexto plantea consideraciones específicas del contexto laboral, que podrían regularse mediante leyes laborales a nivel nacional que no pueden detallarse en estas Directrices[22].

33. Aunque el tratamiento de datos en el contexto de los vehículos comerciales utilizados con fines profesionales (como el transporte público) y el transporte compartido y las soluciones de movilidad como servicio (MaaS)pueden plantear consideraciones específicas que quedan fuera del ámbito de estas Directrices generales, muchos de los principios y recomendaciones aquí expuestos también serán aplicables a dichos tipos de tratamiento.

34. Los vehículos conectados, al ser sistemas habilitados por radio, son objeto de seguimiento pasivo, como el seguimiento por wifi o Bluetooth. En ese sentido, no se diferencian de otros dispositivos conectados y entran en el ámbito de aplicación de la Directiva sobre la

[21] Véase el artículo 2, apartado 2, letra c), del RGPD.
[22] El Grupo de Trabajo del Artículo 29 profundizó en este tema en su Dictamen 2/2017 sobre el tratamiento de datos en el trabajo (WP249); https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

privacidad y las comunicaciones electrónicas, que se está revisando actualmente. Por lo tanto, esto excluye también el seguimiento a gran escala de los vehículos equipados con wifi[23] por una red densa de transeúntes que utilizan servicios comunes de localización de teléfonos inteligentes. Estos informan rutinariamente de todas las redes wifi visibles a los servidores centrales. Dado que el sistema de conexión wifi incorporado puede considerarse un identificador secundario del vehículo[24], se corre el riesgo de que se recojan sistemáticamente y de forma continua los perfiles completos de desplazamiento del vehículo.

35. Los vehículos están cada vez más equipados con dispositivos de registro de imágenes (por ejemplo, sistemas de cámaras de aparcamiento o *dashcams*). Dado que se trata de la filmación de lugares públicos, que requiere una evaluación del marco legislativo pertinente específico de cada Estado miembro, este tratamiento de datos queda fuera del ámbito de las presentes Directrices.

36. El tratamiento de datos que permiten los sistemas de transporte inteligentes y cooperativos (STI-C), tal como se define en la Directiva 2010/40/UE[25], se ha abordado en un dictamen específico del Grupo de Trabajo del Artículo 29[26]. Aunque la definición del concepto de STI-C en la Directiva no lleva ninguna especificación técnica, el Grupo de Trabajo del Artículo 29 se centra en su Dictamen en las comunicaciones de corto alcance, es decir, que no implican la intervención de un operador de red. Más concretamente, proporciona análisis para casos de uso específicos elaborados para el despliegue inicial y se compromete a evaluar en una fase posterior los nuevos problemas que sin duda se plantearán cuando aumenten los niveles de automatización. Dado que las implicaciones para la protección de datos en el contexto de los STI-C son muy específicas (cantidades sin precedentes de datos de localización, transmisión continua de datos personales, intercambio de datos entre vehículos y otras instalaciones de infraestructura vial, etc.) y que todavía se están debatiendo a nivel europeo, las presentes Directrices no abordan el tratamiento de datos personales en ese contexto.

37. Por último, este documento no pretende abordar todos los posibles problemas y cuestiones que plantean los vehículos conectados, por lo que no puede considerarse exhaustivo.

1.4 Definiciones

38. El **tratamiento** de datos personales incluye cualquier operación que implique datos personales como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión o difusión, o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción, etc.[27]

[23] Para más información consúltese: https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html.
[24] Markus Ullmann, Tobias Franz, and Gerd Nolden, *Vehicle Identification Based on Secondary Vehicle Identifier -- Analysis, and Measurements, in Proceedings*, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Niza, Francia, 23 a 27 de julio de 2017, p. 32.
[25] Directiva 2010/40/UE del Parlamento Europeo y del Consejo, de 7 de julio de 2010, por la que se establece el marco para la implantación de los sistemas de transporte inteligentes en el sector del transporte por carretera y para las interfaces con otros modos de transporte; https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010L0040.
[26] Grupo de Trabajo del Artículo 29, Dictamen 3/2017 sobre el tratamiento de los datos personales en el contexto de los sistemas de transporte inteligentes (STI) cooperativos; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.
[27] Véase el artículo 4, apartado 2, del RGPD.

39. El **interesado** es la persona física a la que se refieren los datos objeto del tratamiento. En el contexto de los vehículos conectados, puede ser, en particular, el conductor (principal u ocasional), el pasajero o el propietario del vehículo[28].

40. El **responsable del tratamiento** es la persona que determina los fines y medios del tratamiento que tiene lugar en los vehículos conectados[29]. Los responsables del tratamiento de datos pueden ser proveedores de servicios que tratan los datos del vehículo para enviar al conductor información sobre el tráfico, mensajes de conducción eficiente o alertas sobre el funcionamiento del vehículo, compañías de seguros que ofrecen contratos de pago por uso (*Pay as you Drive*) o fabricantes de vehículos que recopilan datos sobre el desgaste de las piezas del vehículo para mejorar su calidad. De conformidad con el artículo 26 del RGPD, dos o más responsables del tratamiento pueden determinar conjuntamente los objetivos y los medios del tratamiento y, por tanto, ser considerados corresponsables. En este caso, tienen que definir claramente sus respectivas obligaciones, especialmente en lo que se refiere al ejercicio de los derechos de los interesados y al suministro de información a que se refieren los artículos 13 y 14 del RGPD.

41. El **encargado del tratamiento** es cualquier persona que trata datos personales para y por cuenta del responsable del tratamiento[30]. El encargado del tratamiento recoge y trata los datos siguiendo instrucciones del responsable del tratamiento, sin utilizarlos para sus propios fines. Por ejemplo, en algunos casos, los fabricantes de equipos y los proveedores de automóviles pueden tratar datos por cuenta de los fabricantes de vehículos (lo que no implica que no puedan ser responsables del tratamiento para otros fines). Además de exigir que los encargados del tratamiento de datos apliquen las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adaptado al riesgo, el artículo 28 del RGPD establece las obligaciones de los encargados del tratamiento.

42. El **destinatario** es la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero[31]. Por ejemplo, un socio comercial del proveedor de servicios que recibe del proveedor de servicios datos personales generados a partir del vehículo es un receptor de datos personales. Tanto si actúan como nuevos responsables del tratamiento de datos como si lo hacen como encargados del mismo, deberán cumplir todas las obligaciones impuestas por el RGPD.

43. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros[32]; el tratamiento posterior de tales datos por las citadas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento. Por ejemplo, las autoridades policiales y judiciales son terceros autorizados cuando solicitan datos personales en el marco de una investigación de acuerdo con el Derecho de la Unión Europea o de los Estados miembros.

[28] Véase el artículo 4, apartado 1, del RGPD.
[29] Véase el artículo 4, apartado 7, del RGPD y las Directrices 7/2020 del CEPD sobre los conceptos de responsable y encargado del tratamiento en el RGPD (en lo sucesivo, las «Directrices 7/2020»).
[30] Véanse el artículo 4, apartado 8, del RGPD y las Directrices 7/2020.
[31] Véanse el artículo 4, apartado 9, del RGPD y las Directrices 7/2020.
[32] Véanse el artículo 4, apartado 9, y el considerando 31 del RGPD.

1.5 Riesgos para la intimidad y la protección de datos

44. El Grupo de Trabajo del Artículo 29 ya ha expresado varias preocupaciones sobre los sistemas de Internet de los objetos (IO) que también pueden aplicarse a los vehículos conectados[33]. Las cuestiones relativas a la seguridad y el control de los datos ya destacadas en relación con la IO son aún más sensibles en el contexto de los vehículos conectados, ya que conllevan problemas de seguridad vial —y pueden afectar a la integridad física del conductor— en un entorno tradicionalmente percibido como aislado y protegido de interferencias externas.

45. Además, los vehículos conectados plantean problemas importantes para la protección de los datos y la intimidad en relación con el tratamiento de los datos de localización, ya que su carácter cada vez más intrusivo puede poner en peligro las posibilidades actuales de permanecer en el anonimato. El CEPD quiere hacer especial hincapié, y concienciar a las partes interesadas sobre ello, en que el uso de las tecnologías de localización requiere la aplicación de garantías específicas para evitar la vigilancia de las personas y el uso indebido de los datos.

1.5.1 Falta de control y asimetría de la información

46. Es posible que los conductores y los pasajeros de los vehículos no estén siempre adecuadamente informados sobre el tratamiento de datos que tiene lugar en un vehículo conectado o a través de él. La información puede facilitarse solo al propietario del vehículo, que puede no ser el conductor, y también puede no proporcionarse a tiempo. Por lo tanto, existe el riesgo de que las funcionalidades u opciones propuestas para ejercer el control necesario no basten para que los afectados puedan hacer valer sus derechos de protección de los datos y a la intimidad. Este aspecto es importante ya que, a lo largo de su vida útil, los vehículos pueden pertenecer a más de un propietario, ya sea porque se venden o porque se alquilan en régimen de arrendamiento financiero en lugar de comprarse.

47. Además, la comunicación en el vehículo puede activarse automáticamente o por defecto, sin que la persona sea consciente de ello. Si no existe la posibilidad de controlar eficazmente cómo interactúan el vehículo y sus equipos conectados, será sumamente difícil para el usuario controlar el flujo de datos. Será aún más difícil controlar su uso posterior y, por lo tanto, evitar la posible «desvirtuación de funciones».

1.5.2 Calidad del consentimiento del usuario

48. El CEPD subraya que, cuando el tratamiento de datos se basa en el consentimiento, deben cumplirse todos los elementos de un consentimiento válido, lo que significa que el consentimiento deberá ser libre, específico e informado y constituir una manifestación de voluntad inequívoca del interesado, tal como se interpreta en las Directrices del CEPD sobre el consentimiento[34]. Los responsables del tratamiento de datos deben prestar especial atención a las modalidades de obtención de un consentimiento válido por parte de los distintos participantes, como los propietarios o los usuarios de vehículos. Dicho consentimiento debe prestarse por separado, para fines específicos, no podrá agruparse con el contrato de compra o de arrendamiento de un automóvil nuevo. Debe ser igual de fácil retirar el consentimiento como lo fue darlo.

49. Lo mismo debe aplicarse cuando se requiera el consentimiento para cumplir con la Directiva sobre la privacidad y las comunicaciones electrónicas, por ejemplo, si hay almacenamiento de información u obtención de acceso a la información ya almacenada en el vehículo, como

[33] Grupo de Trabajo del Artículo 29, Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf.
[34] Comité Europeo de Protección de Datos, Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, versión 1.1, 4 de mayo de 2020 (en lo sucesivo, las «Directrices 5/2020»).

requiere en ciertos casos el artículo 5, apartado 3, de dicha Directiva. De hecho, como ya se ha señalado, el consentimiento en este contexto debe interpretarse a la luz del RGPD.

50. En muchos casos, el usuario puede no ser consciente del tratamiento de datos que se realiza en su vehículo. Esta falta de información constituye un obstáculo importante para demostrar un consentimiento válido con arreglo al RGPD, ya que el consentimiento debe ser informado. En tales circunstancias, el consentimiento no puede invocarse como base jurídica para el correspondiente tratamiento de datos con arreglo al RGPD.

51. Los mecanismos clásicos utilizados para obtener el consentimiento de los interesados pueden ser difíciles de aplicar en el contexto de los vehículos conectados, lo que da lugar a un consentimiento de «baja calidad» debido a la falta de información o a la imposibilidad fáctica de dar un consentimiento ajustado a las preferencias expresadas por las personas. En la práctica, el consentimiento también puede ser difícil de obtener para los conductores y pasajeros que no estén relacionados con el propietario del vehículo en el caso de vehículos de segunda mano o que han sido objeto de arrendamiento financiero, alquiler o préstamo.

52. Cuando la Directiva sobre la privacidad y las comunicaciones electrónicas no exige el consentimiento del interesado, el responsable del tratamiento tiene, no obstante, la responsabilidad de elegir la base jurídica, con arreglo al artículo 6 del RGPD, que resulte más adecuada para el tratamiento de los datos personales.

1.5.3 Tratamiento ulterior de datos personales

53. Cuando los datos se recojan sobre la base del consentimiento, tal como exige el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas, o de una de las excepciones de dicho artículo, y posteriormente se tratan de acuerdo con el artículo 6 del RGPD, solo podrán seguir tratándose si el responsable del tratamiento solicita un consentimiento específico para esta otro fin distinto o si el responsable del tratamiento puede demostrar que se basa en una ley de la Unión o de un Estado miembro para salvaguardar los objetivos mencionados en el artículo 23, apartado 1, del RGPD[35]. El CEPD considera que el tratamiento ulterior sobre la base de una prueba de compatibilidad según el artículo 6, apartado 4, del RGPD no es posible en estos casos, ya que socavaría la norma de protección de datos de la Directiva sobre la privacidad y las comunicaciones electrónicas. De hecho, el consentimiento, cuando se requiera en virtud de la Directiva sobre la privacidad y las comunicaciones electrónicas, debe ser específico e informado, lo que significa que los interesados deben conocer cada finalidad del tratamiento de datos y tener derecho a rechazar finalidades específicas[36]. Si se considera que el tratamiento ulterior sobre la base de una prueba de compatibilidad con arreglo al artículo 6, apartado 4, del RGPD es posible, se eludiría el principio mismo de los requisitos de consentimiento establecidos por la actual Directiva.

54. El CEPD recuerda que el consentimiento inicial nunca legitimará el tratamiento ulterior, ya que el consentimiento debe ser informado y específico para ser válido.

55. Por ejemplo, los datos de telemetría, que se recogen durante el uso del vehículo con fines de mantenimiento, no pueden divulgarse a las compañías de seguros de automóviles sin el consentimiento de los usuarios con el fin de crear perfiles de conductores para ofrecer pólizas de seguros basadas en el comportamiento de conducción.

56. Además, los datos recogidos por los vehículos conectados pueden ser tratados por las autoridades policiales para detectar el exceso de velocidad u otras infracciones siempre y cuando se cumplan las condiciones específicas de la Directiva sobre protección de datos en el ámbito penal. En este caso, dichos datos se considerarán relativos a condenas e

[35] Véanse también las Directrices 10/2020 del CEPD sobre las restricciones en virtud del artículo 23 del RGPD.
[36] Directrices 5/2020, apartados 3.2 y 3.3.

infracciones penales en las condiciones establecidas por el artículo 10 del RGPD y cualquier legislación nacional aplicable. Los fabricantes pueden facilitar a las autoridades policiales dichos datos si se cumplen las condiciones específicas para el tratamiento. El CEPD señala que el tratamiento de datos personales con el único fin de satisfacer las solicitudes de las autoridades policiales no constituye un fin determinado, explícito y legítimo en el sentido del artículo 5, apartado 1, letra b), del RGPD. Cuando las autoridades policiales están autorizadas por la ley, podrían ser terceros en el sentido del artículo 4, apartado 10, del RGPD, en cuyo caso los fabricantes tendrían derecho a facilitarles los datos de que dispongan, siempre que se respete el marco jurídico pertinente de cada Estado miembro.

1.5.4 Recogida excesiva de datos

57. Con el número cada vez mayor de sensores que se despliegan en los vehículos conectados, existe un riesgo muy alto de que se recojan demasiados datos en comparación con lo necesario para lograr la finalidad.

58. El desarrollo de nuevas funcionalidades, y más concretamente las basadas en algoritmos de aprendizaje automático, puede requerir que se recoja una gran cantidad de datos durante un largo periodo de tiempo.

1.5.5 Seguridad de los datos personales

59. La pluralidad de funcionalidades, servicios e interfaces (por ejemplo, web, USB, RFID, wifi) que ofrecen los vehículos conectados aumenta la superficie de ataque y, por lo tanto, el número de posibles vulnerabilidades a través de las cuales se podrían comprometer los datos personales. A diferencia de la mayoría de los dispositivos basados en la IO, los vehículos conectados son sistemas críticos en los que un fallo de seguridad puede poner en peligro la vida de sus usuarios y de las personas de su entorno. Por lo tanto, se acentúa la importancia de abordar el riesgo de que los piratas informáticos intenten explotar las vulnerabilidades de los vehículos conectados.

60. Además, los datos personales almacenados en vehículos o en ubicaciones externas (por ejemplo, en infraestructuras de computación en la nube) deben estar adecuadamente protegidos contra el acceso no autorizado. Por ejemplo, durante el mantenimiento, hay que entregar un vehículo a un técnico que necesitará acceder a algunos datos técnicos del vehículo. El técnico debe tener acceso a los datos técnicos, pero existe la posibilidad de que intente acceder a todos los datos almacenados en el vehículo.

2 RECOMENDACIONES GENERALES

61. Con el fin de mitigar los riesgos para los interesados mencionados anteriormente, los fabricantes de vehículos y equipos, los proveedores de servicios o cualquier otra parte interesada que pueda actuar como responsable o encargado del tratamiento de datos en relación con los vehículos conectados deben seguir las siguientes recomendaciones generales.

2.1 Categorías de datos

62. Como se ha señalado en la introducción, la mayoría de los datos asociados a los vehículos conectados se considerarán datos personales en la medida en que sea posible vincularlos a una o varias personas identificables. Esto incluye los datos técnicos relativos a los desplazamientos del vehículo (por ejemplo, velocidad, distancia recorrida), así como los relativos al estado del vehículo (por ejemplo, temperatura del refrigerante del motor, revoluciones por minuto del motor, presión de los neumáticos). Ciertos datos generados por los vehículos conectados también pueden justificar una atención especial dada su sensibilidad o su posible impacto en los derechos e intereses de los interesados. En la actualidad, el CEPD ha establecido tres categorías de datos personales que merecen especial

atención por parte de los fabricantes de vehículos y equipos, los proveedores de servicios y otros responsables del tratamiento de datos: los datos de localización, los datos biométricos (y cualquier categoría especial de datos definida en el artículo 9 del RGPD) y los datos que puedan revelar delitos o infracciones de tráfico.

2.1.1 Datos de localización

63. Al recopilar datos personales, los fabricantes de vehículos y equipos, los proveedores de servicios y otros responsables del tratamiento de datos deben tener en cuenta que los datos de localización son especialmente reveladores de los hábitos de vida de los interesados. Los desplazamientos realizados son muy característicos, ya que permiten deducir el lugar de trabajo y de residencia, así como los centros de interés (ocio) del conductor, y posiblemente revelen información sensible como la religión a través del lugar de culto, o la orientación sexual a través de los lugares visitados. En consecuencia, el fabricante de vehículos y equipos, el proveedor de servicios y otros responsables del tratamiento de datos deben prestar especial atención a no recopilar datos de localización, excepto si es absolutamente necesario para la finalidad del tratamiento. Por ejemplo, cuando el tratamiento consiste en detectar el movimiento del vehículo, el giroscopio es suficiente para cumplir esa función, sin que sea necesario recoger datos de localización.

64. En general, la recogida de datos de localización también está sujeta al cumplimiento de los siguientes principios:

- una configuración adecuada de la frecuencia de acceso y del nivel de detalle de los datos de localización recogidos en relación con la finalidad del tratamiento. Por ejemplo, una aplicación meteorológica no debería poder acceder a la ubicación del vehículo cada segundo, ni siquiera con el consentimiento del interesado;

- proporcionar información precisa sobre la finalidad del tratamiento (por ejemplo, ¿se almacena el historial de localización? Si es así, ¿cuál es su finalidad?);

- cuando el tratamiento se basa en el consentimiento, la obtención de un consentimiento válido (libre, específico e informado) distinto de las condiciones generales de venta o uso, por ejemplo sobre el ordenador a bordo;

- activar la localización solo cuando el usuario inicia una funcionalidad que requiere conocer la localización del vehículo, y no por defecto y de forma continua al arrancar el vehículo;

- informar al usuario de que se ha activado la localización, en particular mediante el uso de iconos (por ejemplo, una flecha que se mueve por la pantalla);

- la opción de desactivar la localización en cualquier momento;

- definir un periodo de almacenamiento limitado.

2.1.2 Datos biométricos

65. En el contexto de los vehículos conectados, los datos biométricos utilizados con el fin de identificar de forma única a una persona física pueden tratarse, en el ámbito del artículo 9 del RGPD y las excepciones nacionales, entre otras cosas, para permitir el acceso a un vehículo, para autenticar al conductor/propietario, o para permitir el acceso a los ajustes y preferencias del perfil del conductor. Al considerar el uso de datos biométricos, garantizar al interesado el pleno control sobre sus datos implica, por un lado, prever la existencia de una alternativa no biométrica (por ejemplo, mediante una clave física o un código) sin restricciones adicionales (es decir, el uso de la biometría no debe ser obligatorio), y, por otro lado, almacenar y comparar la plantilla biométrica de forma encriptada solo a nivel local, sin que los datos biométricos sean tratados por un terminal de lectura/comparación externo.

66. En el caso de los datos biométricos[37], es importante garantizar que la solución de autenticación biométrica sea suficientemente fiable, en particular mediante el cumplimiento de los siguientes principios:

- el ajuste de la solución biométrica utilizada (por ejemplo, la tasa de falsos positivos y falsos negativos) se adapta al nivel de seguridad del control de acceso requerido;
- la solución biométrica utilizada se basa en un sensor resistente a los ataques (como el uso de una huella plana para el reconocimiento de huellas dactilares);
- el número de intentos de autentificación es limitado;
- la plantilla / modelo biométrico se almacena en el vehículo, de forma encriptada mediante un algoritmo criptográfico y una gestión de claves que se ajustan al estado de la técnica;
- los datos brutos utilizados para componer la plantilla biométrica y para la autentificación del usuario se tratan en tiempo real sin que se almacenen nunca, ni siquiera localmente.

2.1.3 Datos que revelan infracciones penales o de otro tipo

67. Para el tratamiento de datos relacionados con posibles infracciones penales en el sentido del artículo 10 del RGPD, el CEPD recomienda recurrir al tratamiento local de los datos cuando el interesado tenga pleno control sobre el tratamiento en cuestión (véase el debate sobre el tratamiento local en la sección 2.4). En efecto, salvo algunas excepciones (véase el ejemplo sobre los estudios de accidentología que se presenta más adelante en la sección 3.3), el tratamiento externo de datos que revelen infracciones penales u otras infracciones está prohibido. Así, en función de la sensibilidad de los datos, se deben establecer fuertes medidas de seguridad como las descritas en el apartado 2.7 para ofrecer protección contra el acceso, la modificación y la supresión ilegítimos de dichos datos.

68. De hecho, algunas categorías de datos personales de los vehículos conectados podrían revelar que se ha cometido o se está cometiendo una infracción penal o de otro tipo («datos relacionados con infracciones») y, por lo tanto, estarían sujetos a restricciones especiales (por ejemplo, los datos que indican que el vehículo ha cruzado una línea blanca, la velocidad instantánea de un vehículo combinada con datos precisos de localización). En particular, en el caso de que estos datos sean tratados por las autoridades nacionales competentes con fines de investigación y enjuiciamiento de infracciones penales, se aplicarán las garantías previstas en el artículo 10 del RGPD.

2.2 Fines

69. Los datos personales se pueden tratar para una amplia variedad de fines en relación con los vehículos conectados, como la seguridad del conductor, los seguros, el transporte eficiente y los servicios de entretenimiento o información. De acuerdo con el RGPD, los responsables del tratamiento de datos deben garantizar que sus fines son «determinados, explícitos y legítimos», los datos no se tratan de manera incompatible con dichos fines y existe una base jurídica válida para el tratamiento, como se requiere en el artículo 5 del RGPD. En la parte III de las presentes Directrices se exponen algunos ejemplos concretos de los fines que pueden perseguir los responsables del tratamiento que operan en el contexto de los vehículos conectados, junto con recomendaciones específicas para cada tipo de tratamiento.

2.3 Pertinencia y minimización de datos

70. Para cumplir con el principio de minimización de datos[38], los fabricantes de vehículos y equipos, los proveedores de servicios y otros responsables del tratamiento deben prestar

[37] El principio de prohibición establecido en el artículo 9, apartado 1, del RGPD solo se refiere a los «datos biométricos dirigidos a identificar de manera unívoca a una persona física».
[38] Artículo 5, apartado 1, letra c), del RGPD.

especial atención a las categorías de datos que necesitan de un vehículo conectado, ya que solo recogerán los datos personales que sean pertinentes y necesarios para el tratamiento. Por ejemplo, los datos de localización son especialmente intrusivos y pueden revelar muchos hábitos de vida de los interesados. En consecuencia, los participantes del sector deben prestar especial atención a no recoger datos de localización, excepto si es absolutamente necesario para la finalidad del tratamiento (véanse las consideraciones sobre los datos de localización en el apartado 2.1).

2.4 Protección de datos desde el diseño y por defecto

71. Teniendo en cuenta el volumen y la diversidad de los datos personales producidos por los vehículos conectados, el CEPD señala que los responsables del tratamiento están obligados a garantizar que las tecnologías desplegadas en el contexto de los vehículos conectados estén configuradas para respetar la intimidad de las personas y, para ello, aplicarán las obligaciones de protección de datos desde el diseño y por defecto, como exige el artículo 25 del RGPD. Las tecnologías deben estar diseñadas para minimizar la recogida de datos personales, proporcionar configuraciones por defecto que protejan la intimidad y garantizar que los interesados estén bien informados y tengan la opción de modificar fácilmente las configuraciones asociadas a sus datos personales. Una orientación específica sobre cómo los fabricantes y proveedores de servicios pueden cumplir con la protección de datos desde el diseño y por defecto podría resultar beneficiosa para la industria y los proveedores de aplicaciones de terceros.

72. Ciertas prácticas generales, que se describen a continuación, también pueden ayudar a mitigar los riesgos para los derechos y libertades de las personas físicas en relación con los vehículos conectados[39].

2.4.1 Tratamiento local de datos personales

73. En general, los fabricantes de vehículos y equipos, los proveedores de servicios y otros responsables del tratamiento deben, siempre que sea posible, utilizar procesos que no impliquen datos personales o su transferencia fuera del vehículo (es decir, los datos se tratan internamente). Sin embargo, la naturaleza de los vehículos conectados presenta riesgos, como la posibilidad de sufrir ataques contra el tratamiento local por parte de actores externos o la filtración de datos locales al vender piezas del vehículo. Por lo tanto, deben tenerse en cuenta la atención y las medidas de seguridad adecuadas para garantizar que el tratamiento local siga siendo local. Este escenario ofrece la ventaja de garantizar al usuario el control único y total de sus datos personales y, como tal, presenta, «desde el diseño», menos riesgos de privacidad, especialmente al prohibir todo tratamiento de datos por las partes interesadas sin el conocimiento del interesado. También permite el tratamiento de datos sensibles, como los datos biométricos o los relativos a infracciones penales o de otro tipo, así como datos detallados de localización que, de otro modo, estarían sujetos a normas más estrictas (véase más adelante). En la misma línea, presenta menos riesgos de ciberseguridad e implica poca latencia, lo que lo hace especialmente adecuado para las funciones de asistencia a la conducción automatizada. Algunos ejemplos de este tipo de soluciones podrían ser:

- aplicaciones de conducción eficiente que tratan los datos del vehículo para mostrar consejos sobre este tipo de conducción en tiempo real en la pantalla de a bordo;
- aplicaciones que implican una transferencia de datos personales a un dispositivo como un teléfono inteligente bajo el control total del usuario (a través de, por ejemplo, Bluetooth o wifi), y en el que los datos del vehículo no se transmiten a los proveedores de la aplicación o a los fabricantes del vehículo; esto incluiría, por ejemplo, el acoplamiento de teléfonos

[39] Véanse también las Directrices 4/2019 del CEPD relativas al artículo 25 Protección de datos desde el diseño y por defecto, versión 2.0, adoptadas el 20 de octubre de 2020 (en lo sucesivo, las «Directrices 4/2019»).

inteligentes para utilizar la pantalla del coche, sistemas multimedia, micrófono (u otros sensores) para realizar llamadas telefónicas, etc., en la medida en que los datos recogidos permanezcan bajo el control del interesado y se utilicen exclusivamente para prestar el servicio que ha solicitado;

- aplicaciones que mejoran la seguridad en el vehículo, como las que emiten señales acústicas o vibraciones del volante cuando un conductor adelanta a un coche sin indicarlo o sobrepasa las líneas blancas, o las que emiten alertas sobre el estado del vehículo (por ejemplo, una alerta sobre el desgaste que afecta a las zapatas de freno);

- aplicaciones para el desbloqueo, el arranque o la activación de determinados comandos del vehículo utilizando los datos biométricos del conductor que se almacenan en el vehículo (como los modelos de cara o de voz o los puntos característicos de las huellas dactilares).

74. Aplicaciones como las anteriores implican un tratamiento realizado para desempeñar actividades puramente personales por parte de una persona física (es decir, sin transferencia de datos personales a un responsable o encargado del tratamiento). Por lo tanto, de acuerdo con el artículo 2, apartado 2, del RGPD, **estas aplicaciones quedan fuera del ámbito de aplicación del RGPD.**

75. No obstante, si el RGPD no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica, sí se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas (fabricantes de automóviles, proveedores de servicios, etc.) de conformidad con el considerando 18 del RGPD. Por lo tanto, cuando actúan como responsables o encargados del tratamiento de datos, deben desarrollar aplicaciones integradas en el vehículo seguras y con el debido respeto al principio de protección de la intimidad desde el diseño y por defecto. En cualquier caso, con arreglo al considerando 78 del RGPD, «[a]l desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollen y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos»[40]. Por un lado, mejorará el desarrollo de servicios centrados en el usuario y, por otro, facilitará y asegurará cualquier otro uso en el futuro que pueda entrar en el ámbito del RGPD. Más concretamente, la CEPD recomienda desarrollar una plataforma de aplicaciones integradas en el vehículo segura, separada físicamente de las funciones relevantes para la seguridad del vehículo, de modo que el acceso a los datos de este no dependa de capacidades externas innecesarias en la nube.

76. Los fabricantes de automóviles y los proveedores de servicios deberían considerar el tratamiento local de datos, siempre que sea posible, para mitigar los riesgos potenciales del tratamiento en la nube, como se subraya en el Dictamen 05/2012 sobre la computación en nube publicado por el Grupo de Trabajo del Artículo 29[41].

77. En general, los usuarios deben poder controlar cómo se recogen y tratan sus datos en el vehículo:

[40] Para más recomendaciones sobre la protección de la intimidad desde el diseño y por defecto, véanse también las Directrices 4/2019.
[41] Dictamen 05/2012 sobre la computación en nube del Grupo de Trabajo del Artículo 29; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf.

- la información relativa al tratamiento debe proporcionarse en el idioma del conductor (manual, ajustes, etc.);
- el CEPD recomienda que solo se traten por defecto los datos estrictamente necesarios para el funcionamiento del vehículo. Los interesados deben tener la posibilidad de activar o desactivar el tratamiento de datos para cada uno de los otros fines y responsables/encargados del tratamiento y tener la posibilidad de suprimir los datos en cuestión, teniendo en cuenta la finalidad y la base jurídica del tratamiento;
- los datos no deben transmitirse a terceros (es decir, el usuario es el único que tiene acceso a los datos);
- los datos deben conservarse solo durante el tiempo necesario para la prestación del servicio o mientras lo exija el Derecho de la Unión o de los Estados miembros;
- los interesados deben poder suprimir definitivamente los datos personales antes de que los vehículos se pongan a la venta;
- los interesados deben tener, siempre que sea posible, acceso directo a los datos generados por estas aplicaciones.

78. Por último, aunque no siempre sea posible recurrir al tratamiento local de los datos para todos los casos de uso, a menudo puede establecerse un «tratamiento híbrido». Por ejemplo, en el contexto de los seguros basados en el uso, los datos personales relativos al comportamiento de la conducción (como la fuerza ejercida sobre el pedal del freno, el kilometraje recorrido, etc.) podrían tratarse dentro del vehículo o por el proveedor de servicios telemáticos en nombre de la compañía de seguros (el responsable del tratamiento) para generar puntuaciones numéricas que se transfieren a la compañía de seguros con una regularidad definida (por ejemplo, mensualmente). De este modo, la compañía de seguros no tiene acceso a los datos de comportamiento en bruto, sino solo a la puntuación agregada que es el resultado del tratamiento. Esto garantiza que los principios de minimización de datos se satisfacen desde el diseño. Esto también significa que los usuarios deben tener la posibilidad de ejercer su derecho cuando otras partes conservan los datos: por ejemplo, un usuario debe tener la posibilidad de suprimir los datos almacenados en los sistemas de un taller de mantenimiento de automóviles o de un concesionario en las condiciones del artículo 17 del RGPD.

2.4.2 Anonimización y seudonimización

79. Si se prevé la transmisión de datos personales fuera del vehículo, debe considerarse la posibilidad de anonimizarlos antes de su transmisión. A la hora de anonimizar, el responsable del tratamiento debe tener en cuenta todos los tratamientos implicados que puedan dar lugar a la reidentificación de los datos, como la transmisión de datos anonimizados a nivel local. El CEPD recuerda que los principios de protección de datos no se aplican a la información anónima, es decir, información que no guarda relación con una persona física identificada o identificable o datos convertidos en anónimos de forma que el interesado no sea identificable o deje de serlo[42]. Una vez que un conjunto de datos está verdaderamente anonimizado y las personas dejan de ser identificables, la legislación europea de protección de datos ya no resulta de aplicación. En consecuencia, la anonimización, cuando sea pertinente, puede representar una buena estrategia para mantener los beneficios y mitigar los riesgos en relación con los vehículos conectados.

[42] Véanse el artículo 4, apartado 1, y el considerando 26 del RGPD.

80. Como se detalla en el Dictamen del Grupo de Trabajo del Artículo 29 sobre técnicas de anonimización, se pueden utilizar varios métodos —a veces combinados— para lograr la anonimización de los datos[43].

81. Otras técnicas como la seudonimización[44] pueden ayudar a minimizar los riesgos generados por el tratamiento de datos, teniendo en cuenta que en la mayoría de los casos, los datos directamente identificables no son necesarios para lograr la finalidad del tratamiento. La seudonimización, si se refuerza con garantías de seguridad, mejora la protección de los datos personales al reducir los riesgos de uso indebido. La seudonimización es reversible, a diferencia de la anonimización, y los datos seudonimizados se consideran datos personales sujetos al RGPD.

2.4.3 Evaluaciones de impacto relativas a la protección de los datos

82. Dada la magnitud y la sensibilidad de los datos personales que pueden generarse a través de los vehículos conectados; es probable que el tratamiento —sobre todo en situaciones en las que los datos personales se tratan fuera del vehículo— dé lugar con frecuencia a un alto riesgo para los derechos y libertades de las personas. Cuando este sea el caso, los participantes del sector deberán realizar una evaluación de impacto relativa a la protección de datos (EIPD) para detectar y mitigar los riesgos, tal como se detalla en los artículos 35 y 36 del RGPD. Incluso en los casos en los que no se requiere una EIPD, es recomendable realizarla lo antes posible en el proceso de diseño. De este modo, los participantes de la industria podrán tener en cuenta los resultados de este análisis en sus opciones de diseño antes de poner en marcha nuevas tecnologías.

2.5 Información

83. Antes del tratamiento de los datos personales, se informará al interesado de la identidad del responsable del tratamiento (por ejemplo, el fabricante de vehículos y equipos o el proveedor de servicios), de la finalidad del tratamiento, de los destinatarios de los datos, del período durante el cual se conservarán los datos y de los derechos del interesado en virtud del RGPD[45].

84. Además, el fabricante de vehículos y equipos, el proveedor de servicios o cualquier otro responsable del tratamiento de datos también debe proporcionar al interesado la siguiente información, en un lenguaje claro, sencillo y de fácil acceso:

- los datos de contacto del delegado de protección de datos;
- los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
- la mención explícita de los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, cuando dichos intereses legítimos constituyan la base jurídica del tratamiento;
- los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

[43] Dictamen 05/2014 sobre técnicas de anonimización (WP29); https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf.
[44] Véase el artículo 4, apartado 5, del RGPD. Informe Enisa de 3 de diciembre de 2019: https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices.
[45] Véanse el artículo 5, apartado 1, letra a), y el artículo 13 del RGPD. Véase también Grupo de Trabajo del Artículo 29, Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 (wp260rev.01), refrendadas por el CEPD.

- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
- la existencia del derecho a retirar el consentimiento en cualquier momento sin que ello afecte a la legalidad del tratamiento basado en el consentimiento antes de su retirada, cuando el tratamiento se base en el consentimiento;
- en su caso, el hecho de que el responsable del tratamiento tiene previsto transferir datos personales a un tercer país u organización internacional y las garantías utilizadas para su transferencia;
- si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;
- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, que produzcan efectos jurídicos para el interesado o le afecten significativamente, y la información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. Este podría ser el caso, en particular, en relación con la provisión de seguros basados en el uso a los individuos;
- el derecho a presentar una reclamación ante una autoridad de control;
- información sobre el tratamiento ulterior;
- en situaciones de corresponsabilidad del tratamiento, información clara y completa sobre las responsabilidades de cada responsable del tratamiento de datos.

85. En algunos casos, los datos personales no se recogen directamente de la persona afectada. Por ejemplo, un fabricante de vehículos y equipos puede recurrir a un concesionario para recoger información sobre el propietario del vehículo con el fin de ofrecer un servicio de asistencia de emergencia en carretera. Cuando los datos no se hayan recogido directamente, el fabricante de vehículos y equipos, el proveedor de servicios u otro responsable del tratamiento de datos deberá indicar también, además de la información mencionada anteriormente, las categorías de datos personales de que se trate, la fuente de la que proceden dichos datos y, en su caso, si proceden de fuentes de acceso público. El responsable del tratamiento debe proporcionar dicha información en un plazo razonable tras la obtención de los datos, y **a más tardar en la primera de las siguientes fechas**, de conformidad con el artículo 14, apartado 3, del RGPD: i) un mes después de la obtención de los datos, habida cuenta de las circunstancias específicas en las que se traten dichos datos, ii) en el momento de la primera comunicación con el interesado, o iii) si esos datos se transmiten a un tercero, antes de la transmisión de los datos.

86. También podría ser necesario facilitar nueva información a los interesados cuando sean atendidos por un nuevo responsable del tratamiento. Diferentes responsables del tratamiento pueden prestar un servicio de asistencia en carretera que interactúa con los vehículos conectados en función del país o la región donde se requiera la asistencia. Los nuevos responsables del tratamiento de datos deben proporcionar a los interesados la información necesaria cuando estos cruzan las fronteras y los servicios que interactúan con los vehículos conectados son proporcionados por los nuevos responsables del tratamiento de datos.

87. La información dirigida a los interesados puede proporcionarse en niveles[46], es decir, separando dos niveles de información: por un lado, la información de primer nivel, que es la más importante para los interesados, y, por otro, la información que presumiblemente será de interés en una fase posterior. La información esencial de primer nivel incluye, además de la identidad del responsable del tratamiento, la finalidad del mismo y una descripción de los derechos del interesado, así como cualquier información adicional sobre el tratamiento que tenga mayor repercusión en el interesado y el tratamiento que pueda sorprenderle. El CEPD recomienda que, en el contexto de los vehículos conectados, el interesado tenga conocimiento de todos los destinatarios en el primer nivel de información. Como se indica en las Directrices del Grupo de Trabajo del Artículo 29 sobre transparencia, los responsables deben facilitar la información sobre los destinatarios que sea más significativa para los interesados. En la práctica, esta será habitualmente los destinatarios nombrados, con vistas a que los interesados sepan exactamente quién dispone de sus datos personales. Si los responsables no pueden facilitar los nombres de los destinatarios, la información debe ser tan específica como sea posible, indicando el tipo de destinatario (es decir, en referencia a las actividades que este ejerce), la industria, el sector y el subsector y la ubicación de los destinatarios.

88. Los interesados podrán ser informados mediante cláusulas concisas y fácilmente comprensibles en el contrato de compraventa del vehículo, en el contrato de prestación de servicios, o en cualquier soporte escrito, mediante el uso de distintos documentos (por ejemplo, el libro o manual de mantenimiento del vehículo) o el ordenador de a bordo.

89. Podrían utilizarse iconos normalizados además de la información necesaria, como se exige en los artículos 13 y 14 del RGPD, para mejorar la transparencia al reducir potencialmente la necesidad de presentar grandes cantidades de información escrita al interesado. Debe ser visible en los vehículos para proporcionar, en relación con el tratamiento previsto, una buena visión general que sea comprensible y claramente legible. El CEPD subraya la importancia de normalizar esos iconos para que el usuario encuentre los mismos símbolos independientemente de la marca o el modelo del vehículo. Por ejemplo, cuando se recogen ciertos tipos de datos, como los de localización, los vehículos podrían tener una señal clara a bordo (como una luz dentro del vehículo) para informar a los pasajeros sobre la recogida de datos.

2.6 Derechos del interesado

90. Los fabricantes de vehículos y equipos, los proveedores de servicios y otros responsables del tratamiento deben facilitar a los interesados el control de sus datos durante todo el período de tratamiento, mediante la implementación de herramientas específicas que les ofrezcan una forma eficaz de ejercer sus derechos, en particular su derecho de acceso, rectificación, supresión, su derecho a restringir el tratamiento y, en función de la base jurídica del tratamiento, su derecho a la portabilidad de los datos y su derecho de oposición.

91. Para facilitar la modificación de los ajustes, debe implantarse un sistema de gestión de perfiles para almacenar las preferencias de los conductores conocidos y ayudarles a cambiar fácilmente sus ajustes de privacidad en cualquier momento. El sistema de gestión de perfiles debe centralizar todos los ajustes de datos para cada tratamiento de datos, especialmente para facilitar el acceso, la supresión, la eliminación y la portabilidad de los datos personales de los sistemas del vehículo a petición del interesado. Los responsables del tratamiento deben poder detener la recogida de determinados tipos de datos, temporal o permanentemente, en cualquier momento, a menos que exista un fundamento jurídico específico en el que pueda basarse el responsable del tratamiento para continuar con la recogida de datos específicos. En el caso de un contrato que proporcione una oferta

[46] Véase Grupo de Trabajo del Artículo 29, Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679 (wp260rev.01), refrendadas por el CEPD.

personalizada basada en el comportamiento de conducción, esto puede implicar que las condiciones del usuario se reviertan a las condiciones estándar de ese contrato. Estas funciones deben implantarse en el interior del vehículo, aunque también podrían proporcionarse a los interesados a través de medios adicionales (por ejemplo, una aplicación específica). Además, para permitir que los interesados eliminen de manera rápida y fácil los datos personales que puedan almacenarse en el salpicadero del coche (por ejemplo, el historial de navegación del GPS, la navegación por Internet, etc.), el CEPD recomienda que los fabricantes ofrezcan una funcionalidad sencilla (como un botón de borrado).

92. La venta de un vehículo conectado y el consiguiente cambio de titularidad también deben dar lugar a la supresión de cualquier dato personal que ya no sea necesario para los fines especificados anteriormente y el interesado debería poder ejercer su derecho a la portabilidad.

2.7 Seguridad

93. Los fabricantes de vehículos y equipos, los proveedores de servicios y otros responsables del tratamiento de datos deben establecer medidas que garanticen la seguridad y la confidencialidad de los datos tratados y tomar todas las precauciones útiles para evitar que una persona no autorizada se haga con el control de dichos datos. En particular, los participantes de la industria deben considerar la adopción de las siguientes medidas:

- cifrar los canales de comunicación mediante un algoritmo de última generación;
- poner en marcha un sistema de gestión de claves de cifrado que sea único para cada vehículo, no para cada modelo;
- cuando se conservan los datos a distancia, cifrarlos mediante algoritmos de última generación;
- renovar regularmente las claves de cifrado;
- proteger las claves de cifrado de cualquier divulgación;
- autenticar los dispositivos de recepción de datos;
- garantizar la integridad de los datos (por ejemplo, mediante direccionamiento calculado);
- someter el acceso a los datos personales a técnicas fiables de autenticación de los usuarios (contraseña, certificado electrónico, etc.);

94. En lo que respecta más específicamente a los fabricantes de vehículos, el CEPD recomienda la aplicación de las siguientes medidas de seguridad:

- separar las funciones vitales del vehículo de las que dependen siempre de las capacidades de telecomunicación (por ejemplo, el «infotenimiento»);
- aplicar medidas técnicas que permitan a los fabricantes de vehículos solventar rápidamente las vulnerabilidades de seguridad durante toda la vida útil del vehículo;
- para las funciones vitales del vehículo, dar prioridad, en la medida de lo posible, a la utilización de medios de comunicación seguros y específicamente dedicados al transporte;
- establecer un sistema de alarma en caso de ataque a los sistemas del vehículo, con la posibilidad de funcionar en modo degradado[47];

[47] El modo degradado es un modo de funcionamiento del vehículo que asegura que las funciones esenciales para el funcionamiento seguro del vehículo (es decir, los requisitos mínimos de seguridad) estarían garantizadas, aunque otras funcionalidades menos importantes estarían desactivadas (por ejemplo, el funcionamiento del dispositivo de geo-guiado puede considerarse como no esencial, a diferencia del sistema de frenado).

- almacenar un historial de registro de cualquier acceso al sistema de información del vehículo, por ejemplo, remontándose a seis meses como período máximo, para poder entender el origen de cualquier posible ataque y realizar periódicamente una revisión de la información registrada para detectar posibles anomalías.

95. Estas recomendaciones generales deben completarse con requisitos específicos que tengan en cuenta las características y la finalidad de cada tratamiento de datos.

2.8 Transmisión de datos personales a terceras partes

96. En principio, solo el responsable del tratamiento y el interesado tienen acceso a los datos generados por un vehículo conectado. No obstante, el responsable del tratamiento puede transmitir datos personales a un socio comercial (destinatario), en la medida en que dicha transmisión se haga con arreglo a una de las bases jurídicas indicadas en el artículo 6 del RGPD.

97. Habida cuenta de la posible sensibilidad de los datos sobre el uso del vehículo (por ejemplo, los trayectos realizados, el estilo de conducción), el CEPD recomienda que se obtenga sistemáticamente el consentimiento del interesado antes de transmitir sus datos a un socio comercial que actúe como responsable del tratamiento (por ejemplo, marcando una casilla que no esté previamente marcada o, cuando sea técnicamente posible, utilizando un dispositivo físico o lógico al que la persona pueda acceder desde el vehículo). El socio comercial, a su vez, se convierte en responsable de los datos que recibe y está sujeto a todas las disposiciones del RGPD.

98. El fabricante de vehículos, el proveedor de servicios u otro responsable del tratamiento de datos puede transmitir los datos personales a un encargado del tratamiento seleccionado para participar en la prestación del servicio al interesado, siempre que el encargado del tratamiento no utilice esos datos para sus propios fines. Los responsables y los encargados del tratamiento redactarán un contrato u otro documento legal en el que se especifiquen las obligaciones de cada parte y se establezcan las disposiciones del artículo 28 del RGPD.

2.9 Transferencia de datos personales fuera de la UE / el EEE

99. Cuando los datos personales se transfieren fuera del Espacio Económico Europeo, están previstas garantías especiales para asegurar que la protección acompaña los datos.

100. En consecuencia, el responsable del tratamiento solo podrá transferir datos personales a un destinatario en la medida en que dicha transferencia se ajuste a los requisitos establecidos en el capítulo V del RGPD.

2.10 Uso de tecnologías wifi en el vehículo

101. Los avances en la tecnología móvil han hecho posible utilizar fácilmente Internet en la carretera. Aunque es posible obtener conectividad wifi en un vehículo a través de un punto de acceso de un teléfono inteligente o de un dispositivo especializado (mochila OBD-II, módem o router inalámbrico, etc.), la mayoría de los fabricantes ofrecen hoy en día modelos que incluyen una conexión de datos móvil integrada y que también son capaces de crear redes inalámbricas. Según el caso, hay que tener en cuenta varios aspectos:

- la conectividad wifi se ofrece como servicio por un profesional de la carretera, como un taxista a sus clientes. En este caso, el profesional o su empresa puede ser considerado como un proveedor de servicios de Internet (PSI), por lo que estará sujeto a obligaciones y restricciones específicas en relación con el tratamiento de los datos personales de sus clientes;

- la conectividad wifi se facilita para el uso exclusivo del conductor (con exclusión del conductor y sus pasajeros). En este caso, el tratamiento de los datos personales se considera una actividad exclusivamente personal o doméstica de acuerdo con el artículo 2, apartado 2, letra c) y el considerando 18 del RGPD.

102. En general, la proliferación de interfaces de conexión a Internet a través de wifi plantea mayores riesgos para la vida privada de las personas. De hecho, a través de sus vehículos, los usuarios se convierten en emisores continuos, y por tanto se les puede identificar y rastrear. Para evitar el rastreo, los fabricantes de vehículos y de equipos deben establecer opciones de exclusión fáciles de utilizar que garanticen que no se recoge el identificador del conjunto de servicios (SSID) de la red wifi a bordo.

3 ESTUDIOS DE CASOS

103. En esta sección se abordan cinco ejemplos concretos de tratamiento en el contexto de los vehículos conectados, que corresponden a escenarios que probablemente encontrarán las partes interesadas en el sector. Los ejemplos abarcan el tratamiento de datos que requiere una potencia de cálculo que no puede movilizarse localmente en el vehículo, o el envío de datos personales a un tercero para llevar a cabo un análisis más profundo o para proporcionar una funcionalidad adicional a distancia. Para cada tipo de tratamiento, este documento especifica la finalidad prevista, las categorías de datos recogidos, el periodo de conservación de dichos datos, los derechos de los interesados, las medidas de seguridad que se aplicarán y los destinatarios de la información. En el caso de que algunos de estos campos no se describan a continuación, se aplican las recomendaciones generales descritas en la parte anterior.

104. Los ejemplos elegidos no son exhaustivos y pretenden ser indicativos de la variedad de tipos de tratamiento, bases jurídicas, actores, etc. que podrían participar en el contexto de los vehículos conectados.

3.1 Prestación de un servicio por parte de un tercero

105. Los interesados pueden contratar con un proveedor de servicios para obtener servicios de valor añadido relacionados con su vehículo. Por ejemplo, un interesado puede suscribir un contrato de seguro basado en el uso que ofrece primas de seguro reducidas por conducir menos («Pay As You Drive») o por buen comportamiento al volante («Pay How You Drive») y que requiere un seguimiento de los hábitos de conducción por parte de la compañía de seguros. El interesado también podría contratar con una empresa que ofrezca asistencia en carretera en caso de avería y que implique la transmisión de la ubicación del vehículo a la empresa o a un proveedor de servicios para recibir mensajes o alertas relacionados con el

funcionamiento del vehículo (por ejemplo, una alerta sobre el estado de desgaste de los frenos o un recordatorio de la fecha de la inspección técnica).

3.1.1 Seguros basados en el uso

106. «Pay as you drive» es un tipo de seguro basado en el uso que hace un seguimiento del kilometraje o de los hábitos de conducción para diferenciar y recompensar a los conductores «seguros» ofreciéndoles primas más bajas. La aseguradora exigirá al conductor que instale un servicio de telemática integrado, una aplicación móvil o que active un módulo integrado de fabricación que haga un seguimiento de los kilómetros recorridos o del comportamiento de conducción (patrón de frenado, aceleración rápida, etc.) del asegurado. La información recogida por el dispositivo de telemática se utilizará para asignar una puntuación al conductor con el fin de analizar los riesgos que puede suponer para la compañía de seguros.

107. Dado que los seguros basados en el uso requieren el consentimiento en virtud del artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas, el CEPD señala que el tomador del seguro debe tener la opción de suscribir una póliza de seguro no basada en el uso. De lo contrario, no se consideraría que el consentimiento se ha dado libremente, ya que la ejecución del contrato estaría condicionada al consentimiento. Además, el artículo 7, apartado 3, del RGPD exige que el interesado tenga derecho a retirar su consentimiento.

3.1.1.1 Base jurídica

108. Cuando los datos se recojan a través de un servicio de comunicación electrónica disponible al público (por ejemplo, a través de la tarjeta SIM contenida en el dispositivo telemático), será necesario el consentimiento para poder acceder a la información que ya está almacenada en el vehículo, tal como establece el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas. De hecho, ninguna de las exenciones previstas en esas disposiciones puede aplicarse en este contexto: el tratamiento no tiene como única finalidad realizar la transmisión de una comunicación a través de una red de comunicaciones electrónicas ni está relacionado con un servicio de la sociedad de la información explícitamente solicitado por el abonado o usuario. El consentimiento podría obtenerse en el momento de la celebración del contrato.

109. En cuanto al tratamiento de datos personales tras el almacenamiento o el acceso al equipo terminal del usuario final, la compañía de seguros puede basarse en el artículo 6, apartado 1, letra b), del RGPD en este contexto específico, siempre que pueda demostrar que el tratamiento tiene lugar en el contexto de un contrato válido con el interesado y que el tratamiento es necesario para que pueda ejecutarse dicho contrato. En la medida en que el tratamiento es objetivamente necesario para la ejecución del contrato con el interesado, el CEPD considera que recurrir al artículo 6, apartado 1, letra b), del RGPD no tendría el efecto de reducir la protección específica proporcionada por el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas en este caso concreto. Esta base jurídica se materializa en la firma de un contrato por parte del interesado con la compañía de seguros.

3.1.1.2 Datos recopilados

110. Hay que tener en cuenta dos tipos de datos personales:

- **datos comerciales y de transacciones**: datos de identificación del interesado, datos relacionados con transacciones, datos relativos a los medios de pago, etc.;
- **datos de uso**: datos personales generados por el vehículo, hábitos de conducción, ubicación, etc.

111. El CEPD recomienda que se traten los datos brutos relativos al comportamiento del conductor, en la medida de lo posible, y dado que existe el riesgo de que los datos recogidos

a través de la caja telemática puedan utilizarse indebidamente para crear un perfil preciso de los movimientos del conductor:

- dentro del vehículo en cajas telemáticas o en el teléfono inteligente del usuario para que la aseguradora solo acceda a los datos de los resultados (por ejemplo, una puntuación relativa a los hábitos de conducción), no a los datos brutos detallados (véase el apartado 2.1);

- o por el proveedor de servicios telemáticos en nombre del responsable del tratamiento (la compañía de seguros) para generar puntuaciones numéricas que se transfieren a dicha compañía sobre una base definida. En este caso, hay que separar los datos brutos de los datos directamente relacionados con la identidad del conductor. Esto significa que el proveedor de servicios telemáticos recibe los datos en tiempo real, pero no conoce los nombres, las matrículas, etc., de los asegurados. Por otro lado, la aseguradora conoce los nombres de los asegurados, pero solo recibe las puntuaciones y los kilómetros totales y no los datos brutos utilizados para elaborar dichas puntuaciones.

112. Además, hay que tener en cuenta que si solo es necesario el kilometraje para la ejecución del contrato, no se recogerán los datos de localización.

3.1.1.3 Periodo de conservación

113. En el contexto del tratamiento de datos que tiene lugar para la ejecución de un contrato (es decir, la prestación de un servicio), es importante distinguir entre dos tipos de datos antes de definir sus respectivos períodos de conservación:

- **datos comerciales y de transacciones:** esos datos pueden conservarse en una base de datos activa durante toda la duración del contrato. Al final del contrato, pueden archivarse en formato físico (en un soporte aparte: DVD, etc.) o en formato electrónico (mediante la gestión de autorizaciones) en caso de posibles litigios. Posteriormente, una vez transcurridos los plazos de prescripción, los datos se eliminarán o anonimizarán;

- **datos de uso:** los datos de uso pueden clasificarse como datos brutos y datos agregados. Como ya se ha dicho, en la medida de lo posible, los responsables o encargados del tratamiento no deben tratar los datos en bruto. Si es necesario, los datos brutos deben conservarse solo el tiempo necesario para elaborar los datos agregados y para comprobar la validez de ese proceso de agregación. Los datos agregados deben conservarse mientras sean necesarios para la prestación del servicio o sean requeridos por el Derecho de la Unión o de los Estados miembros.

3.1.1.4 Información y derechos de los interesados

114. Antes del tratamiento de los datos personales, se informará al interesado de acuerdo con el artículo 13 del RGPD, de forma transparente y comprensible. En particular, se le debe informar del período durante el cual se almacenarán los datos personales o, si no es posible, de los criterios utilizados para determinar dicho período. En este último caso, el CEPD recomienda adoptar un enfoque pedagógico para subrayar la diferencia entre los datos brutos y la puntuación obtenida sobre esta base, subrayando, cuando sea el caso, que la aseguradora solo recogerá el resultado de la puntuación cuando proceda.

115. Cuando los datos no son tratados dentro del vehículo, sino por un proveedor de telemática en nombre del responsable del tratamiento (la compañía de seguros), la información podría mencionar de manera útil que, en este caso, el proveedor no tendrá acceso a los datos directamente relacionados con la identidad del conductor (como nombres, matrículas, etc.). Asimismo, habida cuenta de la importancia de informar a los interesados sobre las consecuencias del tratamiento de sus datos personales y del hecho de que el tratamiento no debe coger por sorpresa a los interesados, el CEPD recomienda que se informe a los interesados de la existencia de la elaboración de perfiles y de las consecuencias de dicha

elaboración, aunque no implique las decisiones automatizadas a las que se refiere el artículo 22 del RGPD.

116. En cuanto al derecho de los interesados, se les informará específicamente de los medios disponibles para ejercer su derecho de acceso, rectificación, limitación y supresión. Dado que los datos brutos recogidos en este contexto son facilitados por el interesado (a través de formularios específicos o a través de su actividad) y se tratan sobre la base del artículo 6, apartado 1, letra b), del RGPD (ejecución de un contrato), el interesado está facultado para ejercer su derecho a la portabilidad de los datos. Como se destaca en las Directrices sobre el derecho a la portabilidad de los datos, el CEPD recomienda, en especial, «que los responsables del tratamiento expliquen con claridad la diferencia entre los tipos de datos que un interesado puede recibir en virtud del derecho de acceso o del derecho a la portabilidad de los datos»[48].

117. La información puede facilitarse en el momento de la firma del contrato.

3.1.1.5 Beneficiario:

118. El CEPD recomienda que, en la medida de lo posible, los datos de uso del vehículo se traten directamente en las cajas telemáticas, de modo que la aseguradora solo acceda a los datos de los resultados (por ejemplo, una puntuación), no a los datos brutos detallados.

119. Si un proveedor de servicios telemáticos recoge los datos por cuenta del responsable del tratamiento (la compañía de seguros) para generar puntuaciones numéricas, no necesita conocer la identidad del conductor (como nombres, matrículas, etc.) de los tomadores del seguro.

3.1.1.6 Seguridad:

120. Se aplican las recomendaciones generales. Véase el punto 2.7.

3.1.2 Arrendamiento y reserva de una plaza de estacionamiento

121. El propietario de una plaza de estacionamiento puede querer arrendarla. Para ello, inscribe dicha plaza en una aplicación web y fija un precio. A continuación, una vez que la plaza de estacionamiento está publicada en la lista, la aplicación avisa al propietario cuando un conductor quiere reservarla. El conductor puede seleccionar un destino y ver qué plazas de estacionamiento hay disponibles en función de múltiples criterios. Tras la aprobación por parte del propietario, se confirma la transacción y el proveedor de servicios se encarga de la operación de pago y, a continuación, utiliza la navegación para conducir hasta el lugar.

3.1.2.1 Base jurídica

122. Cuando los datos se recogen a través de una comunicación electrónica disponible al público, se aplica el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

123. Al tratarse de un servicio de la sociedad de la información, dicho artículo no exige el consentimiento para acceder a la información que ya está almacenada en el vehículo cuando el abonado solicita explícitamente este servicio.

124. Para el tratamiento de los datos personales y solo para los datos necesarios para la ejecución del contrato en el que el interesado es parte, la base jurídica será el artículo 6, apartado 1, letra b), del RGPD.

3.1.2.2 Datos recopilados

125. Los datos tratados incluyen los datos de contacto del conductor (nombre, correo electrónico, número de teléfono, tipo de vehículo (por ejemplo, coche, camión,

[48] Grupo de Trabajo del Artículo 29, Directrices sobre el derecho a la portabilidad de los datos, WP242 rev.01, refrendadas por el CEPD, p. 15.

motocicleta), número de matrícula, período de estacionamiento, detalles de pago (por ejemplo, información de la tarjeta de crédito), así como los datos de navegación.

3.1.2.3 Periodo de conservación

126. Los datos deben conservarse solo mientras sean necesarios para cumplir el contrato de aparcamiento o, en su defecto, según lo dispuesto en el Derecho de la Unión o de los Estados miembros. Posteriormente, los datos se anonimizan o se suprimen.

3.1.2.4 Información y derechos de los interesados

127. Antes del tratamiento de los datos personales, se debe informar al interesado de acuerdo con el artículo 13 del RGPD, de forma transparente y comprensible.

128. Se debe informar a los interesados específicamente de los medios disponibles para ejercer su derecho de acceso, rectificación, limitación y supresión. Dado que los datos brutos recogidos en este contexto son facilitados por el interesado (a través de formularios específicos o a través de su actividad) y se tratan sobre la base del artículo 6, apartado 1, letra b), del RGPD (ejecución de un contrato), el interesado tiene derecho a ejercer su derecho a la portabilidad de los datos. Como se destaca en las Directrices sobre el derecho a la portabilidad de los datos, el CEPD recomienda, en especial, «que los responsables del tratamiento expliquen con claridad la diferencia entre los tipos de datos que un interesado puede recibir en virtud del derecho de acceso o del derecho a la portabilidad de los datos».

3.1.2.5 Beneficiario*:*

129. En principio, solo el responsable y el encargado del tratamiento tienen acceso a los datos.

3.1.2.6 Seguridad:

130. Se aplican las recomendaciones generales. Véase el punto 2.7.

3.2 Llamada de emergencia (eCall)

131. En caso de accidente grave en la Unión Europea, el vehículo activa automáticamente una eCall al 112, el número de emergencias de toda la UE (véase el apartado 1.1 para más detalles) que permite enviar rápidamente una ambulancia al lugar del accidente de acuerdo con el Reglamento (UE) 2015/758 del Parlamento Europeo y del Consejo, de 29 de abril de 2015, relativo a los requisitos de homologación de tipo para el despliegue del sistema eCall basado en el número 112 integrado en los vehículos y por el que se modifica la Directiva 2007/46/CE (en adelante, el «Reglamento (UE) 2015/758»).

132. En efecto, el generador de la eCall instalado en el interior del vehículo, que permite la transmisión a través de una red pública de comunicaciones móviles inalámbricas, inicia una llamada de emergencia, que es activada automáticamente por los sensores del vehículo o manualmente por sus ocupantes solo en caso de accidente. Además de la activación del canal de audio, el segundo evento que se activa automáticamente como consecuencia de un accidente consiste en generar el conjunto mínimo de datos (MSD) y enviarlo al punto de respuesta de seguridad pública (PSAP).

3.2.1 Base jurídica

133. En cuanto a la aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas, hay que tener en cuenta dos disposiciones:

- el artículo 9 relativo a los datos de localización distintos de los datos de tráfico, que solo se aplica a los servicios de comunicaciones electrónicas; y
- el artículo 5, apartado 3, para obtener acceso a la información almacenada en el generador instalado en el interior del vehículo.

134. A pesar de que, en principio, esas disposiciones exigen el consentimiento del interesado, el Reglamento (UE) 2015/758 constituye una obligación legal la que está sujeto el responsable

del tratamiento (el interesado no tiene verdadera o libre elección y no podrá negarse al tratamiento de sus datos). De ahí que el Reglamento (UE) 2015/758 anule la necesidad del consentimiento del conductor para el tratamiento de los datos de localización y del conjunto mínimo de datos[49].

135. La base jurídica del tratamiento de esos datos será el cumplimiento de una obligación legal según lo previsto en el artículo 6, apartado 1, letra c), del RGPD [es decir, el Reglamento (UE) 2015/758].

3.2.2 Datos recopilados

136. El Reglamento (UE) 2015/578 establece que los datos enviados por el sistema eCall basado en el 112 integrado en los vehículos incluirán únicamente la información mínima a la que se refiere la norma EN 15722:2015 «Sistemas inteligentes de transporte. eSafety. Conjunto mínimo de datos del servicio eCall.», como por ejemplo:

- la indicación de si eCall se ha activado manual o automáticamente;
- el tipo de vehículo;
- el número de identificación del vehículo (NIV);
- el tipo de propulsión del vehículo;
- la marca de tiempo de la generación del mensaje de datos inicial dentro del evento de incidente eCall actual;
- la última ubicación conocida de latitud y longitud del vehículo determinada en el último momento posible antes de la generación del mensaje;
- la última dirección real conocida del vehículo, determinada en el último momento posible antes de la generación del mensaje (solo las tres últimas localizaciones del vehículo).

3.2.3 Periodo de conservación

137. El Reglamento (UE) 2015/758 establece que los datos no se conservarán más tiempo del necesario para fines de respuesta a situaciones de emergencia. Dichos datos se suprimirán completamente cuando ya no sean necesarios para ese fin. Además, en la memoria interna del sistema eCall, los datos se suprimirán de forma automática y continuada. Solo se pueden conservar las tres últimas ubicaciones del vehículo, en la medida estrictamente necesaria para determinar la ubicación actual del vehículo y la dirección del viaje en el momento del acontecimiento.

3.2.4 Información y derechos de los interesados

138. El artículo 6 del Reglamento (UE) 2015/758 establece que los fabricantes deben proporcionar información clara y completa sobre el tratamiento de datos realizado mediante el sistema eCall. Esta información se proporcionará en el manual de instrucciones por separado para el sistema eCall basado en el 112 integrado en los vehículos y para cualquier sistema eCall de terceros que sea compatible con el servicio antes del uso del sistema. Esto incluye:

- la referencia a la base jurídica para el tratamiento;

[49] Cabe señalar que el artículo 8, apartado, letra f), del mandato de negociación del Consejo para la propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas establece una exención específica para eCall, ya que el consentimiento no es necesario cuando es necesario localizar el equipo terminal cuando un usuario final realiza una comunicación de emergencia, ya sea al número único europeo de emergencias «112» o a un número nacional de emergencias, de conformidad con el artículo 13, apartado 3.

- la activación por defecto del sistema eCall basado en el número 112 integrado en los vehículos;
- las disposiciones prácticas para el tratamiento de datos que lleva a cabo el sistema eCall basado en el número 112 integrado en los vehículos;
- la finalidad específica del tratamiento de eCall, que se limitará a las situaciones de emergencia a que se refiere el artículo 5, apartado 2, párrafo primero, del Reglamento (UE) 2015/758;
- los tipos de datos recogidos y tratados y los destinatarios de los mismos;
- el plazo máximo de retención de los datos en el sistema eCall basado en el número 112 integrado en los vehículos;
- el hecho de que el vehículo no es objeto de seguimiento permanente;
- las disposiciones prácticas para ejercer los derechos de los interesados a que se refieren los datos y el servicio de contacto responsable de tramitar las solicitudes de acceso;
- toda información adicional necesaria relativa a la trazabilidad, el seguimiento y el tratamiento de los datos personales en relación con la prestación de una eCall basada en servicios prestados por terceros (SPT) o de otros servicios con valor añadido, que estará sujeta al consentimiento expreso por parte del propietario y en cumplimiento del RGPD. Se tendrá especialmente en cuenta el hecho de que pueden existir diferencias entre el tratamiento de datos realizado a través del sistema eCall basado en el 112 y los sistemas eCall SPT integrados en los vehículos u otros servicios con valor añadido.

139. Además, el proveedor de servicios también proporcionará a los interesados información de conformidad con el artículo 13 del RGPD de forma transparente y comprensible. En particular, debe ser informado de los fines del tratamiento a los que se destinan los datos personales, así como del hecho de que el tratamiento de los datos personales se basa en una obligación legal a la que está sujeto el responsable del tratamiento.

140. Además, teniendo en cuenta la naturaleza del tratamiento, la información sobre los destinatarios o las categorías de destinatarios de los datos personales debe ser clara y los interesados deben ser informados de que ninguna entidad externa al sistema eCall basado en el número 112 integrado en el vehículo tendrá acceso a esos datos antes de que se active la eCall.

141. En cuanto a los derechos de los interesados, hay que señalar que, dado que el tratamiento se basa en una obligación legal, no se aplicarán el derecho de oposición ni el derecho a la portabilidad.

3.2.5 Beneficiario:

142. Ninguna entidad externa al sistema eCall basado en el número 112 integrado en los vehículos tendrá acceso a esos datos antes de que se active la eCall.

143. Cuando se activa (ya sea manualmente por los ocupantes del vehículo o automáticamente en cuanto un sensor del vehículo detecta una colisión grave), el sistema eCall establece una conexión de voz con el PSAP correspondiente y el MSD se envía al operador del PSAP.

144. Además, los datos transmitidos a través del sistema eCall basado en el número 112 integrado en los vehículos y tratados por los PSAP podrán transferirse únicamente al servicio de urgencia y a los prestadores de servicios asociados a que se refiere la Decisión no 585/2014/UE en caso de incidentes relacionados con las llamadas eCall y en las condiciones que establece dicha Decisión, y se utilizarán exclusivamente para cumplir con los objetivos de esta. Los datos tratados por los PSAP a través del sistema eCall basado en el número 112 integrado en los vehículos no se transferirán a ningún otro tercero sin el consentimiento expreso previo del interesado al que se refieran.

3.2.6 Seguridad

145. El Reglamento (UE) 2015/758 estipula los requisitos para incorporar al sistema eCall tecnologías que refuercen la protección de la intimidad, con el fin de ofrecer a los usuarios el nivel adecuado de protección de la intimidad, así como las salvaguardias necesarias para evitar la vigilancia y el mal uso. Además, los fabricantes deben garantizar que el sistema de eCall basado en el número 112, así como cualquier otro sistema que proporcione una eCall gestionada por servicios de terceros o un servicio con valor añadido, estén diseñados de tal manera que sea imposible el intercambio de datos personales entre dichos sistemas.

146. En cuanto a los PSAP, los Estados miembros deben garantizar que los datos personales se protejan contra su mal uso, incluido el acceso ilegal a los mismos y su alteración o pérdida, y que sean adecuadamente establecidos al nivel adecuado y debidamente respetados los protocolos relativos al almacenamiento, duración de la retención, tratamiento y protección de los datos personales.

3.3 Estudios de accidentología

147. Los interesados pueden aceptar voluntariamente participar en estudios de accidentología destinados a comprender mejor las causas de los accidentes de tráfico y, en general, con fines científicos.

3.3.1 Base jurídica

148. Cuando los datos se recojan a través de un servicio público de comunicación electrónica, el responsable del tratamiento tendrá que recabar el consentimiento del interesado para poder obtener acceso a la información que ya está almacenada en el vehículo, tal y como establece el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas. De hecho, ninguna de las exenciones previstas en esas disposiciones puede aplicarse en este contexto: el tratamiento no tiene como única finalidad realizar la transmisión de una comunicación a través de una red de comunicaciones electrónicas ni está relacionado con un servicio de la sociedad de la información explícitamente solicitado por el abonado o usuario.

149. En lo que respecta al tratamiento de datos personales y teniendo en cuenta la variedad y la cantidad de datos personales necesarios para los estudios de accidentología, el CEPD recomienda que el tratamiento se base en el consentimiento previo del interesado de acuerdo con el artículo 6 del RGPD. Este consentimiento previo debe ser proporcionado en un formulario específico, a través del cual el interesado se ofrece a participar en el estudio y a que sus datos personales sean tratados con ese fin. El consentimiento será una expresión de la voluntad libre, específica e informada de la persona cuyos datos se están tratando (por ejemplo, marcar una casilla que no está previamente marcada o configurar el ordenador a bordo para activar una función en el vehículo). Dicho consentimiento debe prestarse por separado, para fines específicos, no podrá agruparse con el contrato de compra o de arrendamiento de un automóvil nuevo y debe poder retirarse con la misma facilidad con la que se otorga. La retirada del consentimiento supondrá el cese del tratamiento. A continuación, los datos se suprimirán de la base de datos activa o se anonimizarán.

150. El consentimiento requerido por el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas y el consentimiento necesario como base jurídica para el tratamiento de los datos pueden recogerse al mismo tiempo (por ejemplo, marcando una casilla que indique claramente a qué da su consentimiento el interesado).

151. Hay que señalar que, en función de las condiciones del tratamiento (naturaleza del responsable del tratamiento, etc.), puede elegirse legalmente otra base jurídica siempre que no disminuya la protección específica prevista en el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas (véase el apartado 15). Si el tratamiento se basa en otra base jurídica, como el cumplimiento de una misión realizada en

interés público (artículo 6, apartado 1, letra e), del RGPD), el CEPD recomienda que los interesados se incluyan en el estudio de forma voluntaria.

3.3.2 Datos recopilados

152. El responsable del tratamiento solo recogerá los datos personales que sean estrictamente necesarios para el tratamiento.

153. Hay que tener en cuenta dos tipos de datos:

- **datos relativos a los participantes y a los vehículos;** y
- **datos técnicos de los vehículos** (velocidad instantánea, etc.).

154. La investigación científica vinculada a la accidentología justifica la recogida de la velocidad instantánea, incluso por parte de personas jurídicas que no administran un servicio público en sentido estricto.

155. En efecto, como ya se ha señalado, el CEPD considera que la velocidad instantánea recogida en el marco de un estudio de accidentología no es un dato relacionado con la infracción por destino (es decir, no se recoge con el fin de investigar o enjuiciar una infracción), lo que justifica su recogida por personas jurídicas que no administran un servicio público en sentido estricto.

3.3.3 Periodo de conservación

156. Es importante distinguir entre dos tipos de datos. En primer lugar, los datos relativos a los participantes y a los vehículos pueden conservarse mientras dure el estudio. En segundo lugar, los datos técnicos de los vehículos deben conservarse durante el menor tiempo posible a tal efecto. En este sentido, cinco años a partir de la fecha de finalización del estudio parece un periodo razonable. Al final de dicho período, los datos deberán suprimirse o anonimizarse.

3.3.4 Información y derechos de los interesados

157. Antes del tratamiento de los datos personales, se informará al interesado de acuerdo con el artículo 13 del RGPD, de forma transparente y comprensible. En particular, en el caso de la recogida de la velocidad instantánea, los interesados deben ser informados específicamente de la recogida de datos. Dado que el tratamiento se basa en el consentimiento, se debe informar en concreto al interesado de su derecho a revocarlo en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su revocación. Asimismo, dado que los datos brutos recogidos en este contexto son facilitados por el interesado (a través de formularios específicos o a través de su actividad) y se tratan sobre la base del artículo 6, apartado 1, letra a), del RGPD (consentimiento), el interesado tiene derecho a ejercer su derecho a la portabilidad de los datos. Como se destaca en las Directrices sobre el derecho a la portabilidad de los datos, el CEPD recomienda, en especial, «que los responsables del tratamiento expliquen con claridad la diferencia entre los tipos de datos que un interesado puede recibir en virtud del derecho de acceso o del derecho a la portabilidad de los datos». En consecuencia, el responsable del tratamiento de datos debe proporcionar una forma fácil de retirar su consentimiento, libremente y en cualquier momento, así como desarrollar herramientas para poder responder a las solicitudes de portabilidad de datos.

158. Esta información puede facilitarse al firmar el formulario para aceptar participar en el estudio de accidentología.

3.3.5 Destinatario

159. En principio, solo el responsable y el encargado del tratamiento tienen acceso a los datos.

3.3.6 Seguridad

160. Como se ha señalado anteriormente, las medidas de seguridad establecidas se adaptarán al nivel de sensibilidad de los datos. Por ejemplo, si la velocidad instantánea (o cualquier otro dato relacionado con condenas e infracciones penales) se recoge como parte del estudio de accidentología, el CEPD recomienda encarecidamente que se establezcan fuertes medidas de seguridad, como por ejemplo:

- aplicar medidas de seudonimización (por ejemplo, el direccionamiento calculado mediante clave secreta de datos como el apellido/nombre del interesado y el número de serie);
- almacenar los datos relativos a la velocidad instantánea y a la localización en bases de datos separadas (por ejemplo, utilizando un mecanismo de cifrado de última generación con claves y mecanismos de aprobación distintos);
- o suprimir los datos de localización en cuanto se califica el evento o la secuencia de referencia (por ejemplo, el tipo de carretera, día/noche), y almacenar los datos de identificación directa en una base de datos separada a la que solo puede acceder un número reducido de personas.

3.4 Hacer frente a los robos de vehículos

161. Los interesados pueden desear, en caso de robo, intentar encontrar su vehículo mediante la localización. La utilización de los datos de localización se limita a las estrictas necesidades de la investigación y a la evaluación del caso por parte de las autoridades judiciales competentes.

3.4.1 Base jurídica

162. Cuando los datos se recogen a través de un servicio de comunicación electrónica disponible al público, se aplica el artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

163. Al tratarse de un servicio de la sociedad de la información, dicho artículo no exige el consentimiento para acceder a la información que ya está almacenada en el vehículo cuando el abonado solicita explícitamente este servicio.

164. En cuanto al tratamiento de los datos personales de localización, la base jurídica para su tratamiento será el consentimiento del propietario del vehículo o, en su caso, la ejecución de un contrato (solo para los datos necesarios para la ejecución de un contrato en el que el propietario del vehículo es parte).

165. El consentimiento será una expresión de la voluntad libre, específica e informada de la persona cuyos datos se están tratando (por ejemplo, marcar una casilla que no está previamente marcada o configurar el ordenador a bordo para activar una función en el vehículo). La libertad de dar el consentimiento implica la opción de retirarlo en cualquier momento, de lo que se debe informar expresamente al interesado. La retirada del consentimiento supondrá el cese del tratamiento. A continuación, los datos deben suprimirse de la base de datos activa, anonimizarse o archivarse.

3.4.2 Datos recopilados

166. Los datos de localización únicamente pueden transmitirse a partir de la denuncia del robo, y no pueden recogerse de manera continua el resto del tiempo.

3.4.3 Periodo de conservación

167. Los datos de localización solo pueden conservarse durante el periodo de evaluación del asunto por parte de las autoridades judiciales competentes, o hasta el final de un procedimiento para disipar dudas que no termine con la confirmación del robo del vehículo.

3.4.4 Información de los interesados

168. Antes del tratamiento de los datos personales, se debe informar al interesado de acuerdo con el artículo 13 del RGPD, de forma transparente y comprensible. Más concretamente, el CEPD recomienda que el responsable del tratamiento haga hincapié en que no hay un seguimiento constante del vehículo y que los datos de localización únicamente pueden recogerse y transmitirse a partir de la denuncia del robo. Además, el responsable del tratamiento debe proporcionar al interesado información relativa al hecho de que solo los agentes autorizados de la plataforma de televigilancia y las autoridades legalmente autorizadas tienen acceso a los datos.

169. En cuando a los derechos de los interesados, cuando el tratamiento se base en el consentimiento, se debería informar en concreto al interesado de su derecho a revocarlo en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su revocación. Además, cuando sean los interesados quienes faciliten los datos recogidos en este contexto (a través de formularios específicos o a través de su actividad) y estos se traten sobre la base del artículo 6, apartado 1, letra a), del RGPD (consentimiento) o el artículo 6, apartado 1, letra b), del RGPD (ejecución de un contrato), el interesado tiene derecho a ejercer su derecho a la portabilidad de los datos. Como se destaca en las Directrices sobre el derecho a la portabilidad de los datos, el CEPD recomienda, en especial, «que los responsables del tratamiento expliquen con claridad la diferencia entre los tipos de datos que un interesado puede recibir en virtud del derecho de acceso o del derecho a la portabilidad de los datos».

170. En consecuencia, el responsable del tratamiento de datos debe proporcionar una forma fácil de retirar su consentimiento (solo cuando el consentimiento es la base jurídica), libremente y en cualquier momento, así como desarrollar herramientas para poder responder a las solicitudes de portabilidad de datos.

171. La información puede facilitarse en el momento de la firma del contrato.

3.4.5 Destinatarios

172. En caso de que se denuncie el robo, los datos de localización pueden transmitirse a i) los agentes autorizados de la plataforma de televigilancia, y ii) a las autoridades legalmente autorizadas.

3.4.6 Seguridad

173. Se aplican las recomendaciones generales. Véase la sección 2.7.