

# Diretrizes



## **Diretrizes 01/2020 relativas ao tratamento de dados pessoais no contexto dos veículos conectados e das aplicações relacionadas com a mobilidade**

**Versão 2.0**

**Adotadas em 9 de março de 2021**

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

## Histórico das versões

Versão 2.0	9 de março de 2021	Adoção das diretrizes após consulta pública
Versão 1.0	28 de janeiro de 2020	Adoção das diretrizes para consulta pública

1	INTRODUÇÃO .....	4
1.1	Obras conexas .....	5
1.2	Direito aplicável.....	6
1.3	Âmbito.....	8
1.4	Definições .....	12
1.5	Riscos em matéria de privacidade e proteção de dados.....	14
2	RECOMENDAÇÕES GERAIS .....	16
2.1	Categorias de dados .....	16
2.2	Finalidades.....	18
2.3	Relevância e minimização dos dados .....	19
2.4	Proteção de dados desde a conceção e por defeito .....	19
2.5	Informação .....	22
2.6	Direitos do titular dos dados .....	24
2.7	Segurança .....	25
2.8	Transmissão de dados pessoais para terceiros .....	26
2.9	Transferência de dados pessoais para fora da UE/EEE .....	26
2.10	Utilização de tecnologias Wi-Fi a bordo.....	27
3	ESTUDOS DE CASOS.....	27
3.1	Prestação de um serviço por um terceiro .....	27
3.2	<i>eCall</i> .....	31
3.3	Estudos de acidentologia .....	34
3.4	Combater o furto de automóveis.....	36

Tendo em conta o artigo 70.º, n.º 1, alínea e), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (a seguir designado por «RGPD»),

Tendo em conta o Acordo EEE, nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n.º 154/2018, de 6 de julho de 2018<sup>1</sup>,

Tendo em conta o artigo 12.º e o artigo 22.º do seu regulamento interno,

## ADOTOU AS SEGUINTE DIRETRIZES

### 1 INTRODUÇÃO

1. Símbolo da economia do século XX, o automóvel é um dos produtos de consumo de massa que teve impacto na sociedade no seu conjunto. Geralmente associados à noção de liberdade, os automóveis são frequentemente considerados como mais do que um mero meio de transporte. Com efeito, representam uma área privada na qual as pessoas podem desfrutar de um certo nível de autonomia de decisão, sem se depararem com quaisquer interferências externas. Atualmente, à medida que os veículos conectados se transformam na tendência dominante, tal visão já não corresponde à realidade. A conectividade a bordo está a expandir-se rapidamente, passando dos modelos de luxo e das marcas de qualidade superior para os modelos de elevada produção do mercado médio, e os veículos estão a tornar-se enormes centros de dados. Além dos veículos, também os condutores e os passageiros estão a tornar-se cada vez mais conectados. De facto, muitos modelos lançados no mercado nos últimos anos integram sensores e equipamentos conectados a bordo que podem recolher e registar, entre outros, o desempenho do motor, os hábitos de condução, os locais visitados e, eventualmente, até os movimentos oculares do condutor, a sua pulsação, ou dados biométricos com o objetivo de identificar uma pessoa singular de forma inequívoca<sup>2</sup>.
2. Tal tratamento de dados está a ocorrer num ecossistema complexo, que não se limita aos intervenientes tradicionais do setor automóvel, mas que é igualmente moldado pelo surgimento de novos intervenientes pertencentes à economia digital. Estes novos intervenientes podem prestar serviços de ludoinformação, tais como música em linha, informações a respeito das condições das estradas e do trânsito, ou disponibilizar sistemas e serviços de assistência ao condutor, tais como *software* de piloto automático, atualizações das condições do veículo, seguros baseados na utilização ou mapeamento dinâmico. Além disso, uma vez que os veículos estão conectados por meio de redes de comunicação eletrónica, os gestores de infraestruturas rodoviárias e os operadores de telecomunicações envolvidos neste processo desempenham igualmente um papel importante no que diz respeito às eventuais operações de tratamento aplicáveis aos dados pessoais dos condutores e dos passageiros.

---

<sup>1</sup> As referências a «Estados-Membros» efetuadas ao longo do presente documento devem ser entendidas como referências a «Estados do EEE».

<sup>2</sup> Infografia «Data and the connected car» (Os dados e o automóvel conectado), do Future of Privacy Forum, [https://fpf.org/wp-content/uploads/2017/06/2017\\_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf](https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf).

3. Por outro lado, os veículos conectados estão a gerar quantidades crescentes de dados que, na maioria dos casos, podem ser considerados dados pessoais, uma vez que estão relacionados com os condutores ou com os passageiros. Mesmo que os dados recolhidos por um automóvel conectado não estejam diretamente associados a um nome, mas sim a aspetos e a características técnicas do veículo, dizem respeito ao condutor ou aos passageiros do automóvel. A título exemplificativo, os dados relativos ao estilo de condução ou à distância percorrida, os dados relativos ao desgaste das peças do veículo, os dados de localização ou os dados recolhidos por câmaras podem dizer respeito ao comportamento do condutor, bem como a informações a respeito de outras pessoas que possam estar no interior do veículo ou de titulares de dados que circulem nas imediações. Tais dados técnicos são gerados por uma pessoa singular e permitem a sua identificação direta ou indireta pelo responsável pelo tratamento ou por outra pessoa. O veículo pode ser considerado como um terminal, passível de utilização por diferentes utilizadores. Por conseguinte, tal como no caso de um computador pessoal, esta eventual pluralidade de utilizadores não afeta a natureza pessoal dos dados.
4. Em 2016, a Fédération Internationale de l'Automobile (FIA) realizou uma campanha em toda a Europa com o título «My Car My Data» (O meu automóvel, os meus dados) a fim de obter a opinião dos europeus a respeito dos automóveis conectados<sup>3</sup>. Embora tenha demonstrado o grande interesse dos condutores pela conectividade, a campanha salientou igualmente a vigilância que deve ser exercida no que diz respeito à utilização dos dados gerados pelos veículos, bem como a importância de cumprir a legislação em matéria de proteção de dados pessoais. Assim, o desafio para cada uma das partes interessadas é a inclusão da dimensão de «proteção de dados pessoais» desde a fase de conceção dos produtos e a garantia de que os utilizadores de automóveis beneficiam de transparência e controlo em relação aos seus dados, de acordo com o considerando 78 do RGPD. Tal abordagem ajuda a reforçar a confiança dos utilizadores e, assim, o desenvolvimento a longo prazo dessas tecnologias.

## 1.1 Obras conexas

5. Durante a última década, os veículos conectados tornaram-se um assunto importante para os reguladores, com um forte aumento dessa relevância nos últimos anos. Assim, foram publicadas várias obras a nível nacional e internacional relativas à segurança e à privacidade dos veículos conectados. Tais regulamentos e iniciativas visam complementar os quadros existentes em matéria de privacidade e proteção de dados com regras setoriais específicas ou facultar orientações aos profissionais.

### 1.1.1 Iniciativas a nível europeu e a nível internacional

6. Desde 31 de março de 2018, é obrigatória a existência de um sistema *eCall* a bordo com base no número 112 em todos os novos tipos de veículos M1 e N1 (veículos ligeiros de passageiros e veículos comerciais ligeiros)<sup>4, 5</sup>. Em 2006, o Grupo de Trabalho do Artigo 29.º já havia adotado um documento de trabalho sobre as consequências da iniciativa *eCall* em termos de proteção dos dados e da privacidade<sup>6</sup>. Além disso, tal como abordado anteriormente, em outubro de 2017 o Grupo de Trabalho do Artigo 29.º adotou igualmente

---

<sup>3</sup> Campanha «My Car My Data» (O meu automóvel, os meus dados), <http://www.mycarmydata.eu/>.

<sup>4</sup> «The interoperable EU-wide eCall» (A *eCall* interoperável a nível da UE), [https://ec.europa.eu/transport/themes/its/road/action\\_plan/ecall\\_en](https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en).

<sup>5</sup> Decisão n.º 585/2014/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa à implantação do serviço interoperável de chamadas de urgência a nível da UE (*eCall*) (Texto relevante para efeitos do EEE), <https://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32014D0585>.

<sup>6</sup> Documento de trabalho sobre as consequências da iniciativa *eCall* em termos de proteção dos dados e da privacidade, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125\\_pt.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_pt.pdf).

um parecer relativo ao tratamento de dados pessoais no contexto dos sistemas de transporte inteligentes cooperativos (STIC).

7. Em janeiro de 2017, a Agência Europeia para a Segurança das Redes e da Informação (ENISA) publicou um estudo centrado na cibersegurança e na resiliência dos automóveis inteligentes, enumerando os ativos sensíveis, bem como as correspondentes ameaças, riscos, fatores de atenuação e eventuais medidas de segurança a implementar<sup>7</sup>. Em setembro de 2017, a Conferência Internacional de Comissários para a Proteção dos Dados e da Vida Privada (ICDPPC) adotou uma resolução relativa aos veículos conectados<sup>8</sup>. Finalmente, em abril de 2018, o Grupo Internacional de Trabalho relativo à Proteção de Dados nas Telecomunicações (IWGDPT) adotou igualmente um documento de trabalho relativo aos veículos conectados<sup>9</sup>.

### 1.1.2 Iniciativas nacionais dos membros do Comité Europeu para a Proteção de Dados (CEPD)

8. Em janeiro de 2016, a conferência das autoridades federais e estatais alemãs de proteção de dados e a associação alemã do setor automóvel (VDA) publicaram uma declaração comum relativa aos princípios da proteção de dados em veículos conectados e não conectados<sup>10</sup>. Em agosto de 2017, o centro para os veículos conectados e autónomos (CCAV) do Reino Unido publicou um guia que estabelece princípios de cibersegurança para veículos conectados e automatizados, a fim de aumentar a sensibilização sobre esta matéria no setor automóvel<sup>11</sup>. Em outubro de 2017, a autoridade francesa de proteção de dados, a Commission Nationale de l'Informatique et des Libertés (CNIL), publicou um pacote de conformidade para automóveis conectados, a fim de prestar assistência às partes interessadas sobre como integrar a proteção de dados desde a conceção e por defeito, permitindo que os titulares dos dados tenham um controlo eficaz dos seus dados<sup>12</sup>.

## 1.2 Direito aplicável

9. O quadro jurídico pertinente da UE é o RGPD. É aplicável a qualquer caso em que o tratamento de dados no contexto dos veículos conectados envolva o tratamento de dados pessoais das pessoas.
10. Para além do RGPD, a Diretiva 2002/58/CE, alterada pela Diretiva 2009/136/CE (a seguir designada por «Diretiva Privacidade Eletrónica»), **estabelece uma norma específica para todos os intervenientes que pretendam conservar ou aceder a informações conservadas no equipamento terminal de um assinante ou de um utilizador no Espaço Económico Europeu (EEE).**

---

<sup>7</sup> «Cyber security and resilience of smart cars» (Cibersegurança e resiliência dos automóveis inteligentes), <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>.

<sup>8</sup> «Resolution on data protection in automated and connected vehicles» (Resolução relativa à proteção de dados em veículos automatizados e conectados), [https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles\\_en\\_1.pdf](https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf).

<sup>9</sup> Documento de trabalho relativo aos veículos conectados, <https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/>.

<sup>10</sup> «Data protection aspects of using connected and non-connected vehicles» (Aspetos da proteção de dados na utilização de veículos conectados e não conectados), [https://www.lida.bayern.de/media/dsk\\_joint\\_statement\\_vda.pdf](https://www.lida.bayern.de/media/dsk_joint_statement_vda.pdf).

<sup>11</sup> «Principles of cyber security for connected and automated vehicles» (Princípios de cibersegurança para veículos conectados e automatizados), <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>.

<sup>12</sup> «Compliance package for a responsible use of data in connected cars» (Pacote de conformidade para uma utilização responsável dos dados em automóveis conectados), <https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data>.

11. De facto, enquanto a maioria das disposições da Diretiva Privacidade Eletrónica (artigo 6.º, artigo 9.º, etc.) é unicamente aplicável aos prestadores de serviços de comunicações eletrónicas publicamente disponíveis e aos fornecedores de redes públicas de comunicação, o artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica é uma disposição geral. É aplicável não apenas aos serviços de comunicações eletrónicas, mas também a todas as entidades, privadas ou públicas, que coloquem informações num equipamento terminal, ou leiam informações do mesmo, independentemente da natureza dos dados que são objeto de conservação ou acesso.
12. Relativamente à noção de «*equipamento terminal*», a definição é apresentada na Diretiva 2008/63/CE<sup>13</sup>. O artigo 1.º, n.º 1, define o equipamento terminal como «*a) Qualquer equipamento ligado direta ou indiretamente ao interface de uma rede pública de telecomunicações para transmitir, tratar ou receber informações; em ambos os casos, de ligação direta ou indireta, a ligação pode ser feita por cabo, fibra ótica ou por via eletromagnética; a conexão é indireta caso haja um aparelho intermédio entre o equipamento terminal e o interface da rede pública; b) É igualmente considerado equipamento terminal o equipamento para estações terrestres de satélites*».
13. Consequentemente, desde que os critérios referidos anteriormente sejam cumpridos, o veículo conectado e o dispositivo que lhe está conectado devem ser considerados como «*equipamento terminal*» (tal como um computador, um telemóvel inteligente ou uma TV conectada) e as disposições do artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica são aplicáveis, se for caso disso.
14. Tal como descrito pelo CEPD no seu Parecer 5/2019 sobre a interação entre a Diretiva Privacidade Eletrónica e o RGPD<sup>14</sup>, o artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica prevê que, como regra, e sem prejuízo das exceções a essa regra mencionadas no n.º 17 *infra*, seja exigido o consentimento prévio para a conservação de informações, ou a obtenção de acesso às informações já conservadas, no equipamento terminal de um assinante ou utilizador. Na medida em que as informações conservadas no dispositivo do utilizador final constituam dados pessoais, o artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica prevalece sobre o artigo 6.º do RGPD no que se refere à atividade de conservação ou à possibilidade de acesso a essas informações<sup>15</sup>. Quaisquer operações de tratamento de dados pessoais no seguimento das operações de tratamento referidas anteriormente, incluindo o tratamento de dados pessoais obtidos por meio do acesso a informações conservadas no equipamento terminal, devem ter uma base jurídica nos termos do artigo 6.º do RGPD para serem lícitas<sup>16</sup>.
15. Dado que o responsável pelo tratamento, ao solicitar o consentimento para a conservação ou a possibilidade de acesso a informações de acordo com o artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica, terá de informar o titular dos dados a respeito de todas as finalidades do tratamento – incluindo qualquer tratamento no seguimento das operações referidas anteriormente (ou seja, o «tratamento posterior») –, o consentimento ao abrigo do artigo 6.º do RGPD será, em geral, o fundamento jurídico mais adequado para abranger o tratamento de dados pessoais no seguimento de tais operações (na medida em que a finalidade do tratamento seguinte seja abrangida pelo consentimento do titular dos dados,

---

<sup>13</sup> Diretiva 2008/63/CE da Comissão, de 20 de junho de 2008, relativa à concorrência nos mercados de equipamentos terminais de telecomunicações (Versão codificada) (Texto relevante para efeitos do EEE), <https://eur-lex.europa.eu/legal-content/pt/ALL/?uri=CELEX%3A32008L0063>.

<sup>14</sup> Parecer 5/2019 sobre a interação entre a Diretiva Privacidade Eletrónica e o RGPD, particularmente em matéria de competência, atribuições e poderes das autoridades de proteção de dados, do Comité Europeu para a Proteção de Dados, adotado em 12 de março de 2019 (a seguir designado por «Parecer 5/2019»), n.º 40.

<sup>15</sup> *Ibidem*, n.º 40.

<sup>16</sup> *Ibidem*, n.º 41.

ver n.ºs 53 e 54). Assim, o consentimento será suscetível de constituir o fundamento jurídico, tanto para a conservação e para a possibilidade de acesso a informações já conservadas como para o tratamento posterior dos dados pessoais<sup>17</sup>. De facto, ao avaliar a conformidade com o artigo 6.º do RGPD, deve ter-se em conta que o tratamento no seu conjunto envolve atividades específicas para as quais o legislador da UE procurou proporcionar proteção adicional<sup>18</sup>. Além disso, os responsáveis pelo tratamento devem ter em conta o impacto nos direitos dos titulares dos dados ao identificarem o fundamento jurídico adequado, a fim de respeitarem o princípio da lealdade<sup>19</sup>. A questão fundamental é que os responsáveis pelo tratamento não podem recorrer ao artigo 6.º do RGPD para efeitos de redução da proteção adicional proporcionada pelo artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica.

16. O CEPD recorda que a noção de consentimento constante da Diretiva Privacidade Eletrónica continua a ser a mesma noção de consentimento constante do RGPD e deve cumprir todos os requisitos em matéria de consentimento, tal como previsto no artigo 4.º, ponto 11, e no artigo 7.º do RGPD.
17. Todavia, embora o consentimento seja o princípio, o artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica permite que a conservação de informações ou a possibilidade de acesso a informações já conservadas no equipamento terminal estejam isentas do requisito de consentimento informado, se cumprirem um dos seguintes critérios:
  - ) **Isenção 1:** tenham como única finalidade efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas;
  - ) **Isenção 2:** sejam estritamente necessárias ao fornecedor para fornecer um serviço da sociedade da informação que tenha sido expressamente solicitado pelo assinante ou pelo utilizador.
18. Em tais casos, o tratamento de dados pessoais, incluindo os dados pessoais obtidos por meio do acesso a informações conservadas no equipamento terminal, baseia-se num dos fundamentos jurídicos previstos no artigo 6.º do RGPD. Por exemplo, o consentimento não é necessário quando o tratamento de dados for necessário para fornecer serviços de navegação por GPS solicitados pelo titular dos dados, quando tais serviços possam ser qualificados como serviços da sociedade da informação.

### 1.3 Âmbito

19. O CEPD gostaria de salientar que as presentes diretrizes se destinam a facilitar a conformidade do tratamento de dados pessoais efetuado por um vasto conjunto de partes interessadas que intervêm neste ambiente. Todavia, não se destinam a abranger todos os casos possíveis de utilização neste contexto, nem a facultar orientações para todas as situações específicas possíveis.
20. O âmbito do presente documento centra-se, em especial, no tratamento de dados pessoais relacionado com a utilização não profissional de veículos conectados por titulares de dados: por exemplo, condutores, passageiros, proprietários de veículos, outros utentes da estrada, etc. Mais especificamente, o presente documento aborda os dados pessoais: i) objeto de tratamento no interior do veículo, ii) partilhados entre o veículo e os dispositivos pessoais que lhe estão conectados (por exemplo, o telemóvel inteligente do utilizador), ou iii)

---

<sup>17</sup> O consentimento exigido pelo artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica e o consentimento necessário como fundamento jurídico para o tratamento de dados (artigo 6.º do RGPD) para a mesma finalidade específica podem ser obtidos simultaneamente (por exemplo, ao assinalar uma caixa de verificação que indique claramente aquilo que o titular dos dados está a consentir).

<sup>18</sup> Parecer 5/2019, n.º 41.

<sup>19</sup> Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados, do Comité Europeu para a Proteção de Dados, versão 2.0, 8 de outubro de 2019, n.º 1.



recolhidos localmente no veículo e exportados para entidades externas (por exemplo, construtores de veículos, gestores de infraestruturas, companhias de seguros, reparadores de automóveis) para efeitos de tratamento posterior.

21. No presente documento, a definição de veículo conectado tem de ser compreendida como um conceito lato. Pode ser definido como um veículo equipado com várias unidades de controlo eletrónico (UCE) que estão associadas entre si por meio de uma rede a bordo, bem como com mecanismos de conectividade que lhe permitem partilhar informações com outros dispositivos, tanto no interior como no exterior do veículo. Como tal, os dados podem ser partilhados entre o veículo e os dispositivos pessoais que lhe estão conectados, permitindo, por exemplo, o espelhamento de aplicações móveis na unidade de informação e de entretenimento no painel de instrumentos do automóvel. Além disso, o desenvolvimento de aplicações móveis autónomas, ou seja, independentes do veículo (por exemplo, que dependem unicamente da utilização do telefone inteligente) destinadas a prestar assistência aos condutores, inclui-se no âmbito do presente documento, dado que estas aplicações contribuem para as capacidades de conectividade do veículo, embora possam não depender efetivamente da transmissão de dados com o veículo. As aplicações para veículos conectados são variadas e distintas e podem incluir<sup>20</sup>:
22. *Gestão da mobilidade*: funções que permitem aos condutores chegarem a um destino de forma rápida e eficiente em termos de custos, ao facultarem informações atempadas a respeito da navegação por GPS, de condições atmosféricas potencialmente perigosas (por exemplo, estradas com piso gelado), de congestionamentos de tráfego ou de trabalhos de construção de estradas, parques de estacionamento ou assistência em oficinas, consumo otimizado de combustível ou tarifação rodoviária.
23. *Gestão do veículo*: funções que devem ajudar os condutores a reduzir os custos de operação e aumentar a facilidade de utilização, tais como notificação das condições do veículo e avisos de manutenção, transferência de dados de utilização (por exemplo, para serviços de reparação de veículos), seguros personalizados em função da quilometragem e da condução, operações à distância (por exemplo, sistema de aquecimento) ou configurações de perfil (por exemplo, posição do banco).
24. *Segurança rodoviária*: funções que alertam o condutor quanto a perigos externos e reações internas, tais como proteção contra colisões, avisos de perigo, avisos de saída da faixa de rodagem, deteção de sonolência do condutor, chamada de emergência (*eCall*) ou «caixas pretas» para investigação de colisões (gravador de dados de eventos).
25. *Entretenimento*: funções que facultam informações e que envolvem o entretenimento do condutor e dos passageiros, tais como interfaces com telefones inteligentes (chamadas telefónicas mãos-livres, mensagens de texto geradas por voz), pontos ativos de acesso à Internet sem fios, música, vídeo, Internet, redes sociais, serviços de escritório móvel ou de «casa inteligente».
26. *Assistência ao condutor*: funções que envolvem a condução parcial ou totalmente automatizada, tais como assistência operacional ou piloto automático em tráfego intenso, no estacionamento, ou em autoestradas.
27. *Bem-estar*: funções de monitorização do conforto, da capacidade e da aptidão do condutor para a condução, tais como deteção de fadiga ou assistência médica.
28. Assim, os veículos podem ou não ser nativamente conectados e os dados pessoais podem ser recolhidos por vários meios, incluindo: i) sensores do veículo, ii) caixas telemáticas, ou

---

<sup>20</sup> Estratégia PwC de 2014, «In the fast lane. The bright future of connected cars» (Na via rápida. O futuro brilhante dos automóveis conectados), [https://www.strategyand.pwc.com/media/file/Strategyand\\_In-the-Fast-Lane.pdf](https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf).

iii) aplicações móveis (por exemplo, acedidas a partir de um dispositivo pertencente a um condutor). Para se enquadrarem no âmbito do presente documento, as aplicações móveis têm de estar relacionadas com o contexto de condução. Por exemplo, as aplicações de navegação por GPS enquadram-se nesse âmbito. No entanto, as aplicações cujas funcionalidades apenas sugiram locais de interesse (restaurantes, monumentos históricos, etc.) aos condutores não se enquadram no âmbito das presentes diretrizes.

29. Muitos dos dados gerados por um veículo conectado dizem respeito a uma pessoa singular identificada ou identificável e, assim, constituem dados pessoais. Por exemplo, os dados incluem dados diretamente identificáveis (por exemplo, a identidade completa do condutor), bem como dados indiretamente identificáveis, tais como os pormenores das viagens efetuadas, os dados de utilização do veículo (por exemplo, dados relativos ao estilo de condução ou à distância percorrida), ou os dados técnicos do veículo (por exemplo, dados relativos ao desgaste das peças do veículo), que, por meio do cruzamento com outros ficheiros e, especialmente, com o número de identificação do veículo (NIV), podem ser associados a uma pessoa singular. Os dados pessoais em veículos conectados podem igualmente incluir metadados, tais como o estado de manutenção do veículo. Por outras palavras, quaisquer dados que possam ser associados a uma pessoa singular enquadram-se, por conseguinte, no âmbito do presente documento.
30. O ecossistema de veículos conectados abrange um vasto espectro de partes interessadas. Este ecossistema inclui, mais precisamente, os intervenientes tradicionais do setor automóvel, bem como os intervenientes emergentes do setor digital. Assim, as presentes diretrizes destinam-se aos construtores de veículos, de equipamentos e de componentes para automóveis, aos reparadores de automóveis, aos concessionários de automóveis, aos prestadores de serviços aos veículos, aos gestores de frotas, às companhias de seguros automóveis, aos prestadores de serviços de entretenimento, aos operadores de telecomunicações, aos gestores de infraestruturas rodoviárias e às autoridades públicas, bem como aos titulares dos dados. O CEPD sublinha que as categorias de titulares dos dados diferirão consoante o serviço (por exemplo, condutores, proprietários, passageiros, etc.). Trata-se de uma lista não exaustiva, dado que o ecossistema engloba uma grande variedade de serviços, incluindo serviços para os quais é necessária uma autenticação ou identificação direta e serviços para os quais tal não é necessário.
31. Alguns dos tratamentos de dados efetuados por pessoas singulares no interior do veículo enquadram-se «*no exercício de atividades exclusivamente pessoais ou domésticas*» e, conseqüentemente, estão excluídos do âmbito de aplicação do RGPD<sup>21</sup>. Tal diz respeito, em especial, à utilização de dados pessoais no interior dos veículos pelos próprios titulares dos dados que introduziram os referidos dados no painel de instrumentos do veículo. Todavia, o CEPD recorda que, de acordo com o respetivo considerando 18, o RGPD «*é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas*».

### 1.3.1 Fora do âmbito do presente documento

32. Os empregadores que disponibilizam automóveis de serviço aos membros do seu pessoal podem pretender controlar as ações dos seus trabalhadores (por exemplo, a fim de garantir a segurança do trabalhador, dos bens ou dos veículos, de afetar recursos, de localizar e cobrar um serviço ou de verificar o tempo de trabalho). O tratamento de dados efetuado neste contexto pelos empregadores suscita considerações específicas a respeito do

---

<sup>21</sup> Ver artigo 2.º, n.º 2, alínea c), do RGPD.

contexto laboral, que podem ser reguladas pelo direito do trabalho a nível nacional e que não podem ser pormenorizadas nas presentes diretizes<sup>22</sup>.

33. Embora o tratamento de dados no contexto de veículos comerciais utilizados para fins profissionais (como os transportes públicos) e transporte partilhado e a solução da mobilidade como serviço possam suscitar considerações específicas que não se enquadrem no âmbito das presentes diretizes gerais, muitos dos princípios e recomendações enunciados no presente documento serão igualmente aplicáveis a esses tipos de tratamento.
34. Dado que os veículos conectados são sistemas habilitados para radiocomunicação, estão sujeitos a seguimento passivo, tal como o seguimento por Wi-Fi ou por Bluetooth. Nesse sentido, não diferem de outros dispositivos conectados e enquadram-se no âmbito de aplicação da Diretiva Privacidade Eletrónica, atualmente em fase de revisão. Por conseguinte, tal exclui igualmente o seguimento em larga escala de veículos equipados com Wi-Fi<sup>23</sup> por uma densa rede de pessoas nas proximidades que utilizam serviços comuns de localização de telemóveis inteligentes, que comunicam sistematicamente todas as redes Wi-Fi visíveis aos servidores centrais. Dado que o Wi-Fi incorporado pode ser considerado como um identificador secundário do veículo<sup>24</sup>, existe o risco de uma recolha sistemática e contínua de perfis completos da deslocação dos veículos.
35. Os veículos estão cada vez mais equipados com dispositivos de gravação de imagens (por exemplo, sistemas de câmaras de estacionamento ou câmaras no painel de instrumentos). Uma vez que está em causa a gravação de locais públicos, que exige uma avaliação do quadro legislativo aplicável em cada Estado-Membro, este tratamento de dados não se enquadra no âmbito das presentes diretizes.
36. O tratamento de dados que permite a utilização de sistemas de transporte inteligentes cooperativos (STIC) – tal como definido na Diretiva 2010/40/UE<sup>25</sup> – foi abordado num parecer específico do Grupo de Trabalho do Artigo 29.<sup>º</sup><sup>26</sup>. Embora a definição do conceito de STIC constante da diretiva não inclua quaisquer especificações técnicas, o Grupo de Trabalho do Artigo 29.<sup>º</sup> centra-se, no seu parecer, nas comunicações de curto alcance, ou seja, que não implicam a intervenção de um operador da rede. Mais especificamente, apresenta análises para casos de utilização específica concebidos para a implantação inicial e compromete-se a avaliar posteriormente as novas questões que seguramente serão suscitadas quando for implementado um nível superior de automatização. Dado que as implicações em matéria de proteção de dados no contexto dos STIC são muito específicas (quantidades sem precedentes de dados de localização, transmissão contínua de dados pessoais, partilha de dados entre veículos e com outras infraestruturas rodoviárias, etc.) e

---

<sup>22</sup> O Grupo de Trabalho do Artigo 29.<sup>º</sup> aprofundou esta matéria no seu Parecer 2/2017 sobre o tratamento de dados no local de trabalho (GT 249), [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=610169](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169).

<sup>23</sup> Para mais pormenores, ver: <https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html>.

<sup>24</sup> Markus Ullmann, Tobias Franz e Gerd Nolden, «Vehicle Identification Based on Secondary Vehicle Identifier – Analysis, and Measurements» (Identificação de veículos com base em identificadores secundários dos veículos – Análises e medições), in *Proceedings, VEHICULAR 2017*, «The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications» (Sexta conferência internacional sobre os desenvolvimentos nos sistemas dos veículos), Nice, França, 23 a 27 de julho de 2017, p. 32 a 37.

<sup>25</sup> Diretiva 2010/40/UE, de 7 de julho de 2010, que estabelece um quadro para a implantação de sistemas de transporte inteligentes no transporte rodoviário, inclusive nas interfaces com outros modos de transporte, <https://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32010L0040>.

<sup>26</sup> Parecer 03/2017 sobre o tratamento de dados pessoais no contexto dos Sistemas de Transporte Inteligentes Cooperativos (STIC), do Grupo de Trabalho do Artigo 29.<sup>º</sup>, [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=610171](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171).

que ainda se encontram em fase de debate a nível europeu, o tratamento de dados pessoais nesse contexto não é abrangido pelas presentes diretrizes.

37. Finalmente, o presente documento não visa abordar todos os possíveis problemas e questões suscitados pelos veículos conectados e não pode, por conseguinte, ser considerado como exaustivo.

#### 1.4 Definições

38. O **tratamento** de dados pessoais abrange qualquer operação que envolva dados pessoais, como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição, etc<sup>27</sup>.
39. O **titular dos dados** é a pessoa singular a quem os dados abrangidos pelo tratamento se referem. No contexto dos veículos conectados, em especial, pode tratar-se do condutor (principal ou ocasional), do passageiro ou do proprietário do veículo<sup>28</sup>.
40. O **responsável pelo tratamento** é a pessoa que determina as finalidades e os meios do tratamento que ocorre nos veículos conectados<sup>29</sup>. Os responsáveis pelo tratamento podem incluir prestadores de serviços que tratam dados do veículo para enviar ao condutor informações relativas ao trânsito, mensagens ou alertas de condução ecológica relativos ao funcionamento do veículo, companhias de seguros que oferecem contratos em função da quilometragem, ou construtores de veículos que recolhem dados relativos ao desgaste que afeta as peças do veículo a fim de melhorar a respetiva qualidade. Nos termos do artigo 26.º do RGPD, dois ou mais responsáveis pelo tratamento podem determinar conjuntamente as finalidades e os meios do tratamento e, assim, serem considerados como responsáveis conjuntos pelo tratamento. Neste caso, têm de definir claramente as respetivas obrigações, especialmente no que diz respeito ao exercício dos direitos dos titulares dos dados e à prestação de informações, tal como referido nos artigos 13.º e 14.º do RGPD.
41. O **subcontratante** é qualquer pessoa que trata os dados pessoais por conta do responsável pelo tratamento<sup>30</sup>. O subcontratante recolhe e trata os dados mediante instruções do responsável pelo tratamento, sem utilizar esses dados para as suas próprias finalidades. A título de exemplo, em alguns casos, os construtores de equipamentos e de componentes para automóveis podem tratar os dados por conta dos construtores de veículos (o que não os impede de ser responsáveis pelo tratamento de dados para outras finalidades). Para além de exigir que os subcontratantes implementem medidas técnicas e organizativas adequadas a fim de garantir um nível de segurança adaptado ao risco, o artigo 28.º do RGPD estabelece as obrigações dos subcontratantes.
42. Entende-se por **destinatário** uma pessoa singular ou coletiva, uma autoridade pública, uma agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro<sup>31</sup>. A título de exemplo, um parceiro comercial do prestador de serviços que recebe do prestador de serviços dados pessoais gerados a partir do veículo é um destinatário de dados pessoais. Quer atue como um novo

---

<sup>27</sup> Ver artigo 4.º, ponto 2, do RGPD.

<sup>28</sup> Ver artigo 4.º, ponto 1, do RGPD.

<sup>29</sup> Ver artigo 4.º, ponto 7, do RGPD e «[Guidelines 07/2020 on the concepts of controller and processor in the GDPR](#)» (Diretrizes 07/2020 relativas aos conceitos de responsável pelo tratamento e de subcontratante do RGPD) (a seguir designadas por «Diretrizes 07/2020»), do Comité Europeu para a Proteção de Dados.

<sup>30</sup> Ver artigo 4.º, ponto 8, do RGPD e as Diretrizes 07/2020.

<sup>31</sup> Ver artigo 4.º, ponto 9, do RGPD e as Diretrizes 07/2020.

responsável pelo tratamento ou como um subcontratante, deve cumprir todas as obrigações impostas pelo RGPD.

43. Todavia, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários<sup>32</sup>; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento. A título de exemplo, as autoridades policiais são terceiros autorizados quando solicitam dados pessoais como parte de uma investigação, em conformidade com o direito da União Europeia ou dos Estados-Membros.

---

<sup>32</sup> Artigo 4.º, ponto 9, e considerando 31 do RGPD.

## 1.5 Riscos em matéria de privacidade e proteção de dados

44. O Grupo de Trabalho do Artigo 29.<sup>o</sup> já manifestou várias preocupações relativas aos sistemas da Internet das Coisas (IdC) que também podem ser aplicáveis aos veículos conectados<sup>33</sup>. As questões relacionadas com a segurança e o controlo dos dados já salientadas em relação à IdC são ainda mais sensíveis no contexto dos veículos conectados, dado que implicam preocupações em matéria de segurança rodoviária – e que podem ter impacto na integridade física do condutor – num ambiente tradicionalmente considerado como isolado e protegido de interferências externas.
45. Além disso, os veículos conectados suscitam preocupações significativas em matéria de proteção de dados e de privacidade no que diz respeito ao tratamento de dados de localização, dado que a sua natureza cada vez mais intrusiva pode dificultar as atuais opções para permanecer anónimo. O CEPD pretende destacar especialmente e sensibilizar as partes interessadas para o facto de a utilização de tecnologias de localização exigir a implementação de garantias específicas, a fim de evitar a vigilância das pessoas e a utilização abusiva dos dados.

### 1.5.1 Falta de controlo e assimetria da informação

46. Nem sempre é possível informar adequadamente os condutores e os passageiros dos veículos a respeito do tratamento de dados que ocorre num veículo conectado ou por meio deste. Só é possível prestar as informações ao proprietário do veículo, que pode não ser o condutor, e essas informações podem também não ser facultadas atempadamente. Assim, existe o risco de que não sejam disponibilizadas funcionalidades ou opções suficientes para o exercício do controlo necessário para que as pessoas afetadas possam usufruir dos seus direitos em matéria de proteção de dados e de privacidade. Este ponto é importante dado que, durante a respetiva vida útil, os veículos podem pertencer a mais do que um proprietário, por serem vendidos ou alugados e não comprados.
47. Além disso, a comunicação no interior do veículo pode ser ativada automaticamente, bem como por defeito, sem que a pessoa tenha consciência desse facto. Na ausência da possibilidade de controlar eficazmente a forma como o veículo e o respetivo equipamento conectado interagem, torna-se extraordinariamente difícil para o utilizador controlar o fluxo de dados. Será ainda mais difícil controlar a sua utilização subsequente e, assim, evitar um potencial desvirtuamento da função.

### 1.5.2 Qualidade do consentimento do utilizador

48. O CEPD sublinha que, quando o tratamento de dados se baseia no consentimento, todos os elementos do consentimento válido têm de ser cumpridos, o que significa que o consentimento deve ser livre, específico e informado e constitui uma indicação inequívoca da vontade do titular dos dados, tal como interpretada nas diretrizes do CEPD relativas ao consentimento<sup>34</sup>. Os responsáveis pelo tratamento devem estar especialmente atentos às modalidades de obtenção de consentimento válido de diferentes participantes, como os proprietários ou os utilizadores de automóveis. Esse consentimento deve ser dado separadamente, para finalidades específicas e não pode ser associado ao contrato de compra ou locação financeira de um automóvel novo. O consentimento deve poder ser retirado com a mesma facilidade com que é dado.
49. Este mesmo princípio tem de ser aplicado quando é necessário o consentimento para cumprir a Diretiva Privacidade Eletrónica, por exemplo, se existir uma conservação de

---

<sup>33</sup> Parecer 8/2014 sobre os recentes desenvolvimentos na Internet das Coisas, do Grupo de Trabalho do Artigo 29.<sup>o</sup>, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223\\_pt.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_pt.pdf).

<sup>34</sup> Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, do Comité Europeu para a Proteção de Dados, versão 1.1, 4 de maio de 2020 (a seguir designadas por «Diretrizes 05/2020»).

informações ou a possibilidade de acesso a informações já conservadas no veículo, tal como exigido em determinados casos pelo artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica. De facto, tal como referido anteriormente, o consentimento neste contexto tem de ser interpretado à luz do RGPD.

50. Em muitos casos, o utilizador pode não ter conhecimento do tratamento de dados efetuado no seu veículo. Tal falta de informação constitui um obstáculo significativo à demonstração de consentimento válido ao abrigo do RGPD, dado que o consentimento deve ser informado. Em tais circunstâncias, não é possível recorrer ao consentimento como fundamento jurídico para o correspondente tratamento de dados ao abrigo do RGPD.
51. No contexto dos veículos conectados, pode revelar-se difícil aplicar os mecanismos clássicos utilizados para obter o consentimento das pessoas, o que resulta num consentimento de «baixa qualidade» associado a falta de informações ou à impossibilidade factual de facultar um consentimento ajustado em consonância com as preferências manifestadas pelas pessoas. Na prática, pode ser igualmente difícil obter o consentimento dos condutores e dos passageiros que não estejam relacionados com o proprietário do veículo, no caso de veículos em segunda mão, alugados ou emprestados.
52. Embora a Diretiva Privacidade Eletrónica não exija o consentimento do titular dos dados, o responsável pelo tratamento tem a responsabilidade de selecionar o fundamento jurídico, ao abrigo do artigo 6.º do RGPD, que seja mais adequado a esse tratamento de dados pessoais.

### 1.5.3 Tratamento posterior dos dados pessoais

53. Quando os dados são recolhidos com base no consentimento, tal como exigido pelo artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica, ou com base numa das isenções do artigo 5.º, n.º 3, e são posteriormente tratados em conformidade com o artigo 6.º do RGPD, só podem ser objeto de tratamento posterior se o responsável pelo tratamento procurar obter consentimento adicional para essa outra finalidade, ou se o responsável pelo tratamento puder demonstrar que o consentimento se baseia no direito da União ou de um Estado-Membro, a fim de salvaguardar os objetivos referidos no artigo 23.º, n.º 1, do RGPD<sup>35</sup>. O CEPD considera que, em tais casos, o tratamento posterior com base num teste de compatibilidade em conformidade com o artigo 6.º, n.º 4, do RGPD não é possível, dado que prejudicaria o nível de proteção de dados da Diretiva Privacidade Eletrónica. De facto, o consentimento, quando é exigido pela Diretiva Privacidade Eletrónica, tem de ser específico e informado, o que significa que os titulares dos dados têm de ter conhecimento de cada uma das finalidades do tratamento de dados e ter o direito de recusar finalidades específicas<sup>36</sup>. Considerar que o tratamento posterior com base num teste de compatibilidade em conformidade com o artigo 6.º, n.º 4, do RGPD é possível constituiria uma forma de contornar o próprio princípio dos requisitos do consentimento estabelecidos pela atual diretiva.
54. O CEPD recorda que o consentimento inicial nunca legitimará o tratamento posterior, dado que, para ser válido, o consentimento tem de ser informado e específico.
55. Por exemplo, os dados de telemetria, que são recolhidos durante a utilização do veículo para fins de manutenção, não podem ser divulgados às companhias de seguro automóvel sem o consentimento dos utilizadores com o objetivo de criar perfis de condutores a fim de oferecer apólices de seguro baseadas no comportamento de condução.

---

<sup>35</sup> Ver também «Guidelines 10/2020 on restrictions under Article 23 GDPR» (Diretrizes 10/2020 relativas às limitações em conformidade com o artigo 23.º do RGPD), do Comité Europeu para a Proteção de Dados.

<sup>36</sup> Diretrizes 05/2020, pontos 3.2 e 3.3.

56. Além disso, os dados recolhidos pelos veículos conectados podem ser tratados pelas autoridades policiais a fim de detetar infrações por excesso de velocidade ou outras, se e quando forem preenchidas as condições específicas da Diretiva sobre a Proteção de Dados na Aplicação da Lei. Neste caso, tais dados serão considerados como sendo relativos a condenações penais e infrações, de acordo com as condições estabelecidas pelo artigo 10.º do RGPD e por qualquer legislação nacional aplicável. Os construtores podem facultar tais dados às autoridades policiais se forem preenchidas as condições específicas para tal tratamento. O CEPD salienta que o tratamento de dados pessoais com a única finalidade de dar resposta aos pedidos apresentados pelas autoridades policiais lei não constitui uma finalidade específica, explícita e legítima na aceção do artigo 5.º, n.º 1, alínea b), do RGPD. Quando as autoridades policiais são legalmente autorizadas, podem ser terceiros na aceção do artigo 4.º, ponto 10, do RGPD. Neste caso, os construtores teriam o direito de lhes facultar quaisquer dados à sua disposição, mediante o cumprimento do quadro jurídico aplicável em cada Estado-Membro.

#### 1.5.4 Recolha excessiva de dados

57. Com a instalação de um número crescente de sensores nos veículos conectados, existe um risco muito elevado de recolha excessiva de dados em comparação com os que são necessários para alcançar a finalidade em causa.

58. O desenvolvimento de novas funcionalidades e, mais especificamente, as que se baseiam em algoritmos de aprendizagem automática, pode exigir a recolha de uma grande quantidade de dados durante um longo período.

#### 1.5.5 Segurança dos dados pessoais

59. A pluralidade de funcionalidades, serviços e interfaces (por exemplo, Web, USB, RFID, Wi-Fi) disponibilizados pelos veículos conectados aumenta a superfície de ataque e, assim, o número de potenciais vulnerabilidades que podem comprometer os dados pessoais. Ao contrário da maioria dos dispositivos da IdC, os veículos conectados são sistemas críticos nos quais uma falha de segurança pode pôr em perigo a vida dos respetivos utilizadores e das pessoas que os rodeiam. Este facto reforça a importância de dar resposta ao risco colocado por piratas informáticos que tentam explorar as vulnerabilidades dos veículos conectados.

60. Além disso, os dados pessoais conservados nos veículos e/ou em locais externos (por exemplo, em infraestruturas de computação na nuvem) devem ser adequadamente protegidos contra o acesso não autorizado. Por exemplo, durante a manutenção, um veículo tem de ser entregue a um técnico que necessitará de acesso a alguns dados técnicos do veículo. Embora o técnico necessite de acesso aos dados técnicos, existe a possibilidade de tentar aceder a todos os dados conservados no veículo.

## 2 RECOMENDAÇÕES GERAIS

61. A fim de atenuar os riscos acima identificados para os titulares dos dados, os construtores de veículos e de equipamentos, os prestadores de serviços ou qualquer outra parte interessada que possa agir como responsável pelo tratamento ou subcontratante em relação aos veículos conectados devem seguir as recomendações gerais que se seguem.

### 2.1 Categorias de dados

62. Tal como referido na introdução, os dados associados aos veículos conectados serão considerados, na sua maioria, como dados pessoais, na medida em que seja possível associá-los a uma ou mais pessoas identificáveis. Tal inclui dados técnicos relativos às deslocações do veículo (por exemplo, a velocidade e a distância percorrida), bem como ao estado do veículo (por exemplo, a temperatura do fluido de arrefecimento do motor, a velocidade do



motor e a pressão dos pneus). Alguns dados gerados por veículos conectados podem merecer igualmente uma atenção especial, dada a sua sensibilidade e/ou potencial impacto nos direitos e interesses dos titulares dos dados. Até ao momento, o CEPD identificou três categorias de dados pessoais que merecem uma atenção especial por parte dos construtores de veículos e de equipamentos, dos prestadores de serviços e de outros responsáveis pelo tratamento: dados de localização, dados biométricos (e qualquer categoria especial de dados, na aceção do artigo 9.º do RGPD) e dados que possam revelar infrações rodoviárias e outras.

### 2.1.1 Dados de localização

63. Quando recolhem dados pessoais, os construtores de veículos e de equipamentos, os prestadores de serviços e outros responsáveis pelo tratamento devem ter em conta que os dados de localização são particularmente reveladores dos hábitos de vida dos titulares dos dados. As viagens realizadas são muito características, na medida em que permitem inferir o local de trabalho e de residência, bem como os centros de interesse (lazer) de um condutor, e podem eventualmente revelar informações sensíveis, tais como a religião, com base no local de culto, ou a orientação sexual, com base nos locais visitados. Consequentemente, o construtor do veículo e do equipamento, o prestador de serviços ou outro responsável pelo tratamento devem estar particularmente atentos a fim de não recolherem dados de localização, salvo se tal for absolutamente necessário para a finalidade do tratamento. A título de exemplo, quando o tratamento consiste na deteção da deslocação do veículo, o giroscópio é suficiente para cumprir essa função, sem que haja necessidade de recolher dados de localização.

64. Em geral, a recolha de dados de localização está igualmente sujeita ao cumprimento dos seguintes princípios:

- Z Configurar adequadamente a frequência de acesso aos dados de localização recolhidos, e o respetivo nível de pormenor, em função da finalidade do tratamento. Por exemplo, uma aplicação meteorológica não deve poder aceder à localização do veículo a cada segundo, mesmo com o consentimento do titular dos dados;
- Z Facultar informações exatas a respeito da finalidade do tratamento (por exemplo, o histórico da localização é conservado? Em caso afirmativo, qual é a sua finalidade?);
- Z Quando o tratamento se baseia no consentimento, obter consentimento válido (livre, específico e informado), distinto das condições gerais de venda ou de utilização, por exemplo no computador de bordo;
- Z Ativar a localização unicamente quando o utilizador inicia uma funcionalidade que requer que a localização do veículo seja conhecida e não por defeito e continuamente quando o automóvel é ligado;
- Z Informar o utilizador de que a localização foi ativada, em especial com recurso a ícones (por exemplo, uma seta que se desloca no ecrã);
- Z Permitir desativar a localização em qualquer altura;
- Z Definir um prazo de conservação limitado.

### 2.1.2 Dados biométricos

65. No contexto dos veículos conectados, é possível proceder ao tratamento dos dados biométricos utilizados para identificar uma pessoa de forma inequívoca, no âmbito do artigo 9.º do RGPD e das exceções a nível nacional, entre outros, a fim de permitir o acesso a um veículo, de autenticar o condutor/proprietário e/ou de permitir o acesso às definições e preferências do perfil de um condutor. Quando se considera a utilização de dados biométricos, garantir ao titular dos dados o controlo total dos seus dados implica, por um

lado, prever a existência de uma alternativa não biométrica (por exemplo, ao utilizar uma chave física ou um código) sem restrições adicionais (ou seja, a utilização da biometria não deve ser obrigatória) e, por outro lado, conservar e comparar o modelo biométrico sob forma encriptada unicamente numa base local, sem que os dados biométricos sejam tratados por um terminal de leitura/comparação externo.

66. No caso dos dados biométricos<sup>37</sup>, é importante assegurar que a solução de autenticação biométrica é suficientemente fiável, em especial cumprindo os seguintes princípios:

- Z A solução biométrica utilizada (por exemplo, a taxa de falsos positivos e de falsos negativos) é ajustada ao nível de segurança do controlo de acesso necessário;
- Z A solução biométrica utilizada baseia-se num sensor resistente a ataques (utilizando, por exemplo, uma impressão digital plana para reconhecimento de impressões digitais);
- Z O número de tentativas de autenticação é limitado;
- Z O modelo biométrico é conservado no veículo, sob forma encriptada, utilizando um algoritmo criptográfico e uma gestão de chaves de acordo com as técnicas mais avançadas;
- Z Os dados em bruto utilizados para a elaboração do modelo biométrico e para a autenticação do utilizador são tratados em tempo real sem nunca serem conservados, mesmo localmente.

### 2.1.3 Dados que revelem infrações penais ou outras

67. Quando são tratados dados relacionados com eventuais infrações penais na aceção do artigo 10.º do RGPD, o CEPD recomenda que se utilize o tratamento local dos dados, no qual o titular dos dados possui pleno controlo do tratamento em questão (ver a análise do tratamento local no ponto 2.4). De facto, salvo algumas exceções (ver o estudo de caso relativo aos estudos de acidentologia apresentado no ponto 3.3), é proibido o tratamento externo de dados que revelem infrações penais ou outras. Assim, de acordo com a sensibilidade dos dados, devem ser aplicadas fortes medidas de segurança, tais como as descritas no ponto 2.7, a fim de proporcionar proteção contra o acesso ilegítimo, a alteração e o apagamento desses dados.

68. De facto, algumas categorias de dados pessoais dos veículos conectados podem revelar que foi ou está a ser cometida uma infração penal ou outra («dados relacionados com infrações») e, por conseguinte, se aplicam limitações especiais (por exemplo, dados que indicam que o veículo transpôs uma linha contínua, a velocidade instantânea de um veículo combinada com dados exatos de localização). Em particular, se tais dados forem tratados pelas autoridades nacionais competentes para fins de investigação criminal e repressão de infrações penais, aplicar-se-ão as garantias previstas no artigo 10.º do RGPD.

## 2.2 Finalidades

69. Os dados pessoais podem ser tratados para uma grande variedade de finalidades no que respeita aos veículos conectados, incluindo a segurança do condutor, os seguros, o transporte eficiente, o entretenimento ou os serviços de informação. Nos termos do RGPD, os responsáveis pelo tratamento devem assegurar que as suas finalidades são «determinadas, explícitas e legítimas», que não são objeto de tratamento posterior incompatível com essas finalidades e que existe um fundamento jurídico válido para o tratamento posterior, tal como exigido pelo artigo 5.º do mesmo regulamento. A parte III das presentes diretrizes aborda alguns exemplos concretos de finalidades que os

---

<sup>37</sup> O princípio da proibição estabelecido no artigo 9.º, n.º 1, do RGPD refere-se unicamente a «*dados biométricos para identificar uma pessoa de forma inequívoca*».

responsáveis pelo tratamento no contexto dos veículos conectados podem prosseguir, juntamente com recomendações específicas para cada tipo de tratamento.

### 2.3 Relevância e minimização dos dados

70. A fim de cumprir o princípio da minimização dos dados<sup>38</sup>, os construtores de veículos e de equipamentos, os prestadores de serviços e outros responsáveis pelo tratamento devem dedicar especial atenção às categorias de dados de que necessitam de um veículo conectado, pois só devem recolher dados pessoais pertinentes e necessários para o tratamento. Por exemplo, os dados de localização são particularmente intrusivos e podem revelar vários hábitos de vida dos titulares dos dados. Consequentemente, os participantes do setor devem estar particularmente atentos a fim de não recolherem dados de localização, salvo se tal for absolutamente necessário para a finalidade do tratamento (ver a análise dos dados de localização no ponto 2.1 *supra*).

### 2.4 Proteção de dados desde a conceção e por defeito

71. Tendo em conta o volume e a diversidade dos dados pessoais gerados pelos veículos conectados, o CEPD observa que os responsáveis pelo tratamento são obrigados a assegurar que as tecnologias utilizadas no contexto dos veículos conectados são configuradas de modo a respeitar a privacidade das pessoas, aplicando as obrigações em matéria de proteção de dados desde a conceção e por defeito estabelecidas no artigo 25.º do RGPD. As tecnologias devem ser concebidas a fim de minimizar a recolha de dados pessoais, facultar predefinições que protejam a privacidade e assegurar que os titulares dos dados são bem informados e têm a opção de alterar facilmente as configurações associadas aos seus dados pessoais. Os construtores terceiros de aplicações e o setor beneficiariam de diretrizes específicas a respeito da forma como os construtores e os prestadores de serviços podem cumprir a proteção de dados desde a conceção e por defeito.

72. Determinadas práticas gerais, descritas abaixo, podem igualmente ajudar a atenuar os riscos que os veículos conectados implicam para os direitos e liberdades das pessoas singulares<sup>39</sup>.

#### 2.4.1 Tratamento local dos dados pessoais

73. Em geral, os construtores de veículos e de equipamentos, os prestadores de serviços e outros responsáveis pelo tratamento devem, sempre que possível, utilizar processos que não envolvam dados pessoais nem a transferência de dados pessoais para o exterior do veículo (ou seja, os dados são tratados internamente). Todavia, a natureza dos veículos conectados apresenta riscos, tais como a possibilidade de ataques ao tratamento local por intervenientes externos ou a fuga de dados locais através da venda de peças do veículo. Por conseguinte, importa ponderar medidas adequadas de deteção e segurança para assegurar que o tratamento local permanece local. Este cenário proporciona a vantagem de assegurar ao utilizador o controlo exclusivo e total dos seus dados pessoais e, como tal, apresenta, «desde a conceção», menos riscos de privacidade, especialmente porque proíbe qualquer tratamento de dados por partes interessadas sem o conhecimento do titular dos dados. Além disso, permite o tratamento de dados sensíveis, como dados biométricos ou dados relativos a infrações penais ou outras, bem como de dados de localização pormenorizados que, de outra forma, estariam sujeitos a regras mais rigorosas (ver abaixo). No mesmo sentido, apresenta menos riscos em matéria de cibersegurança e implica pouca latência, o que o torna especialmente adequado para funções de assistência automatizada ao condutor. Seguem-se alguns exemplos possíveis deste tipo de solução:

---

<sup>38</sup> Artigo 5.º, n.º 1, alínea c), do RGPD.

<sup>39</sup> Ver igualmente as [Orientações 4/2019 relativas ao artigo 25.º – Proteção de Dados desde a Conceção e por Defeito, do Comité Europeu para a Proteção de Dados](#), versão 2.0, adotadas em 20 de outubro de 2020 (a seguir designadas por «Orientações 4/2019»).

- Z Aplicações de condução ecológica que tratam os dados no veículo, a fim de disponibilizar aconselhamento ao nível da condução ecológica em tempo real no ecrã de bordo;
  - Z Aplicações que implicam uma transferência de dados pessoais para um dispositivo, tal como um telemóvel inteligente, sob o controlo total do utilizador (por exemplo, através de Bluetooth ou de Wi-Fi) e em que os dados do veículo não são transmitidos aos fornecedores da aplicação nem aos construtores do veículo; tal incluiria, por exemplo, o emparelhamento de telemóveis inteligentes a fim de utilizar o ecrã do automóvel, os sistemas multimédia, o microfone (ou outros sensores) para chamadas telefónicas, etc., na medida em que os dados recolhidos permaneçam sob o controlo do titular dos dados e sejam exclusivamente utilizados para prestar o serviço que este solicitou;
  - Z Aplicações que reforçam a segurança a bordo, tais como as que emitem sinais sonoros ou vibrações do volante quando um condutor ultrapassa um automóvel sem a devida sinalização ou pisa linhas contínuas, ou que apresentam avisos a respeito do estado do veículo (por exemplo, um aviso relativo ao desgaste das pastilhas dos travões);
  - Z Aplicações para desbloquear, iniciar e/ou ativar determinados comandos do veículo que utilizem os dados biométricos do condutor conservados no interior do veículo (tais como modelos de rosto ou de voz ou minúcias de impressões digitais).
74. As aplicações como as anteriormente referidas implicam um tratamento para o desempenho de atividades exclusivamente pessoais por uma pessoa singular (ou seja, sem a transferência de dados pessoais para um responsável pelo tratamento ou subcontratante). Por conseguinte, nos termos do artigo 2.º, n.º 2, do RGPD, **estas aplicações não se enquadram no âmbito de aplicação do RGPD.**
75. Todavia, se o RGPD não se aplicar ao tratamento de dados pessoais por uma pessoa singular no decurso de uma atividade exclusivamente pessoal ou doméstica, aplica-se aos responsáveis pelo tratamento ou aos subcontratantes que disponibilizam os meios de tratamento de dados pessoais para essas atividades pessoais ou domésticas (construtores de automóveis, prestadores de serviços, etc.), de acordo com o considerando 18 do RGPD. Assim, quando agem na qualidade de responsável pelo tratamento ou de subcontratante, devem desenvolver uma aplicação segura a bordo e no devido respeito pelo princípio da privacidade desde a conceção e por defeito. Em qualquer caso, de acordo com o considerando 78 do RGPD *«no contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados»*<sup>40</sup>. Por um lado, reforçará o desenvolvimento de serviços centrados no utilizador e, por outro lado, facilitará e garantirá que quaisquer utilizações adicionais no futuro possam ser enquadradas no âmbito de aplicação do RGPD. Mais especificamente, o CEPD recomenda o desenvolvimento de uma plataforma de aplicação segura a bordo, fisicamente separada de funções de segurança relevantes do automóvel, a fim de que o acesso aos dados do automóvel não dependa de capacidades desnecessárias de nuvens externas.
76. Sempre que possível, o tratamento local de dados deve ser tido em consideração pelos construtores de automóveis e pelos prestadores de serviços, a fim de atenuar os potenciais

---

<sup>40</sup> Para mais recomendações relativas à privacidade desde a conceção e por defeito, ver igualmente as Orientações 4/2019.

riscos do tratamento em nuvem, tal como sublinhados no parecer relativo a computação em nuvem, do Grupo de Trabalho do Artigo 29.<sup>o</sup><sup>41</sup>.

77. Em geral, os utilizadores devem poder controlar a forma como os seus dados são recolhidos e tratados no veículo:

- Z As informações relativas ao tratamento devem ser apresentadas na língua do condutor (manual, definições, etc.);
- Z O CEPD recomenda que o tratamento por defeito contemple apenas os dados estritamente necessários ao funcionamento do veículo. Os titulares dos dados devem ter a possibilidade de ativar ou desativar o tratamento de dados para cada uma das finalidades e dos responsáveis pelo tratamento/subcontratantes e ter a possibilidade de apagar os dados em questão, tendo em conta a finalidade e o fundamento jurídico do tratamento de dados;
- Z Os dados não devem ser transmitidos a terceiros (ou seja, o utilizador possui o acesso exclusivo aos dados);
- Z Os dados devem ser conservados unicamente durante o tempo necessário para a prestação do serviço ou consoante exigido pelo direito da União ou dos Estados-Membros;
- Z Os titulares dos dados devem poder apagar permanentemente quaisquer dados pessoais antes de os veículos serem colocados à venda;
- Z Sempre que possível, os titulares dos dados devem ter acesso direto aos dados gerados por estas aplicações.

78. Finalmente, embora nem sempre seja possível recorrer ao tratamento local de dados para cada caso de utilização, é frequentemente possível implementar o «tratamento híbrido». Por exemplo, no contexto do seguro baseado na utilização, os dados pessoais relativos ao comportamento de condução (tais como a força exercida no pedal do travão, a quilometragem percorrida, etc.) poderiam ser tratados no interior do veículo ou pelo prestador de serviços de telemática por conta da companhia de seguros (o subcontratante), a fim de gerar pontuações numéricas que são transferidas para a companhia de seguros numa base definida (por exemplo, mensalmente). Desta forma, a companhia de seguros não obtém acesso aos dados comportamentais em bruto, mas apenas à pontuação agregada que resulta do tratamento. Tal assegura que os princípios da minimização dos dados são cumpridos desde a conceção. Significa igualmente que os utilizadores têm de poder exercer os seus direitos quando os dados são conservados por outras partes: por exemplo, um utilizador deve poder apagar os dados conservados nos sistemas de uma oficina de manutenção ou de um concessionário de automóveis, de acordo com as condições estabelecidas no artigo 17.<sup>o</sup> do RGPD.

#### 2.4.2 Anonimização e pseudonimização

79. Se estiver prevista a transmissão de dados pessoais para o exterior do veículo, deve ser tida em consideração a possibilidade de os anonimizar previamente à transmissão. Aquando da anonimização, o responsável pelo tratamento deve ter em conta todos os tratamentos envolvidos que possam eventualmente resultar na reidentificação dos dados, tais como a transmissão de dados anonimizados localmente. O CEPD recorda que os princípios da proteção de dados não se aplicam às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável, nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja identificável ou já não possa ser identificado<sup>42</sup>. Quando um conjunto de dados se encontra verdadeiramente

---

<sup>41</sup> Parecer 5/2012 relativo a computação em nuvem, do Grupo de Trabalho do Artigo 29.<sup>o</sup>, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196\\_pt.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_pt.pdf).

<sup>42</sup> Ver artigo 4.<sup>o</sup>, ponto 1, e considerando 26 do RGPD.

anonimizado e as pessoas deixam de ser identificáveis, a legislação europeia de proteção de dados deixa de ser aplicável. Consequentemente, a anonimização, quando for relevante, pode ser uma boa estratégia para manter os benefícios e atenuar os riscos relativos aos veículos conectados.

80. Tal como descrito no parecer do Grupo de Trabalho do Artigo 29.º sobre técnicas de anonimização, podem ser utilizados vários métodos – por vezes combinados – a fim de alcançar a anonimização dos dados<sup>43</sup>.

81. Outras técnicas, como a pseudonimização<sup>44</sup>, podem ajudar a minimizar os riscos gerados pelo tratamento de dados, tendo em conta que, na maioria dos casos, os dados diretamente identificáveis não são necessários para alcançar a finalidade do tratamento. A pseudonimização, se for reforçada por garantias em matéria de segurança, melhora a proteção dos dados pessoais ao reduzir os riscos de utilização abusiva. A pseudonimização é reversível, ao contrário da anonimização, e os dados pseudonimizados são considerados como dados pessoais sujeitos ao RGPD.

#### 2.4.3 Avaliações de impacto sobre a proteção de dados

82. Dada a escala e a sensibilidade dos dados pessoais que podem ser gerados através dos veículos conectados, é provável que o tratamento – especialmente em situações nas quais os dados pessoais são tratados no exterior do veículo – resulte frequentemente num risco elevado para os direitos e liberdades das pessoas. Neste caso, os participantes do setor serão obrigados a realizar uma avaliação de impacto sobre a proteção de dados (AIPD) a fim de identificar e atenuar os riscos, tal como descrito nos artigos 35.º e 36.º do RGPD. Mesmo nos casos nos quais não é necessária uma AIPD, é uma boa prática realizá-la o mais cedo possível no processo de conceção, o que permitirá que os participantes do setor tenham em conta os resultados desta análise nas suas opções de conceção previamente à implantação de novas tecnologias.

#### 2.5 Informação

83. Previamente ao tratamento de dados pessoais, o titular dos dados deve ser informado da identidade do responsável pelo tratamento (por exemplo, o construtor do veículo e do equipamento ou o prestador de serviços), da finalidade do tratamento, dos destinatários dos dados, do prazo de conservação dos dados e dos direitos do titular dos dados ao abrigo do RGPD<sup>45</sup>.

84. Além disso, o construtor do veículo e do equipamento, o prestador de serviços ou outro responsável pelo tratamento deve igualmente facultar ao titular dos dados as informações que se seguem, de uma forma facilmente acessível e formuladas numa linguagem clara e simples:

- Z Os contactos do encarregado da proteção de dados;
- Z As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- Z A menção explícita dos interesses legítimos do responsável pelo tratamento dos dados ou de um terceiro, quando tais interesses legítimos constituam o fundamento jurídico para o tratamento;

---

<sup>43</sup> Parecer 05/2014 sobre técnicas de anonimização, do Grupo de Trabalho do Artigo 29.º, [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_pt.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf).

<sup>44</sup> Artigo 4.º, ponto 5, do RGPD. Relatório da ENISA, de 3 de dezembro de 2019, <https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>.

<sup>45</sup> Artigo 5.º, n.º 1, alínea a), e artigo 13.º do RGPD. Ver também as [Orientações relativas à transparência na aceção do Regulamento 2016/679 \(WP 260 rev.01\)](#), do Grupo de Trabalho do Artigo 29.º, aprovadas pelo CEPD.

- Z Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
- Z Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
- Z A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
- Z A existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado, se o tratamento se basear no consentimento;
- Z Se aplicável, o facto de o responsável pelo tratamento pretender transferir dados pessoais para um país terceiro ou para uma organização internacional e as garantias utilizadas para os transferir;
- Z Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;
- Z A existência de decisões automatizadas, incluindo a definição de perfis que produza efeitos na esfera jurídica do titular dos dados ou que o afete significativamente de forma similar, e informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados. Tal poderá aplicar-se, em especial, à disponibilização às pessoas de seguros baseados na utilização;
- Z O direito de apresentar reclamação a uma autoridade de controlo;
- Z Informações a respeito do tratamento posterior;
- Z No caso de controlo conjunto dos dados, informações claras e completas a respeito das responsabilidades de cada responsável pelo tratamento.

85. Em alguns casos, os dados pessoais não são recolhidos diretamente junto da pessoa em questão. Por exemplo, um construtor de veículos e de equipamentos pode recorrer a um concessionário a fim de recolher informações a respeito do proprietário do veículo, de modo a prestar um serviço de assistência em viagem. Se os dados não forem recolhidos diretamente, o construtor do veículo e do equipamento, o prestador de serviços ou outro responsável pelo tratamento deve, além das informações acima referidas, indicar igualmente as categorias de dados pessoais em questão, a origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público. Tais informações devem ser facultadas pelo responsável pelo tratamento num prazo razoável após a obtenção dos dados e, **o mais tardar, na data que ocorrer primeiro entre as que se seguem**, em conformidade com o artigo 14.º, n.º 3, do RGPD: i) um mês após a obtenção dos dados, tendo em conta as circunstâncias específicas nas quais os dados pessoais forem tratados, ii) na primeira comunicação com o titular dos dados, ou iii) se esses dados forem transmitidos a um terceiro, antes da transmissão dos dados.

86. Poderá ser igualmente necessário facultar novas informações aos titulares dos dados, quando os dados forem tratados por um novo responsável pelo tratamento. É possível que um serviço de assistência em viagem que interaja com os veículos conectados seja prestado por diferentes responsáveis pelo tratamento, dependendo do país ou da região em que a assistência é necessária. Os novos responsáveis pelo tratamento devem facultar aos titulares dos dados as informações necessárias quando os titulares dos dados atravessam

fronteiras e os serviços que interagem com veículos conectados são prestados por novos responsáveis pelo tratamento.

87. As informações destinadas aos titulares dos dados podem ser facultadas por meio de uma abordagem estruturada<sup>46</sup>, ou seja, separando dois níveis de informação: por um lado, informações de primeiro nível, que são as mais importantes para os titulares dos dados, e, por outro lado, informações que, em princípio, são importantes numa fase posterior. As informações essenciais de primeiro nível incluem, além da identidade do responsável pelo tratamento, a finalidade do tratamento e uma descrição dos direitos do titular dos dados, bem como informações adicionais a respeito do tratamento com maior impacto no titular dos dados e do tratamento que o possa surpreender. O CEPD recomenda que, no contexto dos veículos conectados, o titular dos dados seja informado de todos os destinatários do primeiro nível de informações. Tal como indicado nas orientações do Grupo de Trabalho do Artigo 29.º relativas à transparência, os responsáveis pelo tratamento devem facultar informações relativas aos destinatários que sejam mais significativas para os titulares dos dados. Na prática, trata-se em geral de identificar os destinatários para que os titulares dos dados saibam exatamente quem tem os seus dados pessoais. Caso os responsáveis pelo tratamento não possam facultar os nomes dos destinatários, as informações devem ser tão específicas quanto possível, indicando o tipo de destinatário (ou seja, fazendo referência às atividades que este realiza), a indústria, o setor e o subsetor, bem como a localização dos destinatários.
88. Os titulares dos dados podem ser informados por meio de cláusulas concisas e facilmente compreensíveis no contrato de venda do veículo, no contrato de prestação de serviços e/ou em qualquer suporte escrito, utilizando documentos distintos (por exemplo, o manual ou o livro de registo de manutenção do veículo) ou o computador de bordo.
89. Além das informações necessárias, podem ser utilizados ícones normalizados, tal como exigido nos artigos 13.º e 14.º do RGPD, a fim de melhorar a transparência, eventualmente reduzindo a necessidade de apresentação de grandes quantidades de informações escritas ao titular dos dados. Devem ser visíveis nos veículos a fim de proporcionar, em relação ao tratamento previsto, uma boa visão geral que seja compreensível e claramente legível. O CEPD sublinha a importância da normalização desses ícones, a fim de que o utilizador visualize os mesmos símbolos independentemente da marca ou do modelo do veículo. Por exemplo, quando determinados tipos de dados estão a ser recolhidos, tais como dados de localização, os veículos podem possuir um sinal evidente a bordo (tal como uma luz no interior do veículo) a fim de informar os passageiros a respeito da recolha de dados.

## 2.6 Direitos do titular dos dados

90. Os construtores de veículos e de equipamentos, os prestadores de serviços e outros responsáveis pelo tratamento devem facilitar o controlo dos dados pelos seus titulares durante todo o período do tratamento, por meio da implementação de ferramentas específicas que proporcionem uma forma eficaz de exercerem os seus direitos, em especial os seus direitos de acesso, de retificação e de apagamento, o seu direito de restringir o tratamento e, dependendo do fundamento jurídico do tratamento, o seu direito à portabilidade dos dados e o seu direito de oposição.
91. A fim de facilitar as alterações de definições, deve ser implementado um sistema de gestão de perfis, de modo a conservar as preferências dos condutores conhecidos e de os ajudar a alterar facilmente as suas definições de privacidade em qualquer altura. O sistema de gestão de perfis deve centralizar todas as definições de dados para cada tratamento de dados, especialmente a fim de facilitar o acesso, o apagamento, a remoção e a portabilidade de

---

<sup>46</sup> Ver as Orientações relativas à transparência na aceção do Regulamento 2016/679 (WP 260 rev.01), do Grupo de Trabalho do Artigo 29.º, aprovadas pelo CEPD.



dados pessoais dos sistemas dos veículos a pedido do titular dos dados. Os condutores devem poder interromper a recolha de determinados tipos de dados, temporária ou permanentemente, a qualquer momento, salvo se existir um fundamento jurídico específico ao qual o responsável pelo tratamento possa recorrer a fim de continuar a recolha de dados específicos. Consequentemente, no caso de um contrato que contenha uma oferta personalizada baseada no comportamento de condução, tal pode implicar que o utilizador regresse às condições normalizadas desse contrato. Estas funcionalidades devem ser implementadas no interior do veículo, embora possam ser igualmente disponibilizadas aos titulares dos dados por meios adicionais (por exemplo, aplicação específica). Além disso, a fim de permitir aos titulares dos dados removerem rápida e facilmente os dados pessoais que possam estar conservados no painel de instrumentos do automóvel (por exemplo, histórico de navegação por GPS, navegação na Web, etc.), o CEPD recomenda que os construtores disponibilizem uma funcionalidade simples (tal como um botão para eliminar).

92. A venda de um veículo conectado e a consequente mudança de proprietário devem igualmente desencadear o apagamento de quaisquer dados pessoais que já não sejam necessários para as finalidades anteriormente especificadas e o titular dos dados deve poder exercer o seu direito à portabilidade.

## 2.7 Segurança

93. Os construtores de veículos e de equipamentos, os prestadores de serviços e outros responsáveis pelo tratamento devem adotar medidas que garantam a segurança e a confidencialidade dos dados tratados e tomar todas as precauções úteis para evitar que uma pessoa não autorizada assuma o controlo. Em especial, os participantes do setor devem ponderar a adoção das seguintes medidas:

- Z Encriptar os canais de comunicação por meio de um algoritmo avançado;
- Z Implementar um sistema de gestão de chaves de encriptação que seja único para cada veículo, não para cada modelo;
- Z Se forem conservados à distância, encriptar os dados por meio de algoritmos avançados;
- Z Renovar regularmente as chaves de encriptação;
- Z Proteger as chaves de encriptação contra qualquer divulgação;
- Z Autenticar os dispositivos de receção de dados;
- Z Assegurar a integridade dos dados (por exemplo, por meio de dispersão);
- Z Sujeitar o acesso aos dados pessoais a técnicas fiáveis de autenticação do utilizador (palavra-passe, certificado eletrónico, etc.).

94. No que respeita, mais concretamente, aos construtores de veículos, o CEPD recomenda a implementação das seguintes medidas de segurança:

- Z Separar as funções vitais do veículo das funções que se baseiam sempre em capacidades de telecomunicação (por exemplo, a «ludoinformação»);
- Z Implementar medidas técnicas que permitam aos construtores de veículos corrigir rapidamente as vulnerabilidades de segurança durante toda a vida útil do veículo;
- Z Quanto às funções vitais do veículo, dar prioridade, tanto quanto possível, à utilização de meios de comunicação seguros que sejam especificamente dedicados ao transporte;

- Z Criar um sistema de alarme em caso de ataque aos sistemas do veículo, com a possibilidade de funcionamento em modo reduzido<sup>47</sup>;
  - Z Conservar um histórico de registo de qualquer acesso ao sistema de informações do veículo, por exemplo, retrocedendo seis meses como período máximo, a fim de permitir a compreensão da origem de qualquer potencial ataque, e realizar periodicamente uma análise das informações registadas para detetar eventuais anomalias.
95. As presentes recomendações gerais devem ser complementadas por requisitos específicos que tenham em conta as características e a finalidade de cada tratamento de dados.

## 2.8 Transmissão de dados pessoais para terceiros

96. Em princípio, apenas o responsável pelo tratamento e o titular dos dados têm acesso aos dados gerados por um veículo conectado. Todavia, o responsável pelo tratamento pode transmitir dados pessoais a um parceiro comercial (destinatário), na medida em que tal transmissão recorra licitamente a um dos fundamentos jurídicos enunciados no artigo 6.º do RGPD.
97. Tendo em conta a eventual sensibilidade dos dados de utilização do veículo (por exemplo, viagens realizadas e estilo de condução), o CEPD recomenda que o consentimento do titular dos dados seja sistematicamente obtido previamente à transmissão dos respetivos dados para um parceiro comercial que atue como responsável pelo tratamento (por exemplo, ao assinalar uma opção que não esteja pré-assinalada, ou, quando tecnicamente possível, ao utilizar um dispositivo físico ou lógico ao qual a pessoa possa aceder a partir do veículo). O parceiro comercial, por sua vez, torna-se responsável pelos dados que recebe e está sujeito a todas as disposições do RGPD.
98. O construtor do veículo, o prestador de serviços ou outro responsável pelo tratamento pode transmitir dados pessoais a um subcontratante selecionado para desempenhar um papel na prestação do serviço ao titular dos dados, desde que o subcontratante não utilize esses dados para as suas próprias finalidades. Os responsáveis pelo tratamento e os subcontratantes devem redigir um contrato ou outro documento legal que especifique as obrigações de cada parte e explicita as disposições do artigo 28.º do RGPD.

## 2.9 Transferência de dados pessoais para fora da UE/EEE

99. Quando os dados pessoais são transferidos para fora do Espaço Económico Europeu, são previstas garantias especiais para assegurar que a proteção correspondente acompanha esses dados.
100. Consequentemente, o responsável pelo tratamento só pode transferir dados pessoais para um destinatário na medida em que tal transferência cumpra os requisitos estabelecidos no capítulo V do RGPD.

---

<sup>47</sup> O modo reduzido é um modo de funcionamento do veículo que assegura que as funções essenciais para o funcionamento seguro do veículo (ou seja, os requisitos mínimos de segurança) estariam garantidas, mesmo que outras funcionalidades menos importantes fossem desativadas (por exemplo, o funcionamento do dispositivo de geo-orientação pode ser considerado como não essencial, ao contrário do sistema de travagem).

## 2.10 Utilização de tecnologias Wi-Fi a bordo

101. Os avanços na tecnologia celular possibilitaram a fácil utilização da Internet em viagem. Embora seja possível obter conectividade Wi-Fi num veículo por meio de um ponto de acesso à Internet sem fios de um telemóvel inteligente ou de um dispositivo dedicado (*dongle* OBD-II, *modem* ou encaminhador sem fios, etc.), atualmente a maioria dos construtores disponibiliza modelos que incluem uma ligação de dados celulares incorporada e têm igualmente a capacidade de criar redes Wi-Fi. Consoante o caso, devem ser tidos em consideração vários aspetos:

ZA conectividade Wi-Fi é disponibilizada como um serviço por um condutor profissional, por exemplo um taxista aos seus clientes. Neste caso, o profissional ou a respetiva empresa poderá ser considerado como um fornecedor de serviços Internet, estando assim sujeito a obrigações e limitações específicas no que respeita ao tratamento dos dados pessoais dos seus clientes;

ZA conectividade Wi-Fi é implementada para utilização exclusiva do condutor (a critério do condutor e dos seus passageiros). Neste caso, o tratamento de dados pessoais é considerado como uma atividade exclusivamente pessoal ou doméstica, nos termos do artigo 2.º, n.º 2, alínea c), e do considerando 18 do RGPD.

102. Em geral, a proliferação de interfaces de ligação à Internet por Wi-Fi implica riscos acrescidos para a privacidade das pessoas. De facto, através dos seus veículos, os utilizadores tornam-se emissores contínuos e, por conseguinte, podem ser identificados e seguidos. A fim de evitar o seguimento, os construtores do veículo e do equipamento devem implementar opções de exclusão de fácil utilização que impeçam a recolha do identificador do conjunto de serviço (SSID) da rede Wi-Fi a bordo.

## 3 ESTUDOS DE CASOS

103. A presente secção aborda cinco exemplos específicos de tratamento no contexto dos veículos conectados, correspondentes a cenários que podem ser encontrados no setor pelas partes interessadas. Os exemplos abrangem o tratamento de dados que requer um poder de cálculo impossível de mobilizar localmente no veículo e/ou o envio de dados pessoais para terceiros a fim de realizar análises mais aprofundadas ou disponibilizar mais funcionalidades à distância. O presente documento especifica as finalidades pretendidas, as categorias de dados recolhidos, o prazo de conservação de tais dados, os direitos dos titulares dos dados, as medidas de segurança a implementar e os destinatários das informações para cada tipo de tratamento. Caso alguns destes campos não sejam descritos a seguir, aplicam-se as recomendações gerais descritas na parte anterior.
104. Os exemplos selecionados não são exaustivos e destinam-se a exemplificar a variedade de tipos de tratamento, de fundamentos jurídicos, de intervenientes, etc., que possam estar envolvidos no contexto dos veículos conectados.

### 3.1 Prestação de um serviço por um terceiro

105. Os titulares dos dados podem contratar um prestador de serviços para obter serviços de valor acrescentado relacionados com o seu veículo. Por exemplo, um titular de dados pode celebrar um contrato de seguro baseado na utilização que ofereça prémios de seguro reduzidos em função da quilometragem ou do bom comportamento de condução, o que requer a monitorização dos hábitos de condução por parte da companhia de seguros. Um titular de dados pode igualmente contratar uma empresa que disponibilize assistência em viagem no caso de avarias, o que implica a transmissão da localização do veículo à empresa, ou pode contratar um prestador de serviços a fim de receber mensagens ou alertas

relacionados com o funcionamento do veículo (por exemplo, um alerta a respeito do estado de desgaste dos travões, ou um lembrete da data da inspeção técnica).

### 3.1.1 Seguro baseado na utilização

106. O seguro em função da quilometragem é um tipo de seguro baseado na utilização que faz o seguimento da quilometragem do veículo e/ou dos hábitos de condução do condutor a fim de distinguir e recompensar os condutores «seguros», concedendo-lhes prémios mais reduzidos. A seguradora exigirá ao condutor que instale um serviço de telemática incorporado ou uma aplicação móvel, ou que ative um módulo incorporado de fabrico que faça o seguimento da quilometragem percorrida e/ou do comportamento de condução (padrão de travagem, aceleração rápida, etc.) do tomador do seguro. As informações recolhidas pelo dispositivo telemático serão utilizadas para atribuir pontuações ao condutor, de modo a analisar os riscos que este pode representar para a companhia de seguros.
107. Dado que o seguro baseado na utilização requer o consentimento ao abrigo do artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica, o CEPD sublinha que tem de ser dada a opção ao tomador do seguro de subscrever uma apólice de seguro que não se baseie na utilização. Caso contrário, não se poderia considerar que o consentimento fosse livre, dado que a execução do contrato estaria condicionada ao consentimento. Além disso, o artigo 7.º, n.º 3, do RGPD exige que o titular dos dados tenha o direito de retirar o consentimento.

#### 3.1.1.1 Fundamento jurídico

108. Quando os dados são recolhidos por meio de um serviço de comunicações eletrónicas publicamente disponível (por exemplo, através do cartão SIM contido no dispositivo telemático), será necessário consentimento para obter acesso às informações já conservadas no veículo, tal como previsto no artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica. De facto, neste contexto, não é possível aplicar nenhuma das isenções previstas nas disposições em causa: o tratamento não tem a finalidade exclusiva de efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, nem se refere a um serviço da sociedade da informação explicitamente solicitado pelo assinante ou utilizador. O consentimento pode ser obtido no momento da celebração do contrato.
109. No que respeita ao tratamento de dados pessoais após a conservação ou o acesso ao equipamento terminal do utilizador final, a companhia de seguros pode recorrer ao artigo 6.º, n.º 1, alínea b), do RGPD neste contexto específico, desde que possa estabelecer que o tratamento se realiza no contexto de um contrato válido celebrado com o titular dos dados e que o tratamento é necessário para que o contrato específico com o titular dos dados seja executado. Na medida em que o tratamento seja objetivamente necessário para a execução do contrato com o titular dos dados, o CEPD considera que recorrer ao artigo 6.º, n.º 1, alínea b), do RGPD não diminuiria, neste caso específico, a proteção adicional proporcionada pelo artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica. Esse fundamento jurídico é concretizado pelo titular dos dados ao assinar um contrato com a companhia de seguros.

#### 3.1.1.2 Dados recolhidos

110. Existem dois tipos de dados pessoais a ter em consideração:
  - Z **Dados comerciais e transacionais:** informações de identificação do titular dos dados, dados relativos às transações, dados relativos aos meios de pagamento, etc.;
  - Z **Dados de utilização:** dados pessoais gerados pelo veículo, hábitos de condução, localização, etc.
111. O CEPD recomenda que, na medida do possível, e dado que existe o risco de os dados recolhidos através da caixa telemática serem utilizados abusivamente a fim de criar um

perfil exato das deslocações do condutor, os dados em bruto relativos ao comportamento de condução sejam tratados:

- Z No interior do veículo, em caixas telemáticas, ou no telemóvel inteligente do utilizador, para que a seguradora aceda unicamente aos dados dos resultados (por exemplo, uma pontuação relativa aos hábitos de condução) e não aos dados em bruto pormenorizados (ver ponto 2.1);
  - Z Ou pelo prestador de serviços de telemática por conta do responsável pelo tratamento (a companhia de seguros) a fim de gerar pontuações numéricas que são transferidas para a companhia de seguros numa base definida. Neste caso, os dados em bruto e os dados diretamente relacionados com a identidade do condutor têm de ser separados. Tal significa que o prestador de serviços de telemática recebe os dados em tempo real, mas não sabe os nomes, as matrículas, etc., dos tomadores dos seguros. Por outro lado, a seguradora sabe os nomes dos tomadores dos seguros, mas recebe unicamente as pontuações e o total de quilómetros e não os dados em bruto utilizados para gerar tais pontuações.
112. Além disso, importa salientar que se a quilometragem for necessária apenas para a execução do contrato, os dados de localização não devem ser recolhidos.

#### 3.1.1.3 *Prazo de conservação*

113. No contexto do tratamento de dados que ocorra para efeitos de execução de um contrato (ou seja, prestação de um serviço), importa distinguir entre dois tipos de dados antes de definir os respetivos prazos de conservação:
- Z **Dados comerciais e transacionais:** podem ser conservados numa base de dados ativa durante toda a vigência do contrato. No final do contrato, podem ser arquivados de modo físico (num suporte separado: DVD, etc.) ou lógico (por gestão de autorização) para o caso de eventual litígio. Posteriormente, no termo do prazo de prescrição legal, os dados são apagados ou anonimizados;
  - Z **Dados de utilização:** podem ser classificados como dados em bruto e como dados agregados. Tal como referido anteriormente, os responsáveis pelo tratamento e os subcontratantes não devem tratar dados em bruto, se possível. Se forem necessários, os dados em bruto devem ser conservados unicamente enquanto forem necessários para gerar os dados agregados e verificar a validade desse processo de agregação. Os dados agregados devem ser conservados durante o tempo necessário para a prestação do serviço ou consoante exigido pelo direito da União ou dos Estados-Membros.

#### 3.1.1.4 *Informações a facultar aos titulares dos dados e respetivos direitos*

114. Previamente ao tratamento de dados pessoais, o titular dos dados deve ser informado em conformidade com o artigo 13.º do RGPD, de uma forma transparente e compreensível. Em especial, deve ser informado do prazo de conservação dos dados pessoais ou, se não for possível, dos critérios usados para fixar esse prazo. Neste último caso, o CEPD recomenda a adoção de uma abordagem pedagógica, a fim de salientar a diferença entre os dados em bruto e a pontuação gerada nesta base, realçando, se for o caso, que a seguradora recolherá apenas o resultado da pontuação, sempre que for adequado.
115. Quando os dados não são tratados no interior do veículo, mas sim por um prestador de telemática por conta do responsável pelo tratamento (a companhia de seguros), poderá ser útil mencionar nas informações que, neste caso, o prestador não terá acesso aos dados diretamente relacionados com a identidade do condutor (tais como nomes, matrículas, etc.). Além disso, tendo em consideração a importância de informar os titulares dos dados a respeito das consequências do tratamento dos seus dados pessoais e o facto de que os titulares dos dados não devem ser surpreendidos pelo tratamento dos seus dados pessoais, o CEPD recomenda que os titulares dos dados sejam informados da existência de perfis e

das consequências de tais perfis, mesmo que não envolvam qualquer decisão automatizada, tal como referido no artigo 22.º do RGPD.

116. No que respeita aos direitos dos titulares dos dados, estes devem ser especificamente informados a respeito dos meios disponíveis para exercerem os seus direitos de acesso, de retificação, de limitação e de apagamento. Uma vez que os dados recolhidos neste contexto são facultados pelo titular dos dados (por meio de formulários específicos ou da sua atividade) e tratados com base no artigo 6.º, n.º 1, alínea b) (execução de um contrato), do RGPD, o titular dos dados está habilitado a exercer o seu direito à portabilidade dos dados. Tal como referido nas orientações sobre o direito à portabilidade dos dados, o CEPD recomenda vivamente «que os responsáveis pelo tratamento expliquem claramente a diferença entre os tipos de dados que um titular de dados pode receber no âmbito dos direitos de acesso e de portabilidade dos dados»<sup>48</sup>.
117. As informações podem ser facultadas no momento da assinatura do contrato.

#### 3.1.1.5 *Destinatário:*

118. O CEPD recomenda que, na medida do possível, os dados de utilização do veículo sejam tratados diretamente em caixas telemáticas, para que a seguradora aceda unicamente aos dados dos resultados (por exemplo, uma pontuação) e não aos dados em bruto pormenorizados.
119. Se um prestador de serviços de telemática recolher os dados por conta do responsável pelo tratamento (a companhia de seguros) a fim de gerar pontuações numéricas, não precisa de saber a identidade do condutor (nomeadamente nomes, matrículas, etc.) que é tomador do seguro.

#### 3.1.1.6 *Segurança:*

120. Aplicam-se as recomendações gerais. Ver ponto 2.7.

### 3.1.2 *Alugar e reservar um parque de estacionamento*

121. O proprietário de um parque de estacionamento pode querer alugá-lo. Para tal, identifica um lugar e estabelece um preço para o mesmo numa aplicação Web. Em seguida, uma vez identificado o lugar de estacionamento, a aplicação notifica o proprietário quando um condutor quiser reservá-lo. O condutor pode selecionar um destino e verificar os lugares de estacionamento disponíveis com base em vários critérios. Após a aprovação do proprietário, a transação é confirmada e o prestador de serviços trata da transação de pagamento e, posteriormente, utiliza a navegação para conduzir até ao local.

#### 3.1.2.1 *Fundamento jurídico*

122. Quando os dados são recolhidos por meio de um serviço de comunicações eletrónicas publicamente disponível, aplica-se o artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica.
123. Dado que se trata de um serviço da sociedade da informação, o artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica não exige o consentimento para a possibilidade de acesso a informações já conservadas no veículo quando tal serviço é explicitamente solicitado pelo assinante.
124. O artigo 6.º, n.º 1, alínea b), do RGPD será o fundamento jurídico para o tratamento de dados pessoais e unicamente para os dados necessários à execução do contrato no qual o titular dos dados é uma das partes.

---

<sup>48</sup> Orientações sobre o direito à portabilidade dos dados ao abrigo do Regulamento 2016/679 (WP 242 rev.01), do Grupo de Trabalho do Artigo 29.º, aprovadas pelo CEPD, p. 13.

### 3.1.2.2 Dados recolhidos

125. Os dados tratados incluem os contactos do condutor (nome, endereço eletrónico, número de telefone), o tipo de veículo (por exemplo, automóvel, camião, motociclo), o número da matrícula, o período de estacionamento, os dados de pagamento (por exemplo, informações sobre o cartão de crédito), bem como dados de navegação.

### 3.1.2.3 Prazo de conservação

126. Os dados só devem ser conservados enquanto forem necessário para a execução do contrato de estacionamento ou consoante exigido pelo direito da União ou dos Estados-Membros. Posteriormente, os dados são anonimizados ou apagados.

### 3.1.2.4 Informações a facultar aos titulares dos dados e respetivos direitos

127. Previamente ao tratamento de dados pessoais, o titular dos dados deve ser informado em conformidade com o artigo 13.º do RGPD, de uma forma transparente e compreensível.
128. O titular dos dados deve ser especificamente informado a respeito dos meios disponíveis para exercer os seus direitos de acesso, de retificação, de limitação e de apagamento. Uma vez que os dados recolhidos neste contexto são facultados pelo titular dos dados (por meio de formulários específicos ou da sua atividade) e tratados com base no artigo 6.º, n.º 1, alínea b) (execução de um contrato), do RGPD, o titular dos dados está habilitado a exercer o seu direito à portabilidade dos dados. Tal como referido nas orientações sobre o direito à portabilidade dos dados, o CEPD recomenda vivamente «*que os responsáveis pelo tratamento expliquem claramente a diferença entre os tipos de dados que um titular de dados pode receber no âmbito dos direitos de acesso e de portabilidade dos dados*».

### 3.1.2.5 Destinatário:

129. Em princípio, apenas o responsável pelo tratamento e o subcontratante têm acesso aos dados.

### 3.1.2.6 Segurança:

130. Aplicam-se as recomendações gerais. Ver ponto 2.7.

## 3.2 eCall

131. Em caso de acidente grave na União Europeia, o veículo desencadeia automaticamente uma *eCall* para o 112, o número de chamadas de emergência a nível da UE (ver ponto 1.1 para mais pormenores), que permite enviar rapidamente uma ambulância para o local do acidente, de acordo com o Regulamento (UE) 2015/758, de 29 de abril de 2015, relativo aos requisitos de homologação para a implantação do sistema *eCall* a bordo com base no número 112 em veículos e que altera a Diretiva 2007/46/CE (a seguir designado por «Regulamento (UE) 2015/758»).
132. De facto, o gerador da *eCall* instalado no interior do veículo, que permite a transmissão através de uma rede pública de comunicações móveis sem fios, inicia uma chamada de emergência, que é desencadeada automaticamente pelos sensores do veículo ou manualmente pelos ocupantes do veículo unicamente em caso de acidente. Além da ativação do canal áudio, o segundo evento desencadeado automaticamente como resultado de um acidente consiste em gerar o conjunto mínimo de dados e enviá-lo para o ponto de atendimento de segurança pública (PASP).

### 3.2.1 Fundamento jurídico

133. No que respeita à aplicação da Diretiva Privacidade Eletrónica, têm de ser tidas em consideração duas disposições:

- Z O artigo 9.º, relativo a dados de localização para além dos dados de tráfego, o qual é unicamente aplicável aos serviços de comunicações eletrónicas;

Z O artigo 5.º, n.º 3, para a possibilidade de acesso a informações conservadas no gerador instalado no interior do veículo.

134. Apesar de, em princípio, essas disposições exigirem o consentimento do titular dos dados, o Regulamento (UE) 2015/758 constitui uma obrigação legal à qual o responsável pelo tratamento está sujeito (o titular dos dados não dispõe de uma escolha verdadeira ou livre e não poderá recusar o tratamento dos seus dados). Assim, o Regulamento (UE) 2015/758 prevalece sobre a necessidade do consentimento do condutor para o tratamento dos dados de localização e do conjunto mínimo de dados<sup>49</sup>.

135. O fundamento jurídico do tratamento desses dados será o cumprimento de uma obrigação legal (ou seja, o Regulamento (UE) 2015/758), tal como previsto no artigo 6.º, n.º 1, alínea c), do RGPD.

### 3.2.2 Dados recolhidos

136. O Regulamento (UE) 2015/758 estabelece que os dados enviados pelo sistema *eCall* a bordo com base no número 112 só incluem as informações mínimas necessárias referidas na norma EN 15722:2015 «Sistemas inteligentes de transportes – Segurança eletrónica (*eSafety*) – Conjunto mínimo de dados de *eCall*», incluindo:

Z A indicação se a *eCall* foi desencadeada manual ou automaticamente;

Z O modelo de veículo;

Z O número de identificação do veículo (NIV);

Z O tipo de propulsão do veículo;

Z O carimbo temporal da geração inicial da mensagem de dados inserida no incidente *eCall* atual;

Z A última posição conhecida da latitude e da longitude do veículo, determinada no último momento possível antes da geração da mensagem;

Z O último sentido real da marcha conhecido do veículo, determinado no último momento possível antes da geração da mensagem (apenas as três últimas localizações do veículo).

### 3.2.3 Prazo de conservação

137. O Regulamento (UE) 2015/758 estabelece que os dados não podem ser conservados para além do tempo necessário para o tratamento das situações de emergência. Esses dados são totalmente apagados quando deixarem de ser necessários para essa finalidade. Além disso, na memória interna do sistema *eCall*, os dados devem ser automática e constantemente apagados. Podem ser conservadas unicamente as três últimas posições do veículo, na medida em que tal for estritamente necessário para especificar a posição atual do veículo e o sentido da marcha no momento do evento.

### 3.2.4 Informações a facultar aos titulares dos dados e respetivos direitos

138. O artigo 6.º do Regulamento (UE) 2015/758 estabelece que os construtores devem facultar informações claras e completas relativas ao tratamento de dados efetuado através do sistema *eCall*. Estas informações devem ser facultadas no manual do utilizador separadamente para o sistema *eCall* a bordo com base no número 112 e para quaisquer

---

<sup>49</sup> Importa salientar que o artigo 8.º, n.º 1, alínea f), do mandato de negociação do Conselho para a proposta relativa ao Regulamento Privacidade Eletrónica prevê uma isenção específica para a *eCall*, dado que o consentimento é dispensável nos casos em que «é necessário localizar o equipamento terminal quando um utilizador final efetua uma comunicação de emergência para o número único europeu de chamadas de emergência 112 ou para um número nacional de chamadas de emergência, em conformidade com o artigo 13.º, n.º 3.



sistemas de *eCall* baseada em serviços prestados por entidades terceiras antes da utilização do sistema. Incluem:

- Z A referência ao fundamento jurídico para o tratamento;
  - Z O facto de estar ativado por defeito o sistema *eCall* a bordo com base no número 112;
  - Z As modalidades do tratamento de dados efetuado pelo sistema *eCall* a bordo com base no número 112;
  - Z A finalidade específica do tratamento da *eCall*, que deve limitar-se às situações de emergência referidas no artigo 5.º, n.º 2, primeiro parágrafo, do Regulamento (UE) 2015/758;
  - Z Os tipos de dados recolhidos e tratados e os destinatários desses dados;
  - Z O prazo de conservação dos dados no sistema *eCall* a bordo com base no número 112;
  - Z O facto de o veículo não ser objeto de localização constante;
  - Z As condições de exercício dos direitos dos titulares dos dados, bem como o contacto do serviço responsável pelos pedidos de acesso;
  - Z Todas as informações adicionais necessárias no que respeita à rastreabilidade, à localização e ao tratamento de dados pessoais em relação a uma *eCall* baseada em serviços prestados por terceiros e/ou outros serviços de valor acrescentado, que devem ser objeto de consentimento expresso do proprietário e respeitar o RGPD. Deve ser tido particularmente em conta o facto de poderem existir diferenças entre o tratamento de dados efetuado através do sistema *eCall* a bordo com base no número 112 e o tratamento efetuado pelos sistemas *eCall* a bordo de serviços prestados por entidades terceiras ou por outros serviços de valor acrescentado.
139. Além disso, o prestador de serviços deve facultar aos titulares dos dados informações em conformidade com o artigo 13.º do RGPD de uma forma transparente e compreensível. Em especial, devem ser informados das finalidades do tratamento para as quais os dados pessoais se destinam, bem como do facto de o tratamento de dados pessoais se basear numa obrigação legal à qual o responsável pelo tratamento está sujeito.
140. Além disso, tendo em conta a natureza do tratamento, as informações relativas aos destinatários ou às categorias de destinatários dos dados pessoais devem ser claras e os titulares dos dados devem ser informados de que os dados não estão disponíveis fora do sistema *eCall* a bordo com base no número 112 para nenhuma entidade antes de a *eCall* ser desencadeada.
141. No que respeita aos direitos dos titulares dos dados, importa notar que, dado que o tratamento se baseia numa obrigação legal, o direito de oposição e o direito à portabilidade não se aplicarão.

### 3.2.5 Destinatário:

142. Os dados não são disponibilizados fora do sistema *eCall* a bordo com base no número 112 a quaisquer entidades antes do desencadeamento da *eCall*.
143. Quando é desencadeado (manualmente pelos ocupantes do veículo ou automaticamente logo que um sensor a bordo deteta uma colisão grave), o sistema *eCall* estabelece uma ligação de voz com o PASP relevante e o conjunto mínimo de dados é enviado para o operador do PASP.
144. Além disso, os dados transmitidos através do sistema *eCall* a bordo com base no número 112 e tratados pelos PASP só podem ser transferidos para o serviço de emergência e para serviços parceiros referidos na Decisão n.º 585/2014/UE em caso de incidentes relacionados com *eCalls* e nas condições fixadas nessa decisão, e são exclusivamente utilizados para a

consecução dos objetivos da mesma. Os dados tratados pelos PASP através do sistema *eCall* a bordo com base no número 112 não são transferidos para entidades terceiras sem o consentimento prévio e expresso do titular dos dados.

### 3.2.6 Segurança

145. O Regulamento (UE) 2015/758 estabelece os requisitos para integrar no sistema *eCall* tecnologias que reforçam a proteção da privacidade, de modo a proporcionar aos utilizadores o nível adequado de proteção da privacidade, bem como as garantias necessárias para evitar a vigilância e utilizações abusivas. Além disso, os construtores devem assegurar que o sistema *eCall* com base no número 112 e qualquer sistema que permita a realização de uma *eCall* baseada em serviços prestados por entidades terceiras, ou serviço de valor acrescentado, sejam concebidos de tal forma que não sejam possíveis trocas de dados pessoais entre esses sistemas.
146. No que respeita aos PASP, os Estados-Membros devem assegurar a proteção dos dados pessoais contra qualquer utilização abusiva, incluindo o acesso ilegal aos mesmos, sua alteração ou perda, e que os protocolos relativos a conservação, duração de conservação, tratamento e proteção de dados pessoais são estabelecidos ao nível adequado e devidamente observados.

## 3.3 Estudos de acidentologia

147. Os titulares dos dados podem aceitar voluntariamente participar em estudos de acidentologia que visem uma melhor compreensão das causas dos acidentes rodoviários e, em termos mais gerais, outras finalidades científicas.

### 3.3.1 Fundamento jurídico

148. Quando os dados são recolhidos por meio de um serviço público de comunicações eletrónicas, o responsável pelo tratamento tem de obter o consentimento do titular dos dados para a possibilidade de acesso a informações já conservadas no veículo, tal como previsto no artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica. De facto, neste contexto, não é possível aplicar nenhuma das isenções previstas nas disposições em causa: o tratamento não tem a finalidade exclusiva de efetuar a transmissão de uma comunicação através de uma rede de comunicações eletrónicas, nem se refere a um serviço da sociedade da informação explicitamente solicitado pelo assinante ou utilizador.
149. No que respeita ao tratamento de dados pessoais e tendo em conta a variedade e a quantidade de dados pessoais necessários para os estudos de acidentologia, o CEPD recomenda que o tratamento se baseie no consentimento prévio do titular dos dados, em conformidade com o artigo 6.º do RGPD. Tal consentimento prévio deve ser dado num formulário específico, por meio do qual o titular dos dados se voluntaria a participar no estudo e consente no tratamento dos seus dados pessoais para essa finalidade. O consentimento deve ser uma expressão da vontade livre, específica e informada da pessoa cujos dados são objeto de tratamento (por exemplo, assinalar uma opção que não esteja pré-assinalada, ou configurar o computador de bordo para ativar uma função no veículo). Esse consentimento deve ser dado separadamente, para fins específicos, não pode ser associado ao contrato de compra ou locação financeira de um automóvel novo e deve ser possível retirá-lo com a mesma facilidade com que é dado. A retirada do consentimento resultará na interrupção do tratamento. Nesse caso, os dados serão apagados da base de dados ativa, ou anonimizados.
150. O consentimento exigido pelo artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica e o consentimento necessário como fundamento jurídico para o tratamento de dados podem ser obtidos simultaneamente (por exemplo, ao assinalar uma caixa de verificação que indique claramente aquilo que o titular dos dados está a consentir).

151. Importa notar que, dependendo das condições do tratamento (natureza do responsável pelo tratamento, etc.), pode ser licitamente selecionado outro fundamento jurídico, desde que não reduza a proteção adicional proporcionada pelo artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica (ver n.º 15). Se o tratamento se basear noutra fundamento jurídico, como o exercício de funções de interesse público (artigo 6.º, n.º 1, alínea e), do RGPD), o CEPD recomenda que os titulares dos dados sejam incluídos no estudo de forma voluntária.

### 3.3.2 Dados recolhidos

152. O responsável pelo tratamento deve recolher apenas os dados pessoais estritamente necessários para o tratamento.

153. Existem dois tipos de dados a ter em consideração:

**Z Dados relativos aos participantes e aos veículos;**

**Z Dados técnicos dos veículos** (velocidade instantânea, etc.).

154. A investigação científica associada à acidentologia justifica a recolha da velocidade instantânea, incluindo por pessoas coletivas que não administram um serviço público em sentido estrito.

155. De facto, tal como anteriormente referido, o CEPD considera que a velocidade instantânea recolhida no contexto de um estudo de acidentologia não equivale a dados relacionados com infrações por destino (ou seja, não é recolhida para fins de investigação ou repressão de uma infração), o que justifica a respetiva recolha por parte de pessoas coletivas que não administram um serviço público em sentido estrito.

### 3.3.3 Prazo de conservação

156. Importa distinguir entre dois tipos de dados. Em primeiro lugar, os dados relativos aos participantes e aos veículos podem ser conservados durante o período do estudo. Em segundo lugar, os dados técnicos dos veículos devem ser conservados durante o prazo mais reduzido possível para a finalidade em questão. A este respeito, cinco anos a contar do final do estudo parece constituir um prazo razoável. No termo desse prazo, os dados são apagados ou anonimizados.

### 3.3.4 Informações a facultar aos titulares dos dados e respetivos direitos

157. Previamente ao tratamento de dados pessoais, o titular dos dados deve ser informado em conformidade com o artigo 13.º do RGPD, de uma forma transparente e compreensível. Em especial, no caso da recolha da velocidade instantânea, os titulares dos dados devem ser especificamente informados da recolha dos dados. Dado que o tratamento dos dados se baseia no consentimento, o titular dos dados deve ser especificamente informado da existência do direito de retirar o consentimento a qualquer momento, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado. Além disso, uma vez que os dados recolhidos neste contexto são facultados pelo titular dos dados (por meio de formulários específicos ou da sua atividade) e tratados com base no artigo 6.º, n.º 1, alínea a) (consentimento), do RGPD, o titular dos dados está habilitado a exercer o seu direito à portabilidade dos dados. Tal como referido nas orientações sobre o direito à portabilidade dos dados, o CEPD recomenda vivamente «que os responsáveis pelo tratamento expliquem claramente a diferença entre os tipos de dados que um titular de dados pode receber no âmbito dos direitos de acesso e de portabilidade dos dados». Consequentemente, o responsável pelo tratamento deve disponibilizar uma forma simples para a retirada do seu consentimento, livremente e a qualquer momento, bem como desenvolver ferramentas para que possa dar resposta a pedidos de portabilidade dos dados.

158. Essa informação pode ser apresentada no momento da assinatura do formulário destinado a obter o consentimento para a participação no estudo de acidentologia.

### 3.3.5 Destinatário

159. Em princípio, apenas o responsável pelo tratamento e o subcontratante têm acesso aos dados.

### 3.3.6 Segurança

160. Tal como referido anteriormente, as medidas de segurança adotadas devem ser adaptadas ao nível de sensibilidade dos dados. Por exemplo, se a velocidade instantânea (ou quaisquer outros dados relativos a condenações penais e infrações) for recolhida no âmbito do estudo de acidentologia, o CEPD recomenda vivamente a implementação de medidas de segurança sólidas, tais como:

- Z Implementar medidas de pseudonimização (por exemplo, dispersão com chave secreta de dados como o apelido/nome do titular dos dados e o número de série);
- Z Conservar dados relativos à velocidade instantânea e à localização em bases de dados separadas (por exemplo, utilizando um mecanismo de encriptação avançado com chaves e mecanismos de aprovação distintos);
- Z E/ou apagar os dados de localização logo que o evento ou a sequência de referência seja qualificado (por exemplo, o tipo de estrada, dia/noite) e conservar os dados que permitam a identificação direta numa base de dados separada, à qual só um reduzido número de pessoas tenha acesso.

## 3.4 Combater o furto de automóveis

161. Os titulares dos dados podem desejar, no caso de furto, tentar encontrar o seu veículo recorrendo à localização. A utilização de dados de localização encontra-se limitada às necessidades estritas de investigação e de avaliação do caso pelas autoridades legais competentes.

### 3.4.1 Fundamento jurídico

162. Quando os dados são recolhidos por meio de um serviço de comunicações eletrónicas publicamente disponível, aplica-se o artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica.
163. Dado que se trata de um serviço da sociedade da informação, o artigo 5.º, n.º 3, da Diretiva Privacidade Eletrónica não exige o consentimento para a possibilidade de acesso a informações já conservadas no veículo quando tal serviço é explicitamente solicitado pelo assinante.
164. No que respeita ao tratamento de dados pessoais, o fundamento jurídico para o tratamento dos dados de localização será o consentimento do proprietário do veículo ou, se aplicável, a execução de um contrato (unicamente no caso dos dados necessários para a execução do contrato no qual o proprietário do veículo é uma das partes).
165. O consentimento deve ser uma expressão da vontade livre, específica e informada da pessoa cujos dados são objeto de tratamento (por exemplo, assinalar uma opção que não esteja pré-assinalada, ou configurar o computador de bordo para ativar uma função no veículo). A liberdade de dar o consentimento implica a opção de retirar o consentimento a qualquer momento, da qual o titular dos dados deve ser expressamente informado. A retirada do consentimento resultará na interrupção do tratamento. Nesse caso, os dados devem ser apagados da base de dados ativa, anonimizados ou arquivados.

### 3.4.2 Dados recolhidos

166. Os dados de localização podem ser transmitidos apenas a partir da declaração de furto e não podem ser recolhidos continuamente durante o tempo restante.

### 3.4.3 Prazo de conservação

167. Os dados de localização podem ser conservados apenas durante o período de avaliação do caso pelas autoridades legais competentes, ou até ao termo de um procedimento que vise dissipar as dúvidas que subsistam após a confirmação do furto do veículo.

### 3.4.4 Informações a facultar aos titulares dos dados

168. Previamente ao tratamento de dados pessoais, o titular dos dados deve ser informado em conformidade com o artigo 13.º do RGPD, de uma forma transparente e compreensível. Mais especificamente, o CEPD recomenda que o responsável pelo tratamento saliente que não existe um seguimento constante do veículo e que só é possível recolher e transmitir os dados de localização a partir da declaração de furto. Além disso, o responsável pelo tratamento deve apresentar ao titular dos dados informações relacionadas com o facto de o acesso aos dados ser concedido apenas aos gestores aprovados da plataforma de vigilância à distância e às autoridades legalmente aprovadas.
169. No que respeita aos direitos dos titulares dos dados, quando o tratamento dos dados se baseia no consentimento, o titular dos dados deve ser especificamente informado da existência do direito de retirar o consentimento a qualquer momento, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado. Além disso, quando os dados recolhidos neste contexto são facultados pelo titular dos dados (por meio de formulários específicos ou da sua atividade) e tratados com base no artigo 6.º, n.º 1, alínea a) (consentimento), ou no artigo 6.º, n.º 1, alínea b) (execução de um contrato), do RGPD, o titular dos dados está habilitado a exercer o seu direito à portabilidade dos dados. Tal como referido nas orientações sobre o direito à portabilidade dos dados, o CEPD recomenda vivamente «que os responsáveis pelo tratamento expliquem claramente a diferença entre os tipos de dados que um titular de dados pode receber no âmbito dos direitos de acesso e de portabilidade dos dados».
170. Consequentemente, o responsável pelo tratamento deve disponibilizar uma forma simples para a retirada do seu consentimento (unicamente no caso de o consentimento ser o fundamento jurídico), livremente e a qualquer momento, bem como desenvolver ferramentas para que possa dar resposta a pedidos de portabilidade dos dados.
171. As informações podem ser facultadas no momento da assinatura do contrato.

### 3.4.5 Destinatários

172. No caso de declaração de furto, os dados de localização podem ser transmitidos i) aos gestores aprovados da plataforma de vigilância à distância e ii) às autoridades legalmente aprovadas.

### 3.4.6 Segurança

173. Aplicam-se as recomendações gerais. Ver ponto 2.7.