GRUPO DE PESQUISA EM

# DESAFIOS DA PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL

ANALÍTICOS

JUS SCRIPTUM'S
INTERNATIONAL JOURNAL OF LAW
a. 20 • v. 10 • dossiê • 2025

12 Ana Cristina Oliveira Mahle
Dark patterns e neurodireitos: proteção da privacidade e desafios regulatórios no contexto digital

41 Camila Franzo
Veículos autônomos e as implicações em matéria de proteção de dados

76 Dânton Hilário Zanetti de Oliveira
Inteligência artificial e codificação: avanço ou retrocesso regulatório?

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA
Associação Académica da Faculdade de Direito de Lisboa
AAFDL
nelb

JUS SCRIPTUM'S
INTERNATIONAL JOURNAL OF LAW
REVISTA INTERNACIONAL DE DIREITO

# DESAFIOS DA PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL

Analíticos do Grupo de Pesquisa em
Proteção de Dados e Inteligência Artificial

Núcleo de Estudo Luso-Brasileiro
Faculdade de Direito da Universidade de Lisboa

2025
a. 20 v. 10 d. 1
EDIÇÃO ESPECIAL

**Jus Scriptum's International Journal of Law**
Revista Internacional de Direito do Núcleo de Estudo Luso-Brasileiro da Faculdade de Direito da Universidade de Lisboa
Ano 20 • Volume 10 • Edição Especial • 2025
Analíticos do Grupo de Pesquisa em Proteção de Dados e Inteligência Artificial

Periodicidade Trimestral
ISSN 1645-9024

## Equipe Editorial

**Corpo de Avaliadores – Peer Review Board**

Anjuli Tostes Faria Melo
Camila Franco Henriques
Carla Valério
Caroline Lima Ferraz
César Fiuza
Eduardo Alvares de Oliveira
Francine Pinto da Silva Joseph
Isaac Kofi Medeiros
J. Eduardo Amorim
José Antonio Cordeiro de Oliveira
Leonardo Bruno Pereira de Moraes
Leonardo Castro de Bone
Marcelo Ribeiro de Oliveira
Marcial Duarte de Sá Filho
Maria Vitoria Galvan Momo
Plínio Régis Baima de Almeida
Rafael Vasconcellos de Araújo Pereira
Rafaela Câmara Silva
Renato Sedano Onofre
Silvia Gabriel Teixeira
Thais Cirne
Vânia dos Santos Simões

## Grupo de Pesquisa em Proteção de Dados e Inteligência Artificial

Profa. Doutora Mariana Moraes Palmeira, Coordenadora Científica
Dr. Daniel Serrão, Coordenador Executivo

Alessandra Fonseca de Carvalho;
Aline Pinheiro;
Ana Cristina Oliveira Mahle;
Anna Carolina Almeida da Cruz;
Camila Franzo;
Carlos Mendes da Silveira Cunha;
Carolina Tavares Vieira Félix;
Cláudio Cardona;
Claudio Roberto Sales Kistler Junior;
Cristiane Rafaela Dallastra;
Dânton Zanetti;
Francisco Soares Reis Júnior;
Gabriela Cristine Buzzi;
Jade Caldas Sibalde;
Joice Bernardo do Carmo;
Júlia Castro John;
Lorena Garrido Borges;
Lucas Azoubel;
Maria Vitória Galvan Momo;
Mariana Fernandes Conrado;
Marina Goulart de Queiroz;
Patrícia Ferreira de Almeida;
Sharlynn Margery De Jongh Martins;
Thiago de Araújo Carneiro Leão;
Wilson Furtado Roberto.

# VEÍCULOS AUTÔNOMOS E AS IMPLICAÇÕES EM MATÉRIA DE PROTEÇÃO DE DADOS

*Autonomous vehicles and the implications for data protection*

Camila Franzo*

O presente trabalho visou analisar a relação entre os veículos autônomos e a proteção de dados no âmbito da União Europeia, verificando a existência de normativas que se aplicam a esse contexto. Para tanto, a metodologia empregada foi a pesquisa qualitativa, descritiva, bibliográfica e documental. Os resultados obtidos indicam que a implantação de veículos autônomos pode ser um desafio à proteção de dados, diante da abundância de dados pessoais coletados durante a sua utilização e dos riscos advindos do tratamento. Entretanto, verificou-se que as normativas da União Europeia em matéria de proteção de dados são robustas e capazes de abranger o cenário dos carros autônomos. Concluiu-se que, para que seja garantida a proteção de dados nesse contexto, devem ser adotadas medidas de segurança e de governança nas empresas, garantindo o cumprimento às legislações, com vistas a mitigar os riscos inerentes aos veículos autônomos, sem impedir o desenvolvimento tecnológico.

Palavras-chave: Privacidade; proteção de dados; RGPD; veículos autônomos.

The aim of this study was to analyze the relation between autonomous vehicles and data protection in the European Union, verifying the existence of regulations that apply to this context. For this purpose, the methodology employed was qualitative, descriptive, bibliographical and documentary research. The results obtained indicate that the deployment of autonomous vehicles can be a challenge for data protection, given the abundance of personal data collected during their use and the risks arising from their processing. However, it was found that the European Union's data protection regulations are robust and capable of covering the autonomous car scenario. It was concluded that, to guarantee data protection in this context, companies must adopt security and governance measures, ensuring compliance with legislation, with the intention of mitigating the risks inherent to autonomous vehicles, without impeding technological development.

Key words: Privacy; data protection; GDPR; autonomous vehicles.

* Mestre em Direito Penal e Ciências Criminais pela Faculdade de Direito da Universidade de Lisboa. Pós-graduada em Advocacia Empresarial pela Escola Brasileira de Direito. Advogada.

Sumário: 1. Introdução; 2. Metodologia; 3. Resultados e discussão; 3.1. Os veículos autónomos; 3.1.1. Tecnologias-chave por trás dos veículos autónomos; 3.1.2. Benefícios na implantação de veículos autónomos; 3.1.3. Desafios enfrentados na implantação de veículos autónomos; 3.2. Privacidade e proteção de dados nos veículos autónomos; 3.2.1. Tipos de dados coletados por veículos autónomos; 3.2.2. Desafios à proteção de dados; 3.3. O presente e o futuro da proteção de dados nos veículos autónomos; 3.4. Propostas de medidas técnicas de privacidade; 4. Conclusão; Referências bibliográficas.

## 1. Introdução

Acredita-se que a história dos veículos autônomos remonta à primeira metade do século XX, nos Estados Unidos da América, quando os acidentes de tráfego já eram uma preocupação social. Nessa época, o erro humano já era reconhecido como a causa principal dos sinistros e o *design* dos veículos também era tido como um dos fatores relevantes[1]. Na década de 1930, já havia a apresentação de ideias para o desenvolvimento de cidades com rodovias automatizadas e sistemas de transporte autônomos[2].

A partir das décadas que se seguiram, muitos foram os protótipos e modelos criados para tentar chegar a um veículo que fosse o mais autônomo possível. A busca pelo desenvolvimento de veículos totalmente autônomos tem levado as grandes empresas fabricantes de veículos e empresas de tecnologia à busca desenfreada pelo pioneirismo no setor. Isso, porque essa tecnologia promete trazer uma série de benefícios à sociedade, principalmente no que concerne à segurança viária.

---

1. Fabian Kröger, "Automated Driving in Its Social, Historical and Cultural Contexts," em *Autonomous Driving: Technical, Legal and Social Aspects*, ed. Markus Maurer, Joseph Christian Gerdes, Barbara Lenz, Hermann Winner (Berlim: SpringerOpen, 2016), PDF, p. 42.
2. Kröger, "Automated Driving", PDF, 46-47. Também, Matthew Blunt, "Highway to a Headache: Is Tort-Based Automotive Insurance on a Collision Course with Autonomous Vehicles", *Willamette Law Review* 53, no. 2 (2017): XXX. https://heinonline.org/HOL/Page?handle=hein.journals/willr53&div=9&g_sent=1&casa_token=, 114-115.

Entretanto, há desafios a serem enfrentados com a adoção de carros sem motorista, como os relativos à proteção de dados pessoais, à imprevisibilidade da máquina e à responsabilização.

A preocupação com a proteção de dados pessoais é extremamente relevante e vem sendo tema de discussão no mundo todo, sendo impulsionada pela crescente utilização de inteligências artificiais nos mais variados setores do mercado. Quando se trata de veículos sem motorista, o cenário pode tornar-se bastante complexo. Estima-se que veículos autônomos geram em torno de 20 *terabytes* (TB) de dados por dia, mas que podem produzir, no futuro, uma quantidade tão vasta que será possível chegar em montantes na unidade de *exabyte* (EB)[3] por dia[4].

Esses dados são geralmente coletados pelos sensores existentes nos veículos e tratam-se, em grande parte, de dados pessoais. O tratamento desse grande montante de dados pessoais levanta questões relacionadas à proteção de dados, à privacidade e à cibersegurança.

Assim, o objetivo geral do presente trabalho é o de verificar se as atuais legislações, no âmbito da União Europeia, conseguem proteger os titulares de dados de eventuais violações a seus direitos e liberdades individuais no contexto de carros sem motorista.

Para tanto, dividiu-se o trabalho em tópicos. Primeiramente, contextualiza-se os veículos autônomos, trazendo seu conceito, explicando a tecnologia por trás, e os benefícios e desafios associados a eles. Após, aborda-se questões relativas à

3. Uma unidade de *exabyte* é equivalente a um milhão de *terabytes*.
4. Alex Vakulov, "Addressing Data Processing Challenges in Autonomous Vehicles," IoT For All, última modificação 5 de fevereiro de 2024, https://www.iotforall.com/addressing-data-processing-challenges-in-autonomous-vehicles.

proteção de dados no contexto dos veículos autônomos, os dados coletados durante sua utilização e os desafios enfrentados nesse contexto. Por último, realiza-se uma abordagem voltada à contextualização com as normativas atuais e sua possível aplicação no caso dos carros autônomos, bem como possíveis mecanismos de mitigação de riscos.

## 2. Metodologia

Para a elaboração do presente trabalho, o tipo de pesquisa utilizado, quanto à abordagem, foi a pesquisa qualitativa e, quanto aos objetivos, a pesquisa descritiva. Os métodos de pesquisa utilizados foram a pesquisa bibliográfica e a pesquisa documental.

Para contextualização do tema e compreensão do atual estado da arte no que diz respeito à proteção de dados no contexto dos veículos autônomos, buscou-se bibliografias contidas em artigos científicos, livros, revistas, *websites* e outros documentos, tanto em ambiente físico como em ambiente digital.

Também, utilizou-se de documentos legais, como leis, regulamentos, resoluções e diretrizes, com o fim de verificar se as normativas referentes à proteção de dados já existentes são suficientes para abranger o cenário compreendido pelos carros sem motorista.

Essa abordagem metodológica traz uma visão a respeito da proteção de dados na União Europeia e sua possível aplicação a novos cenários, como o dos carros autônomos.

# 3. Resultados e discussão

## 3.1. Os veículos autônomos

Os veículos autônomos, também chamados de carros autônomos, carros sem motorista, carros-robô, carros autoconduzidos, dentre outras denominações, são aqueles capazes de conduzir de forma autônoma, independente de um condutor humano[5].

O Código de Estrada Alemão (*Straßenverkehrsgeset - StB*), em sua oitava emenda, passou a tratar sobre os veículos com alta ou total autonomia, definindo-os como aqueles equipados com tecnologia que: assim que ativada, é capaz de controlar o motor do veículo, assumindo a função de motorista; seja capaz de cumprir com as normas de trânsito e demais regulamentações para operar veículos; possa ser substituída ou desativada de forma manual pelo condutor humano; seja capaz de verificar a necessidade de que o condutor humano retome o controle do veículo e indique ao motorista, de forma clara, a necessidade da retomada de controle com tempo suficiente; possa indicar que o uso vai contra o descrito no sistema[6].

A *SAE International*, associação internacional de engenheiros dos setores aeroespacial e automotivo[7], estipulou padrões e classificou os veículos em seis

[5]. Armin Engländer, "O veículo autônomo e o tratamento de situações dilemáticas," em *Veículos autônomos e direito penal,* org. Heloisa Estellita e Alaor Leite (São Paulo: Marcial Pons, 2019), 88.
[6]. "Eight Act amending the Road Traffic Act, section 1a." Federal Law Gazette I, 2017. https://bmdv.bund.de/SharedDocs/EN/Documents/DG/eight-act-amending-the-road-traffic-act.pdf?__blob=publicationFile.
[7]. SAE International, "Sobre nós," acessado em Abril 15, 2024, http://br.sae.org/about/.

diferentes níveis, levando em consideração a sua autonomia em relação ao condutor humano.

Nos primeiros três níveis (nível 0, nível 1 e nível 2), o humano é quem conduz o veículo, sendo que a tecnologia é considerada apenas um suporte ao motorista, motivo pelo qual ele deve estar sempre atento. No nível 0, há ferramentas que auxiliam o condutor momentaneamente, como freios de emergência automáticos, aviso de pontos cegos e avisos de saídas de faixa. No nível 1, há ferramentas de suporte ao motorista no freio ou na aceleração, podendo haver, por exemplo, ou o controle de cruzeiro adaptativo, ou o centralizador de faixa. Já no nível 2, há tanto ferramentas de suporte ao motorista no freio como na aceleração, podendo haver controle de cruzeiro adaptativo e centralizador de faixa[8].

Nos três últimos níveis (nível 3, nível 4 e nível 5), o humano não é considerado condutor quando as tecnologias de condução autônoma estão ativadas. No nível 3, o sistema autônomo poderá conduzir o veículo em condições limitadas, podendo ainda haver a solicitação ao humano para que conduza, se assim for necessário. Nos níveis mais altos de autonomia, que seriam os níveis 4 e 5, não há a solicitação para o humano conduzir o veículo em nenhum momento, podendo, inclusive, não haver pedais instalados. A diferença entre os dois níveis reside no fato de que, enquanto a tecnologia de nível 4 funciona apenas sob condições controladas e limitadas, a de nível 5 funciona sob qualquer circunstância[9].

8. SAE International, “Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_202104,” acessado em Abril 15, 2024, https://www.sae.org/standards/content/j3016_202104.
9. SAE International, “Taxonomy and Definitions.”

### 3.1.1. Tecnologias-chave por trás dos veículos autônomos

Os veículos autônomos contam com uma variedade de tecnologias que, quando integradas, permitem que os automóveis conduzam de forma autônoma, realizando a leitura e interpretação do meio que os cerca e tomando decisões autonomamente.

Algumas das principais tecnologias que integram um carro autônomo são o GPS (*Global Positioning System*), LiDAR (*Light Detection and Ranging*), radar, câmera, sensor ultrassônico, dentre outros[10]. Por meio desses dispositivos, dados externos como sons, imagens e localização são obtidos, possibilitando ao veículo realizar uma leitura de todo o meio que o cerca. A leitura e o processamento de dados, bem como a tomada de decisões, são realizados pela inteligência artificial (IA) que integra o veículo.

Nas palavras de Paula Ribeiro de Faria[11]: "Um *robot* com inteligência artificial é um *robot* cujo sistema de aprendizagem reproduz as sinapses neuronais do cérebro humano, permitindo-lhe reconhecer padrões de comportamento e obter informação do meio envolvente, estabelecendo a partir daí novos padrões de comportamento face às circunstâncias e interagindo com outras pessoas ou com outros *robots* dotados de inteligência artificial".

---

10. Anton Hristozov, "The role of artificial intelligence in autonomous vehicles," Embedded, última modificação 15 de julho de 2020, https://www.embedded.com/the-role-of-artificial-intelligence-in-autonomous-vehicles/.

11. Paula Ribeiro de Faria, "Os veículos autónomos e o direito penal," em *Estudos em homenagem ao Conselheiro Presidente Manuel da Costa Andrade vol. II,* org. Pedro Machete, Gonçalo de Almeida Ribeiro e Mariana Canotilho (Coimbra: Almedina, 2023), 384.

Para isso tornar-se possível, tecnologias como *Big Data*, *Machine Learning* e *Deep Learning* são utilizadas. De acordo com Ana Frazão[12], o *Big Data* seria a "matéria-prima" utilizada pelos algoritmos para a tomada de decisões e corresponderia a uma grande quantidade de dados disponibilizados virtualmente e que, após processados, podem tornar-se informações úteis e servir como diretriz no processo de decisão do algoritmo.

O *Machine Learning*, ou aprendizado da máquina, refere-se à capacidade da máquina em aprender com os dados que são processados, por meio da identificação de padrões[13]. Já o *Deep Learning*, ou aprendizado profundo, é um subgrupo do *Machine Learning* e refere-se à capacidade de processamento e extração de informações úteis de grandes quantidades de dados, inclusive de dados de fontes diferentes[14].

Portanto, um veículo autônomo é repleto de tecnologias, tangíveis e intangíveis, que processam uma quantidade vasta de dados, permitindo que ele tenha pouca ou nenhuma dependência de um condutor humano.

---

12. Ana Frazão, "Algoritmos e inteligência artificial: repercussões da sua utilização sobre a responsabilidade civil e punitiva das empresas," Professora Ana Frazão, 16 de maio de 2018, http://professoraanafrazao.com.br/files/publicacoes/2018-05-16-Algoritmos_e_inteligencia_artificial.pdf.

13. Sabbani Rao, Venkata Achuta, K. Kondaiah, G. Rajesh Chandra, e K. Kiran Kumar, "A Survey on Machine Learning: Concept, Algorithms and Applications", *International Conference on Innovative Research in Computer and Communication Engineering February,* (Fevereiro 2017): 1301-1302. https://www.smec.ac.in/assets/images/committee/research/17-18/282.A%20Survey%20on%20Machine%20Learning%20Concept,.pdf. Também, Iria Giuffrida, "Liability for AI Decision-Making: Some Legal and Ethical Considerations", *Fordham Law Review* 88, no. 2 (2019): 441. https://ir.lawnet.fordham.edu/flr/vol88/iss2/3/.

14. Pramila. P. Shinde, Seema Shah, "A Review of Machine Learning and Deep Learning Applications", *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, (Abril 2019): 3. https://doi.org/10.1109/ICCUBEA.2018.8697857.

### 3.1.2.Benefícios na implantação de veículos autônomos

Todo o esforço das grandes empresas para criar essas tecnologias avançadas se dá por motivos que vão muito além da mera busca pela comodidade que os carros sem motorista podem trazer.

De acordo com estimativas da Organização Mundial da Saúde (OMS) publicadas no *Global Status Report on Road Safety 2023*, o número de mortes por acidentes de trânsito no ano de 2021 foi de aproximadamente 1,19 milhões, sendo a décima segunda maior causa de mortes de pessoas de todas as idades e a maior causa de mortes de pessoas que possuem entre cinco e vinte e nove anos[15].

Visando a redução de acidentes veiculares, a Organização das Nações Unidas (ONU) declarou, por meio da Resolução 74/299, que esta seria a década de ação pela segurança no trânsito (2021–2030), tendo como meta a redução de 50% no número de acidentes veiculares[16]. A OMS e as Comissões Regionais das Nações Unidas lançaram o Plano Global, um documento que serve de apoio à implantação de medidas para atingir a meta proposta pela ONU[17]. Nesse documento, são citados os principais fatores de risco para a ocorrência elevada de acidentes de trânsito com resultado lesão corporal grave ou morte decorrentes de erro humano, quais sejam: velocidade, condução sob influência de álcool e outras substâncias, não utilização

[15]. World Health Organization, "Global status report on road safety 2023," acessado em Maio 29, 2024, https://www.who.int/publications/i/item/9789240086517.
[16]. World Health Organization, "Plano Global: década de ação pela segurança no trânsito 2021-2030," acessado em Maio 29, 2024, https://cdn.who.int/media/docs/default-source/documents/health-topics/road-traffic-injuries/global-plan-for-the-doa-of-road-safety-2021-2030-pt.pdf?sfvrsn=65cf34c8_33&download=true.
[17]. WHO, "Plano Global."

de medidas de segurança, como cintos de segurança e capacetes, direção distraída, não cumprimento de normas/leis de trânsito, dentre outros[18].

Segundo a *The Royal Society for the Prevention of Accidents*, organização britânica, a utilização de veículos totalmente autônomos, ao evitar comportamentos de risco, diminuiria o erro humano na condução, o que poderia levar à diminuição no número de acidentes de trânsito e, consequentemente, o número de vítimas. Além da prevenção de acidentes, conseguiria fornecer apoio a grupos que são incapazes de conduzir um veículo, como adolescentes, idosos e pessoas portadoras de necessidades especiais[19].

Além dos benefícios relativos à segurança e mobilidade, a Resolução do Parlamento Europeu, de 20 de janeiro de 2021, sobre questões de interpretação e aplicação do direito internacional relativas à inteligência artificial, de igual modo destaca os benefícios ambientais, os relacionados à atenuação de congestionamentos e à melhora no fluxo de tráfego[20].

Ainda, é possível pensar em benefícios relativos à comodidade e otimização no tempo, uma vez que em veículos com alto grau de autonomia, não é necessário que o humano esteja conduzindo, sendo possível que realize outras atividades durante o trajeto. Segundo Paula Ribeiro de Faria, é possível que os passageiros

18. WHO, "Plano Global."
19. The Royal Society for the Prevention of Accidents**, "**Road safety factsheet: autonomous vehicles," acessado em Maio 29, 2024. https://www.rospa.com/media/documents/road-safety/factsheets/autonomous-vehicles.pdf.
20. "Resolução do Parlamento Europeu, de 20 de janeiro de 2021, sobre a inteligência artificial: questões de interpretação e de aplicação do direito internacional na medida em que a UE é afetada nos domínios da utilização civil e militar e da autoridade do Estado fora do âmbito da justiça penal (2020/2013(INI))." Parlamento Europeu, 20 de janeiro de 2021, p. 1-19. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_PT.html.

sejam "[…] conduzidos tranquilamente ao seu destino enquanto leem um livro, vêm [sic] um filme, ou atualizam as redes sociais, incluindo as pessoas com dificuldades motoras ou doentes, crianças, ou ocupantes embriagados [...]"[21].

### 3.1.3. Desafios enfrentados na implantação de veículos autônomos

Em que pese o potencial dos carros autônomos em trazer benefícios à sociedade, não se pode ignorar os grandes desafios associados à implantação dessa tecnologia. Há quem classifique em cinco os riscos relacionados aos veículos autônomos: riscos associados à segurança, à responsabilidade, à privacidade, à cibersegurança e à influência da indústria[22]. As dúvidas que permeiam sobre a adoção dos carros sem motorista incluem questões técnicas, regulatórias e de aceitação pública.

Ao mesmo tempo em que a segurança é a principal motivação para o desenvolvimento de veículos sem motorista, a eliminação da interferência humana na condução não impede que outros problemas possam surgir, como aqueles decorrentes de falhas no funcionamento da própria máquina ou de uma má programação.

Também, trata-se de uma novidade tecnológica ainda sob desenvolvimento, com riscos que podem ser desconhecidos. Somado a isso, a utilização de tecnologias como a *Machine Learning* traz uma imprevisibilidade à máquina, já que a tomada de decisões e as ações realizadas são baseadas no autoaprendizado da inteligência artificial.

---

21. Faria, "Os veículos autónomos", 368.
22. Araz Taeihagh, Hazel Si Min Lim, "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks", *Transport reviews* 39, no. 1 (Julho 2018): 106. https://doi.org/10.1080/01441647.2018.1494640.

A imprevisibilidade também afeta o campo da responsabilização nos casos de acidentes que ocorrem com veículos autônomos, já que, nesse contexto, dificulta-se identificar os elementos essenciais para a imputação de uma responsabilidade cível ou criminal.

Araz Taeihagh e Hazel Si Min Lim[23] consideram a influência da indústria um risco associado à implantação de veículos autônomos. Para os autores, a adoção generalizada pelo mercado dessa tecnologia pode causar grandes implicações no setor de empregos, uma vez que alguns serviços realizados de forma manual, como o trabalho como motorista ou taxista, podem ser substituídos pelo sistema autônomo.

No que diz respeito aos riscos relacionados à privacidade e cibersegurança, serão abordados em tópico próprio.

## 3.2. Privacidade e proteção de dados nos veículos autônomos

No ano de 2023, uma reportagem realizada pela Reuters expôs o vazamento de dados de veículos autônomos da Tesla Inc. No referido caso, ex-funcionários da empresa relataram que, de 2019 a 2022, houve o compartilhamento em grupos de funcionários de imagens captadas pelas câmeras dos carros. Conforme a reportagem, dentre os dados compartilhados estavam fotos e vídeos "altamente invasivos" dos usuários, incluindo imagens de nudez explícita. Também, relataram terem sido

[23]. Taeihagh et al., "Governing autonomous vehicles", 118-119.

compartilhados vídeos de acidentes, até mesmo de um caso de atropelamento de uma criança no ano de 2021[24].

Além disso, segundo os ex-funcionários, o sistema que eles utilizavam na empresa poderia mostrar onde as imagens foram captadas, o que permitiria a identificação do local no qual os usuários residiam. Um ex-funcionário ainda relatou à Reuters que alguns registros aparentavam ter sido captados quando o carro estava desligado, sendo possível ver o interior da casa e da garagem do consumidor[25].

O fato ocorrido exemplifica bem a preocupação emergente a respeito da proteção de dados durante a utilização de carros autônomos. Isso, porque os veículos sem motorista necessitam captar e processar uma enorme quantidade de dados para que possam funcionar adequadamente, de acordo com o esperado da tecnologia. Bloom et al.[26] consideram que os carros sem motorista podem ser vistos como uma nova tecnologia invasiva à privacidade, por haver um monitoramento contínuo, mas sem informações sobre como os dados coletados serão utilizados.

Outro aspecto de grande importância é o fato de que, durante o uso de carros autônomos, não são coletados apenas os dados dos seus usuários, mas também de pessoas externas ao veículo, tal como pedestres[27] diante das câmeras e sensores

[24]. Steve Stecklow, Waylon Cunningham, e Hyunjoo Jin, "Tesla workers shared sensitive images recorded by customer cars," Reuters, última modificação 6 de abril de 2023, https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

[25]. Stecklow et al., "Tesla workers shared sensitive images."

[26]. Cara Bloom, Joshua Tan, Javed Ramjohn, e Lujo Bauer, "Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles", *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, (Julho 2017): 360. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bloom.

[27]. Ioannis Krontiris, Kalliroi Grammenou, Kalliopi Terzidou, Marina Zacharopoulou, Marina Tsikintikou, Foteini Baladima, Chrysi Sakellari, e Konstantinos Kaouras, "Autonomous vehicles: Data protection and ethical considerations", *Proceedings of the 4th ACM Computer*

que os integram. Assim, nesse contexto, podem ser considerados titulares de dados os motoristas, usuários e proprietários dos carros autônomos, e transeuntes[28], por exemplo.

De acordo com o Regulamento Geral sobre a Proteção de Dados (RGPD), o titular de dados tem o direito de obter confirmação e comunicação dos dados pessoais que são tratados, bem como a finalidade a que o tratamento se destina[29]. Porém, quando se trata de veículos autônomos, difícil se torna imaginar a possibilidade de comunicação a todos os titulares de dados que foram tratados no sistema autônomo, diante da complexidade do cenário e da pluralidade de agentes.

De fato, todo esse debate traz questionamentos a respeito do cumprimento, por parte das empresas responsáveis, das normas relativas à proteção de dados pessoais e privacidade quando se trata dos automóveis com autonomia.

### 3.2.1. Tipos de dados coletados por veículos autônomos

Para entender quais dados são coletados por veículos autônomos, necessário se faz compreender a sua tecnologia. Como já dito, os carros sem motorista são

*Science in Cars Symposium (CSCS '20)*, (Dezembro 2020): 1. https://doi.org/10.1145/3385958.3430481.

28. Kai Rannenberg, "Opportunities and Risks Associated with Collecting and Making Usable Additional Data," em *Autonomous Driving: Technical, Legal and Social Aspects*, ed. Markus Maurer, Joseph Christian Gerdes, Barbara Lenz, Hermann Winner (Berlim: SpringerOpen, 2016), PDF, 500.

29. "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 (Regulamento Geral sobre a Proteção de Dados)." Jornal Oficial da União Europeia, 4 de maio de 2016, L 119, p. 1-88. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679.

equipados com diversas câmeras e sensores que realizam uma leitura de todo o meio que os circunda.

Pode-se caracterizar os dados coletados por carros autônomos, separando-os em dados sobre o veículo e seus passageiros e em dados sobre elementos externos ao veículo[30]. Dentre os dados referidos ao veículo e aos usuários, estão: dados pessoais dos integrantes do veículo, como nome, endereço; dados biométricos (impressão digital, autenticação facial, autenticação por voz etc.), imagens advindas de câmeras internas para monitorar o comportamento do condutor[31] (nos casos de tecnologias que não são totalmente autônomas); dados relativos a localizações de viagem; dados de localização atual de um veículo; dados de identificação do veículo; dentre outros.

Dentre os dados relativos aos elementos externos ao veículo, estão: dados captados por sensores de pessoas externas; imagens de pessoas externas captadas por câmeras; dados de identificação de outros veículos; dados recebidos de outros veículos[32], nos casos de veículos conectados[33].

Portanto, ao utilizar um veículo com autonomia, uma vasta quantidade de dados é coletada, como dados de identificação pessoal, biométricos,

30. Krontiris et al., "Autonomous vehicles", 2-3.
31. Nesses casos, segundo Kai Rannenberg, os dados que se referem à dinâmica da direção e ao comportamento na direção fornecem informações que dizem respeito ao comportamento do condutor, a forma que dirige, como por exemplo, de forma agressiva ou calma, a velocidade da direção, se dirige de acordo com o limite de velocidade permitida, dentre outros aspectos. Rannenberg, "Opportunities and Risks", 499.
32. É possível que o veículo autônomo seja equipado com tecnologia que o torna capaz de receber dados por outros meios, além daqueles obtidos por seu sistema interno, comunicando-se com outros veículos (V2V – vehicle to vehicle), com infraestruturas (V2I – vehicle to infrastructure) ou com todo o meio ao redor (V2X – vehicle to everything). Faria, "Os veículos autónomos", 388.
33. Krontiris et al., "Autonomous vehicles", 2-3.

comportamentais, de comunicação, de localização, financeiros, dentre outros. Contudo, não apenas os dados dos usuários dos carros são coletados, mas também de outras pessoas que integram o meio no entorno do veículo. Do mesmo modo é possível que dados sejam obtidos de outros automóveis, nos casos de meios de transporte conectados.

### 3.2.2.Desafios à proteção de dados

Apesar dos muitos benefícios esperados dos veículos autônomos, há ainda muitos desafios relacionados à segurança e à privacidade, já que esses automóveis se tornam vulneráveis a problemas oriundos de sistemas computacionais, pelo fato de não serem puramente mecânicos34.

Os agentes inteligentes, como são os automóveis com autonomia, conseguem reagir diretamente a informações captadas pelos seus sensores, procurando por padrões, de forma autônoma, nesses dados já armazenados35. Os dados coletados durante o funcionamento de carros autônomos são processados pelo sistema interno do automóvel, mas podem ser externalizados, a depender da situação, para treinamento da Machine Learning36.

Esses dados podem ser externalizados também pelo fato de que a quantidade de dados captados e processados em um veículo autônomo pode ser muito

34. Muhammad Hataba, Ahmed Sherif, Mohamed Mahmoud, Mohamed Abdallah, e Waleed Alasmary, "Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey", *IEEE Open Journal of the Communications Society* 3, (Abril 2022): 811. https://doi.org/10.1109/OJCOMS.2022.3169500.
35. Sabine Gless, Thomas Weigend "Agentes inteligentes e o direito penal," em *Veículos autônomos e direito penal*, org. Heloisa Estellita e Alaor Leite (São Paulo: Marcial Pons, 2019), 40.
36. Krontiris et al., "Autonomous vehicles", 3.

vasta, ultrapassando os limites de bancos de dados convencionais, sendo necessária a utilização de servidores em nuvens para armazenamento. Isso facilita o aprendizado da máquina, auxiliando-a na tomada de decisões, já que o sistema consegue encontrar padrões, associações, tendências, dentre outros37.

Para Herman Strange38, a utilização de bancos de dados centralizados pode aumentar o risco de violação de dados, bem como de acessos não autorizados. Os sistemas de inteligência artificial, por geralmente armazenarem os dados na nuvem, correm esse risco, já que permitem o acesso de múltiplas pessoas.

Em muitos casos, os dados armazenados podem ser transferidos a terceiros, como o fabricante do automóvel, seguradoras, empresas de locação de carros, agências governamentais, outros participantes do tráfego, outros veículos autônomos e centros de controle de tráfego39. Em alguns casos, ainda, as informações coletadas durante o uso do automóvel são transferidas para centrais especializadas, como no caso do sistema europeu eCall, que aciona automaticamente os números de emergência se porventura se detectar a ocorrência de um sinistro, compartilhando os dados de localização40.

A utilização de veículos conectados tem um impacto significativo na segurança de dados pessoais, apesar de seus potenciais benefícios. A interconexão entre

---

37. Sunny Kumar, Eesha Goel, "Changing the world of Autonomous Vehicles using Cloud and Big Data", *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT),* (Setembro 2018): 369. https://doi.org/10.1109/ICICCT.2018.8473347.

38. Herman Strange, *Machines that Think - History of Artificial Intelligence: Navigating the Ethical*, *Societal, and Technical Dimensions of AI Development* (PN Books, 2023), Kindle, 42.

39. Rannenberg, "Opportunities and Risks", 503-504.

40. Rannenberg, "Opportunities and Risks", 499.

veículos pode ser essencial para que a direção autônoma prospere, já que é imprescindível que os automóveis se comuniquem para trocar informações sobre o tráfego41 e para aumentar a segurança rodoviária. Entretanto, a interconexão entre veículos por redes de comunicação poderia agravar os riscos relacionados à segurança do sistema, uma vez que os deixariam expostos a pessoas externas e a pessoas mal-intencionadas da própria rede42.

A conexão constante com smartphones e outros dispositivos eletrônicos também pode ser um problema, visto que torna o sistema autônomo vulnerável a ataques cibernéticos. Um ataque cibernético poderia causar diversas ameaças à segurança, como falhas propositais no sistema, vazamento de dados, roubo de identidade, stalking e rastreamento do veículo43. As vulnerabilidades dos sistemas de inteligência artificial a ataques cibernéticos, como hacking e malware, tornam possível o comprometimento da confidencialidade, integridade e disponibilidade dos dados44, pilares da segurança da informação.

Para Mansi Girdhar, Junho Hong e John Moore45, as falhas de segurança relacionadas às inteligências artificiais podem ampliar a superfície de ataque e aumentar a probabilidade de que haja ataques físicos e cibernéticos em carros autônomos, ao explorarem vulnerabilidades que são específicas dos sistemas de aprendizado da máquina e falhas de software e hardware em sistemas digitais. Seriam

41. Hataba et al., “Security and Privacy Issues”, 811-812.
42. Hataba et al., “Security and Privacy Issues”, 811-812.
43. Hataba et al., “Security and Privacy Issues”, 812.
44. Strange, *Machines that Think,* Kindle, 42.
45. Mansi Girdhar, Junho Hong, e John Moore, “Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models”, *IEEE Open Journal of Vehicular Technology* 4, (Abril 2023): 426. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10097455.

exemplos desses riscos de segurança e vulnerabilidades associados a carros autônomos: interferência nos sensores; sobrecarregamento do sistema com dados de fontes ilegítimas, impedindo o sistema autônomo de receber ou processar informações legítimas; manipulação dos meios de comunicação; vazamento de dados46.

Os autores classificam em dois os tipos de ameaças relacionadas à inteligência artificial: intencionais e não-intencionais47. Intencionais seriam aquelas ameaças que ocorrem quando há a exploração de vulnerabilidades técnicas da inteligência artificial com o fim específico de intervir no seu sistema e prejudicar operações de segurança. Exemplificam com o caso em que alguém pinta as faixas da pista ou cobrem placas de trânsito, situação que pode levar o sistema autônomo ao cometimento de erros48.

Já os riscos não-intencionais podem se referir ao mau funcionamento ou a falhas causadas pelos algoritmos. Exemplo dessa hipótese é o caso em que o veículo está diante de um cenário crítico e tem dificuldade na tomada de decisões, pelo fato de que o sistema não foi alimentado com aquela previsão, não estando o respectivo cenário dentro daqueles previstos na fase de programação49.

Sendo intencionais ou não, muitos são os riscos que envolvem a utilização de veículos autônomos, havendo diversos desafios em matéria de proteção de dados e cibersegurança relacionados ao uso dessa tecnologia, como: a grande quantidade de dados processados; a forma de armazenamento desses dados; o acesso à nuvem por múltiplas partes; a conexão entre veículos e entre veículos e o meio; a constante

46. Girdhar et al., “Cybersecurity of Autonomous Vehicles”, 426-427.
47. Girdhar et al., “Cybersecurity of Autonomous Vehicles”, 426.
48. Girdhar et al., “Cybersecurity of Autonomous Vehicles”, 426.
49. Girdhar et al., “Cybersecurity of Autonomous Vehicles”, 426.

conexão com a internet; a conexão com smartphones; falhas técnicas ou má-programação. Todos esses são exemplos de fatores que podem trazer riscos à segurança dos dados na utilização de carros autônomos, explorando vulnerabilidades específicas e ameaçando os pilares da segurança da informação.

### 3.3. O presente e o futuro da proteção de dados nos veículos autônomos

Diante da abundância de dados coletados durante o uso de veículos autônomos, sendo parte deles dados pessoais, urge a necessidade do estabelecimento de regras harmonizadas para garantir a proteção de dados dos titulares, nesse contexto. Questiona-se se as normativas já existentes na União Europeia são suficientes para abarcar esse recente cenário.

O RGPD, apesar de não tratar especificamente sobre a matéria em questão, define as regras sobre o tratamento de dados na União Europeia, com vistas à proteção de dados pessoais dos titulares de uma maneira ampla. Essa proteção estabelecida pelo RGPD se estende a todos os âmbitos, inclusive aos ambientes automatizados[50].

O RGPD define os princípios que devem ser observados no tratamento de dados pessoais, estabelece as condições para um tratamento de dados lícito e concede uma série de direitos aos titulares de dados pessoais[51], permitindo-os ter um maior controle sobre seus dados.

50. Regulamento (UE) 2016/679, RGPD.
51. Regulamento (UE) 2016/679, RGPD.

O Regulamento também determina a necessária observância da proteção de dados pessoais desde a concepção e por defeito, e impõe a obrigatoriedade da elaboração de uma avaliação de impacto quando se tratar de novas tecnologias que impliquem em alto risco para os direitos das pessoas singulares. Ainda, prevê mecanismos que ofereçam segurança ao tratamento de dados, como a pseudonimização e a cifragem dos dados. Essas, dentre outras determinações previstas no RGPD, passam a limitar o uso desenfreado de dados pessoais, com vistas a garantir o direito à proteção dos dados dos titulares[52].

A Resolução do Parlamento Europeu, de 15 de janeiro de 2019, sobre a condução autónoma nos transportes europeus (2018/2089(INI)) conta com disposições referentes à privacidade e proteção de dados no contexto dos transportes autônomos. A Resolução defende a importância de se garantir o acesso e o controle dos dados pessoais e os dados de bordo produzidos por carros autônomos pelos seus utilizadores[53]. Também, dispõe sobre a necessidade de proteção máxima dos consumidores no que concerne à cibersegurança, bem como realça que a proteção aos dados sensíveis e à vida privada deverão ser prioridade absoluta[54].

A Resolução legislativa do Parlamento Europeu, de 13 de março de 2024, sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) estabelece, de forma específica, regras a serem aplicadas à

52. Regulamento (UE) 2016/679, RGPD.
53. "Resolução do Parlamento Europeu, de 15 de janeiro de 2019, sobre a condução autónoma nos transportes europeus (2018/2089(INI))." Jornal Oficial da União Europeia, 27 de novembro de 2020, C 411, p. 2-12. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A52019IP0005.
54. Resolução do Parlamento Europeu (2018/2089(INI)).

concepção, desenvolvimento e utilização de sistemas de inteligência artificial, com o intuito de incentivar o desenvolvimento tecnológico e controlar os riscos trazidos por ele[55].

A legislação recém-aprovada prevê a necessidade de se observar a proteção de dados pessoais desde a concepção e durante todo o ciclo de vida do sistema de IA, bem como o princípio da minimização dos dados. Para assegurar que haja a observância a esses princípios, prevê a utilização, por parte dos fornecedores, de métodos como a anonimização e a cifragem de dados. A utilização de tecnologias que permitam o treinamento dos sistemas de IA sem que haja a necessidade de cópia ou transferência dos dados para outros locais, mantendo-os localmente, também é um método de segurança previsto pelo novo Regulamento[56].

O Regulamento de IA realiza uma abordagem pelo risco para classificar os diferentes sistemas de IA, e dedica todo um capítulo à regulamentação de sistemas de risco elevado. Esses são previstos no artigo 6.º e no anexo III do Regulamento de IA e são aqueles que podem trazer riscos significativos para a saúde, segurança ou direitos fundamentais. Como exemplos de sistemas de risco elevado estão o tratamento de dados de identificação biométrica e gestão e funcionamento de infraestruturas críticas, incluindo o trânsito rodoviário[57].

---

55. "Resolução legislativa do Parlamento Europeu, de 13 de março de 2024, sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da união (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))." Parlamento Europeu, 13 de março de 2024, p. 1-459. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PT.pdf.
56. Regulamento de Inteligência Artificial.
57. Regulamento de Inteligência Artificial.

Também, dispõe sobre a necessidade de cumprimento de uma série de requisitos para a colocação no mercado de sistemas de IA com risco elevado. Prevê que, nesse cenário, os fornecedores terão obrigações específicas durante todo o ciclo de vida do sistema de inteligência artificial, com vistas a garantir que seja seguro e em conformidade com a legislação[58].

O artigo 26.º (9) do Regulamento de IA dispõe que, no caso dos sistemas de IA com risco elevado, deverá ser feita uma avaliação de impacto sobre a proteção de dados, nos termos da RGPD[59]. Além disso, estão previstos ambientes de testagem que proporcionem um ambiente controlado para o desenvolvimento seguro de sistemas de IA antes da colocação no mercado[60].

O Comité Europeu para a Proteção de Dados (CEPD), ao publicar as Diretrizes 01/2020, em 9 de março de 2021, trouxe recomendações específicas sobre o tratamento de dados pessoais no contexto dos veículos conectados. As Diretrizes se referem ao tratamento de dados pessoais em contexto não profissional, abrangendo os dados que são tratados no interior do veículo, os que são compartilhados entre o veículo e outros dispositivos pessoais conectados, e aqueles colhidos pelos veículos e exportados para outras entidades com o fim de tratamento posterior[61].

Nas recomendações trazidas pelo Comitê, foram destacadas três categorias de dados pessoais a terem atenção priorizada pelos responsáveis pelo tratamento:

58. Regulamento de Inteligência Artificial.
59. Regulamento de Inteligência Artificial.
60. Regulamento de Inteligência Artificial.
61. "Diretrizes 01/2020 relativas ao tratamento de dados pessoais no contexto dos veículos conectados e das aplicações relacionadas com a mobilidade." European Data Protection Board, 9 de março de 2021, p. 1-37. https://www.edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_pt.pdf.

dados de localização, dados biométricos (assim como todas as categorias especiais de dados destacadas no artigo 9.º da RGPD) e dados que possam revelar infrações de trânsito[62].

A especial atenção em relação aos dados de localização, de acordo com o Comitê, se justificaria pelo fato de que podem ser informações que revelam hábitos da vida dos seus titulares, como onde moram, local em que trabalham, religião e orientação sexual, devendo, assim, ser recolhidos apenas se forem realmente essenciais para a finalidade do tratamento[63].

No que diz respeito à utilização de dados biométricos, segundo as recomendações trazidas pelo CEPD, deve-se garantir que o titular tenha total controle de seus dados, devendo ser oferecidas opções não-biométricas, como códigos ou chaves físicas, sem que haja restrições pelo não uso de biometria. Ainda, os dados biométricos devem ser armazenados de forma encriptada, com o tratamento sendo feito de forma local e não externa. No que concerne aos dados de infrações penais, o Comitê também recomenda a utilização de tratamento local, podendo o titular ter controle total desses dados[64].

O CEPD destaca a obrigatoriedade que os responsáveis pelos tratamentos de dados pessoais têm, no contexto de veículos conectados, de garantir o respeito à privacidade e proteção de dados, aplicando-se os conceitos previstos no RGPD relativos à proteção de dados desde a concepção e por defeito. Orienta o tratamento local, sempre que possível, dos dados pessoais, evitando a utilização de tratamento em nuvem diante dos riscos potenciais. Ainda, segundo o Comitê, deve haver a

62. Diretrizes 01/2020.
63. Diretrizes 01/2020.
64. Diretrizes 01/2020.

possibilidade de que os utilizadores determinem qual será a forma como seus dados pessoais serão recolhidos e tratados, devendo as informações sobre o tratamento serem apresentadas de forma clara e na língua do condutor[65].

O Comitê prevê uma série de recomendações relacionadas aos direitos dos titulares de dados, como: a possibilidade aos titulares de dados de ativar ou desativar o tratamento de dados para cada finalidade e para cada responsável pelo tratamento; a possibilidade de apagamento dos dados pelo titular, considerando-se a finalidade jurídica do tratamento e a base legal; o acesso exclusivo ao utilizador a seus dados pessoais, não podendo haver transferência a terceiros; aos titulares, a garantia de acesso direto aos seus dados; a possibilidade de apagamento dos dados dos utilizadores antes da venda do veículo[66].

O CEPD, reconhecendo a impossibilidade de tratamento de dados localmente em algumas situações, prevê a possibilidade de um tratamento híbrido[67], hipótese em que os dados poderiam ser anonimizados antes de serem transferidos externamente, ou pseudonimizados, como forma de reduzir os riscos.

Ainda tratando sobre a segurança dos dados, o Comitê prevê alguns mecanismos de mitigação de riscos, destacando-se os seguintes: encriptação de canais de comunicação; implantação de um sistema de gestão de chaves de encriptação especificamente para cada veículo; encriptação de dados pessoais tratados externamente; autenticação de dispositivos que recebem dados; implantação de medidas que possibilitem aos fabricantes de veículos a correção de vulnerabilidades durante todo o período de vida útil do automóvel; utilização de meios de comunicação

65. Diretrizes 01/2020.
66. Diretrizes 01/2020.
67. Diretrizes 01/2020.

seguros e que sejam específicos para o transporte; criação de um sistema de alarme dedicado a possíveis ataques ao veículo; manutenção dos registros do veículo e dos acessos a seu sistema de informações[68].

Pelo exposto, o que se observa é que as normativas já existentes são amplas e estabelecem princípios, direitos, deveres e mecanismos de mitigação de riscos, com vistas à proteção dos dados pessoais, podendo ser aplicadas ao contexto dos veículos autônomos e conectados, até que sejam criadas normativas específicas, se assim ocorrer.

### 3.4. Propostas de medidas técnicas de privacidade

O RGPD estabelece a necessidade de que sejam observados dois princípios essenciais para a proteção de dados pessoais, sendo o princípio da proteção de dados desde a concepção e o princípio da proteção de dados por defeito[69]. Quando se fala em proteção de dados desde a concepção, fala-se na adoção de medidas técnicas e organizativas desde o início das operações de tratamento[70]. Quando se fala na proteção de dados por defeito, fala-se na garantia do mais alto nível de proteção aos dados pessoais, observando-se, por exemplo, a quantidade de dados tratados, a necessidade de seu tratamento, a extensão de seu tratamento, o tempo e prazo de conservação desses dados, e o acesso a eles[71].

---

68. Diretrizes 01/2020.
69. Regulamento (UE) 2016/679, RGPD.
70. Comissão Europeia, "O que significa a proteção de dados «desde a conceção» e «por defeito»?," acessado em Maio 29, 2024, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_pt.
71. Regulamento (UE) 2016/679, RGPD.

Para assegurar que sejam cumpridos esses princípios, o Regulamento estabelece a necessidade da adoção de medidas técnicas e organizativas, que incluem: a pseudonimização de dados, a cifragem de dados, a transparência no tratamento dos dados, a possibilidade de controle dos dados pessoais por parte do titular e a criação e melhora constante de sistemas de segurança[72]. Essas medidas ajudam a garantir a aplicação dos princípios previstos no RGPD, como o princípio da minimização de dados.

No contexto dos veículos autônomos, em que são tratados dados em grande escala, o cumprimento dos princípios previstos no RGPD pode se tornar um grande desafio para os agentes de tratamento, aumentando-se as chances de que haja vazamentos de dados ou outras formas de violações aos direitos dos titulares. Diante disso, torna-se de extrema importância a implantação de medidas técnicas para observar os princípios da proteção de dados pessoais antes mesmo de iniciado o tratamento.

Nesse contexto, alguns mecanismos, como a pseudonimização de dados pessoais, podem reduzir as chances de ocorrência de eventual violação à proteção dos dados dos titulares. A pseudonimização refere-se à técnica que impede que os dados pessoais possam ser vinculados a seus titulares, exceto caso haja o contato com outras informações adicionais que devem ser mantidas separadamente[73]. É possível a identificação do titular caso os dados identificadores sejam vinculados novamente a ela; por isso, pode ser considerada uma criptografia parcial[74]. Assim,

72. Regulamento (UE) 2016/679, RGPD.
73. Regulamento (UE) 2016/679, RGPD.
74. Tomáš Pikulík, "GDPR Compliant Methods of Data Protection", *6th SWS International Scientific Conference on Social Sciences ISCSS 2019*, (Agosto 2019): 4. http://dx.doi.org/10.5593/SWS.ISCSS.2019.2/S05.069.

é uma medida que traz uma camada de proteção aos dados pessoais, ainda que não os blinde completamente.

Outra medida extremamente importante para proteção dos dados pessoais é a cifragem de dados[75], que se refere à situação em que os dados são codificados, sendo que apenas pessoas autorizadas podem ter acesso[76]. Com a cifragem, os dados são transformados em códigos, de modo que o acesso ao seu conteúdo é possível apenas com a utilização de uma chave de acesso ou similar, tornando as informações ininteligíveis às pessoas não autorizadas[77]. Assim, mesmo em caso de violações à segurança dos dados, como nos casos de vazamentos ou ciberataques, eles ficam inacessíveis, garantindo sua segurança e o cumprimento ao disposto no artigo 32.º do RGPD[78].

O Regulamento de IA, além das medidas já mencionadas, prevê que sejam utilizadas técnicas de programação da IA que não exijam a cópia de dados pessoais ou sua transferência a outras partes[79], como o que ocorre quando é utilizada nuvem de armazenamento, tornando o tratamento mais seguro.

As Diretrizes 01/2020 sobre veículos conectados orientam a utilização de tratamento de dados local, evitando-se a externalização, principalmente quando diz respeito a dados biométricos – e outros dados de categorias especiais -, e dados de infração de trânsito. Porém, como bem previsto pelo CEPD na elaboração das Diretrizes, pode haver a impossibilidade de tratamento de dados apenas localmente,

75. Regulamento (UE) 2016/679, RGPD.
76. Comissão Europeia, "O que significa a proteção de dados."
77. Pikulík, "GDPR Compliant Methods", 4.
78. Pikulík, "GDPR Compliant Methods", 4.
79. Regulamento Inteligência Artificial.

hipótese em que sugere a adoção de um tratamento híbrido[80]. Se assim for, os dados devem ser anonimizados ou pseudonimizados antes de externalizados.

De acordo com relatório da OCDE, em que pese grande parte dos dados hoje serem tratados externamente, possivelmente haverá uma transição do tratamento em nuvem para tratamento local nos próximos anos, podendo, então, dar-se no próprio dispositivo[81]. O tratamento local pode apresentar uma segurança a mais, visto que não há a necessidade de exteriorizar o tratamento, dando um maior controle ao titular sobre os seus dados. Além das benesses relacionadas à proteção de dados, o tratamento no próprio dispositivo também poderá ser um benefício na questão da rapidez das respostas do sistema, por redução da distância de processamento[82].

Todos os mecanismos citados podem levar a uma maior proteção aos dados pessoais no contexto dos veículos autônomos, por garantirem o cumprimento aos princípios previstos nas legislações da União Europeia, principalmente no RGPD, reduzindo-se, assim, as chances de violações aos direitos e liberdades das pessoas singulares.

## 4. Conclusão

A crescente busca pelo desenvolvimento e implantação de veículos autônomos tem feito emergir diversas questões relacionadas à privacidade e proteção de dados decorrentes da utilização dessa nova tecnologia. Isso, porque esses

80. Diretrizes 01/2020.
81. OECD, "Data in an evolving technological landscape: The case of connected and automated vehicles," *OECD Digital Economy Papers*, no. 346 (Dezembro 2022): 13. https://doi.org/10.1787/ec7d2f6b-en.
82. OECD, "Data in an evolving technological landscape," 13.

automóveis são frequentemente equipados com uma gama de sensores e de câmeras, coletando uma vasta quantidade de dados do meio.

Também, os carros autônomos utilizam-se das mais modernas técnicas de inteligência artificial, como o *Machine Learning* e o *Deep Learning*, que requerem o processamento de uma grande gama de dados para o treinamento da tecnologia e para possibilitar o processo decisório autônomo. O advento dos veículos conectados, que torna o compartilhamento de dados costumaz, contribui para o aumento da quantidade de dados acessados durante o uso de um carro autônomo.

Grande parte desses dados são pessoais, como dados biométricos, dados de localização, dados de identificação, dados sobre o comportamento do usuário ou proprietário do veículo, dentre outros. Diante do grande montante de dados processados, eles são frequentemente armazenados em nuvens, sendo o tratamento realizado externamente, o que levanta dúvidas quanto à sua segurança.

Eventual violação de dados nesse contexto poderia ser extremamente grave, já que são diversos os dados coletados, processados e armazenados, tirando o controle dos dados por parte de seus titulares. Também, a constante conexão com *smartphones* e com a *internet* aumenta e facilita a chance de ocorrência de ciberataques, o que poderia comprometer toda a segurança viária.

Em que pese toda a problemática envolvendo os carros sem motorista, eles prometem trazer grandes benefícios à sociedade. Também, não é possível e nem viável impedir a evolução tecnológica. Portanto, necessário se faz a criação de mecanismos que possam mitigar os riscos que advenham dessas inovações, para que os direitos e liberdades das pessoas singulares sejam respeitados.

Em que pese não haver legislação específica que se refira ao tratamento de dados pessoais em veículos autônomos no âmbito da União Europeia, há legislações já existentes que podem ser aplicadas como forma de proteção aos titulares de dados pessoais nesse contexto, como é o exemplo do RGPD.

A aplicação dos princípios de proteção de dados, como o princípio da proteção de dados desde a concepção e por defeito, da minimização de dados, da finalidade, da limitação da conservação, da transparência; bem como a utilização de mecanismos técnicos de segurança, como a pseudonimização e a cifragem de dados, e mecanismos organizativos, como a constante conformidade com as legislações por parte das empresas e a realização de Avaliação de Impacto sobre a Proteção de Dados, são formas de mitigar os riscos existentes relacionados à proteção de dados pessoais no cenário dos veículos autônomos.

Ainda, o tratamento local de dados pessoais, sem que seja necessária a transferência para locais externos, como ocorre no caso de utilização de sistemas de armazenamento em nuvem, pode ajudar a reduzir os riscos de violações a dados pessoais, dando mais controle ao titular. Caso não seja possível o tratamento totalmente a bordo, a realização de tratamento híbrido pode ser uma boa solução temporária, com a pseudonimização ou cifragem dos dados que forem externalizados.

Porém, ainda que já existam legislações rígidas quanto à proteção de dados pessoais de forma ampla, e mesmo que sejam criadas legislações mais específicas para regulamentar os veículos autônomos e tratar das questões relacionadas à proteção de dados pessoais, para que efetivamente os direitos sejam protegidos, deve haver a real colaboração de diversos agentes que estão envolvidos, como os órgãos reguladores, as autoridades fiscalizadoras, os agentes de tratamento, os usuários da tecnologia, dentre outros.

Assim, por meio do estabelecimento e do respeito às legislações sobre proteção de dados, do cumprimento às obrigações estabelecidas nelas e da realização das boas práticas de governança, pode-se chegar ao caminho de uma abordagem equilibrada entre inovação e proteção de dados, dando uma maior confiança à população sobre a utilização de veículos autônomos.

## Referências bibliográficas

Ana Frazão, "Algoritmos e inteligência artificial: repercussões da sua utilização sobre a responsabilidade civil e punitiva das empresas," Professora Ana Frazão, 16 de maio de 2018, http://professoraanafrazao.com.br/files/publicacoes/2018-05-16-Algoritmos_e_inteligencia_artificial.pdf.

Bloom, Cara, Joshua Tan, Javed Ramjohn, e Lujo Bauer. "Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles." *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, (Julho 2017): 357-375. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bloom.

Blunt, Matthew. "Highway to a Headache: Is Tort-Based Automotive Insurance on a Collision Course with Autonomous Vehicles." *Willamette Law Review* 53, no. 2 (2017): 107-136. https://heinonline.org/HOL/Page?handle=hein.journals/willr53&div=9&g_sent=1&casa_token=.

Deutschland. "Eight Act amending the Road Traffic Act, section 1a." Federal Law Gazette I, 2017. https://bmdv.bund.de/SharedDocs/EN/Documents/DG/eight-act-amending-the-road-traffic-act.pdf?__blob=publicationFile.

"Diretrizes 01/2020 relativas ao tratamento de dados pessoais no contexto dos veículos conectados e das aplicações relacionadas com a mobilidade." European Data Protection Board, 9 de março de 2021, p. 1-37. https://www.edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_pt.pdf.

Engländer, Armin. "O veículo autônomo e o tratamento de situações dilemáticas." Em *Veículos autônomos e direito penal,* organizado por Heloisa Estellita e Alaor Leite, 86-108. São Paulo: Marcial Pons, 2019.

Faria, Paula Ribeiro de. "Os veículos autónomos e o direito penal." Em *Estudos em homenagem ao Conselheiro Presidente Manuel da Costa Andrade vol. II,* organizado por Pedro Machete, Gonçalo de Almeida Ribeiro e Mariana Canotilho, 365-417. Coimbra: Almedina, 2023.

Girdhar, Mansi, Junho Hong, e John Moore. "Cybersecurity of Autonomous Vehicles: A Systematic Literature Review of Adversarial Attacks and Defense Models." *IEEE Open Journal of Vehicular Technology* 4, (Abril 2023): 417-437. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10097455.

Giuffrida, Iria. "Liability for AI Decision-Making: Some Legal and Ethical Considerations." *Fordham Law Review* 88, no. 2 (2019): 439-456. https://ir.lawnet.fordham.edu/flr/vol88/iss2/3/.
Gless, Sabine, Thomas Weigend. "Agentes inteligentes e o direito penal." Em *Veículos autônomos e direito penal,* organizado por Heloisa Estellita e Alaor Leite, 37-64. São Paulo: Marcial Pons, 2019.
"Global status report on road safety 2023," World Health Organization, acessado em Maio 29, 2024, https://www.who.int/publications/i/item/9789240086517.
Hataba, Muhammad, Ahmed Sherif, Mohamed Mahmoud, Mohamed Abdallah, e Waleed Alasmary. "Security and Privacy Issues in Autonomous Vehicles: A Layer-Based Survey." *IEEE Open Journal of the Communications Society* 3, (Abril 2022): 811-829. https://doi.org/10.1109/OJCOMS.2022.3169500.
Hristozov, Anton. "The role of artificial intelligence in autonomous vehicles." Embedded. Última modificação 15 de julho de 2020. https://www.embedded.com/the-role-of-artificial-intelligence-in-autonomous-vehicles/.
Kröger, Fabian. "Automated Driving in Its Social, Historical and Cultural Contexts." Em *Autonomous Driving: Technical, Legal and Social Aspects*, editado por Markus Maurer, Joseph Christian Gerdes, Barbara Lenz, Hermann Winner, 41-68. Berlim: SpringerOpen, 2016. PDF.
Krontiris, Ioannis, Kalliroi Grammenou, Kalliopi Terzidou, Marina Zacharopoulou, Marina Tsikintikou, Foteini Baladima, Chrysi Sakellari, e Konstantinos Kaouras. "Autonomous vehicles: Data protection and ethical considerations." *Proceedings of the 4th ACM Computer Science in Cars Symposium (CSCS '20)*, (Dezembro 2020): 1-10. https://doi.org/10.1145/3385958.3430481.
Kumar, Sunny, Eesha Goel. "Changing the world of Autonomous Vehicles using Cloud and Big Data." *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT),* (Setembro 2018): 368-376. https://doi.org/10.1109/ICICCT.2018.8473347.
OECD. "Data in an evolving technological landscape: The case of connected and automated vehicles." *OECD Digital Economy Papers*, no. 346 (Dezembro 2022): 1-33. https://doi.org/10.1787/ec7d2f6b-en.
"O que significa a proteção de dados «desde a conceção» e «por defeito»?," Comissão Europeia, acessado em Maio 29, 2024, https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_pt.
Pikulík, Tomáš. "GDPR Compliant Methods of Data Protection." *6th SWS International Scientific Conference on Social Sciences ISCSS 2019*, (Agosto 2019): 1-10. http://dx.doi.org/10.5593/SWS.ISCSS.2019.2/S05.069.
"Plano Global: década de ação pela segurança no trânsito 2021-2030," World Health Organization, acessado em Maio 29, 2024, https://cdn.who.int/media/docs/default-source/documents/health-topics/road-traffic-injuries/global-plan-for-the-doa-of-road-safety-2021-2030-pt.pdf?sfvrsn=65cf34c8_33&download=true.

Rannenberg, Kai. "Opportunities and Risks Associated with Collecting and Making Usable Additional Data." Em *Autonomous Driving: Technical, Legal and Social Aspects*, editado por Markus Maurer, Joseph Christian Gerdes, Barbara Lenz, Hermann Winner, 497-522. Berlim: SpringerOpen, 2016. PDF.

Rao, Sabbani Venkata Achuta, K. Kondaiah, G. Rajesh Chandra, e K. Kiran Kumar. "A Survey on Machine Learning: Concept, Algorithms and Applications." *International Conference on Innovative Research in Computer and Communication Engineering February,* (Fevereiro 2017): 1301-1309. https://www.smec.ac.in/assets/images/committee/research/17-18/282.A%20Survey%20on%20Machine%20Learning%20Concept,.pdf.

"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 (Regulamento Geral sobre a Proteção de Dados)." Jornal Oficial da União Europeia, 4 de maio de 2016, L 119, p. 1-88. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679.

Resolução do Parlamento Europeu, de 15 de janeiro de 2019, sobre a condução autónoma nos transportes europeus (2018/2089(INI))." Jornal Oficial da União Europeia, 27 de novembro de 2020, C 411, p. 2-12. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A52019IP0005.

"Resolução do Parlamento Europeu, de 20 de janeiro de 2021, sobre a inteligência artificial: questões de interpretação e de aplicação do direito internacional na medida em que a UE é afetada nos domínios da utilização civil e militar e da autoridade do Estado fora do âmbito da justiça penal (2020/2013(INI))." Parlamento Europeu, 20 de janeiro de 2021, p. 1-19. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_PT.html.

"Resolução legislativa do Parlamento Europeu, de 13 de março de 2024, sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da união (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))." Parlamento Europeu, 13 de março de 2024, p. 1-459. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_PT.pdf.

**"**Road safety factsheet: autonomous vehicles," The Royal Society for the Prevention of Accidents, acessado em Maio 29, 2024. https://www.rospa.com/media/documents/road-safety/factsheets/autonomous-vehicles.pdf.

Shinde, Pramila. P., Seema Shah. "A Review of Machine Learning and Deep Learning Applications." *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, (Abril 2019): 1-6. https://doi.org/10.1109/ICCUBEA.2018.8697857.

"Sobre nós," SAE International, acessado em Abril 15, 2024, http://br.sae.org/about/.

Stecklow, Steve, Waylon Cunningham, e Hyunjoo Jin. "Tesla workers shared sensitive images recorded by customer cars." Reuters. Última modificação 6 de abril de 2023. https://www.reuters.com/technology/tesla-workers-shared-sensitive-images-recorded-by-customer-cars-2023-04-06/.

Strange, Herman. *Machines that Think - History of Artificial Intelligence: Navigating the Ethical*, *Societal, and Technical Dimensions of AI Development*. PN Books, 2023. Kindle.
Taeihagh, Araz, Hazel Si Min Lim. "Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks." *Transport reviews* 39, no. 1 (Julho 2018): 103-128. https://doi.org/10.1080/01441647.2018.1494640.
"Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles J3016_202104," SAE International, acessado em Abril 15, 2024, https://www.sae.org/standards/content/j3016_202104.
Vakulov, Alex. "Addressing Data Processing Challenges in Autonomous Vehicles." IoT For All. Última modificação 5 de fevereiro de 2024. https://www.iotforall.com/addressing-data-processing-challenges-in-autonomous-vehicles.