Dados OBD-II como prova digital em processo judicial: Os requisitos técnicos, jurídicos e éticos da análise forense automóvel

OBD-II data as digital evidence in legal proceedings: The technical, legal, and ethical requirements of automotive forensic analysis

10.29073/j2.v7i1.1126

Recebido: 01 de março de 2026.
Aprovado: 01 de abril de 2026.
Publicado: 04 de abril de 2026.

Autor/a: Vítor Ruivo, ESTG-IPP, Portugal, ruivovitor@gmail.com.

Resumo

A digitalização dos automóveis modernos transformou-os em plataformas computacionais que geram, em tempo real, volumes substanciais de dados operacionais com potencial forense considerável. Entre os sistemas de diagnóstico disponíveis, o protocolo OBD-II destaca-se pela sua universalidade: obrigatoriamente implementado em todos os veículos ligeiros vendidos na União Europeia desde 2001, oferece acesso normalizado a parâmetros de velocidade, aceleração, códigos de avaria e registos de freeze frame que podem ser determinantes na reconstituição de acidentes e na instrução de processos de responsabilidade civil. O ordenamento jurídico português, todavia, não prevê qualquer regulamentação específica sobre a admissibilidade e os requisitos de recolha destes dados como prova judicial. O presente estudo identifica essa lacuna, analisa as condições em que os dados OBD-II podem constituir prova digital admissível à luz do Código de Processo Civil, do Regulamento Geral sobre a Proteção de Dados e do Regulamento eIDAS, estabelece os requisitos técnicos de integridade forense, e formula propostas concretas de intervenção normativa. A análise é completada por um framework ético que operacionaliza os princípios da minimização e do privacy by design, e pela apresentação de uma solução técnica empiricamente validada que alcançou taxas de sucesso de 98,2% na extração de dados e 98,9% de concordância com sistemas de referência.

Palavras-Chave: Análise Forense Digital; OBD-II; Prova Digital; Responsabilidade Civil; RGPD.

Abstract

The digitization of modern automobiles has transformed them into computational platforms that generate substantial volumes of operational data in real time, with considerable forensic potential. Among the available diagnostic systems, the OBD-II protocol stands out for its universality: mandatory in all light vehicles sold in the European Union since 2001, it offers standardized access to speed, acceleration, fault codes, and freeze frame records that can be crucial in accident reconstruction and in civil liability proceedings. However, Portuguese law does not provide any specific regulations on the admissibility and requirements for collecting this data as judicial evidence. This study identifies this gap, analyzes the conditions under which OBD-II data can constitute admissible digital evidence in light of the Code of Civil Procedure, the General Data Protection Regulation, and the eIDAS Regulation, establishes the technical requirements for forensic integrity, and formulates concrete proposals for regulatory intervention. The analysis is complemented by an ethical framework that operationalizes the principles of minimization and privacy by design, and by the presentation of an empirically validated technical solution that achieved success rates of 98.2% in data extraction and 98.9% agreement with reference systems.

Keywords: Civil Liability; Digital Evidence; Digital Forensic Analysis; GDPR; OBD-II.

1. Introdução

Em novembro de 2019, a Comissão Nacional de Proteção de Dados publicou uma decisão sobre a utilização de dados de geolocalização de frotas automóveis. A decisão reconhecia o potencial dos dados automóveis para fins legítimos, mas advertia para os riscos de vigilância desproporcionada. O mesmo dilema que ocupava a CNPD no contexto das frotas comerciais coloca-se, com intensidade ainda maior, no contexto da prova forense: os dados que o automóvel regista continuamente podem ser o instrumento mais objetivo e preciso para reconstituir o que aconteceu num acidente, mas são também, potencialmente, uma janela de observação altamente intrusiva sobre o comportamento de condução de cada cidadão.

O protocolo OBD-II (On-Board Diagnostics II) está no centro deste dilema. Obrigatoriamente implementado em todos os veículos ligeiros comercializados na União Europeia desde 2001, permite aceder, através de um conector normalizado, a dezenas de parâmetros operacionais em tempo real: a velocidade, a posição do acelerador, o estado dos travões, a ativação dos sistemas de segurança, os erros detetados pelos sistemas de diagnóstico e os registos de freeze frame que capturam as condições de funcionamento do veículo no momento exato em que uma anomalia é registada.[1]

O interesse probatório destes dados é evidente. A velocidade excessiva, a falha de travagem, o estado dos airbags ou a ativação automática de travagem de emergência podem ser determinantes na atribuição de responsabilidade civil num acidente de viação. O problema não reside na existência destes dados, que existe e é crescente. O problema reside na ausência de um quadro normativo que defina as condições da sua utilização como prova judicial, os requisitos técnicos que asseguram a sua integridade, e as salvaguardas éticas que previnem utilizações desproporcionadas.

Essa lacuna não é inocente. Cada acidente de viação em que os dados OBD-II poderiam ser probatórios, mas não são utilizados por falta de protocolo, é uma oportunidade perdida para a administração da justiça. Cada utilização desses dados sem garantias técnicas adequadas é um risco de prova inválida ou manipulável. Cada recolha sem fundamento jurídico expresso é uma potencial violação de dados pessoais. O estado atual do direito português deixa todas estas questões em aberto.

O presente artigo procura contribuir para o preenchimento destas lacunas. A estrutura segue a lógica do problema: começa por descrever o fenómeno técnico com o rigor mínimo necessário à compreensão jurídica (secção 2), passa pelas condições de admissibilidade no processo civil português (secção 3), depois pelos requisitos técnicos de integridade forense (secção 4), seguindo-se a análise da dimensão ética (secção 5), e termina com as propostas de reforma normativa (secção 6) e as conclusões (secção 7). Atravessa estas secções uma interrogação de fundo: pode o direito continuar a ignorar o automóvel como fonte de prova digital quando a ciência demonstrou que ele regista, com precisão e objetividade, o essencial do que acontece durante a condução?

O presente artigo tem origem na dissertação de mestrado do autor, intitulada *Análise Forense Digital a Automóveis – uma perspetiva técnica, jurídica e ética*, apresentada no âmbito do Mestrado em Práticas Jurídico-Digitais da Escola Superior de Tecnologia e Gestão do Instituto Politécnico do Porto, sob orientação do Professor Doutor António Alberto dos Santos Pinto e do Professor Doutor Pedro Miguel Dias Venâncio. O artigo retoma os contributos centrais dessa investigação — a sistematização do quadro normativo aplicável, o protocolo técnico de extração forense e o framework ético de categorização de dados — apresentando-os de forma autónoma e adaptada ao público de uma revista jurídica.

[1] A Diretiva 98/69/CE do Parlamento Europeu e do Conselho, de 13 de outubro de 1998, relativa a medidas a tomar contra a poluição do ar causada pelas emissões dos veículos a motor, impôs a implementação do OBD-II em todos os veículos ligeiros a gasolina vendida na UE desde 1 de janeiro de 2001 e nos veículos a gasóleo desde 1 de janeiro de 2004. O conector normalizado J1962 e o conjunto mínimo de PIDs obrigatórios resultam desta base regulatória.

2. O Automóvel como Plataforma Forense: O Protocolo OBD-II

2.1. Arquitetura Eletrónica e Sistemas de Diagnóstico Embarcados

A arquitetura eletrónica dos veículos modernos é organizada em domínios funcionais — motor, transmissão, chassis, segurança ativa e passiva, conforto e infotainment — geridos por ECUs (Electronic Control Units) que comunicam entre si através de redes internas. O protocolo CAN (Controller Area Network) é o mais difundido para sistemas de segurança e propulsão, garantindo comunicação determinística e tolerância a falhas. O FlexRay, de maior largura de banda, é utilizado em sistemas críticos como a direção ativa e os travões eletromecânicos. A Ethernet automóvel emerge nos veículos mais recentes para suportar os volumes de dados gerados pelos sistemas de assistência avançada à condução (ADAS).

O gateway central, presente na maioria dos veículos modernos, funciona como ponto de mediação entre os diferentes domínios, filtrando e encaminhando mensagens entre redes e gerindo o acesso externo pela interface OBD-II. É através deste gateway que um adaptador de diagnóstico externo, ligado ao conector normalizado, interage com os sistemas do veículo. Esta mediação é relevante para a forense digital porque o gateway pode filtrar, limitar ou registar os acessos externos, o que tem implicações tanto técnicas como jurídicas na cadeia de custódia.

2.2. Os Dados OBD-II e o Seu Potencial Probatório

O protocolo OBD-II disponibiliza três categorias de dados com relevância forense. Os PIDs (Parameter IDs) em tempo real incluem a velocidade (PID 0x0D), a carga do motor (0x04), a posição do acelerador (0x11), a temperatura do líquido de refrigeração (0x05) e dezenas de outros parâmetros cujos valores permitem reconstruir o comportamento do veículo num instante determinado.[2]

Os Diagnostic Trouble Codes (DTCs) são códigos alfanuméricos que registam anomalias detetadas pelos sistemas de diagnóstico. O DTC C1234, por exemplo, indica falha no sensor de velocidade de uma das rodas; o P0500 regista ausência de sinal do sensor de velocidade do veículo. Estes códigos permitem a reconstituição temporal de falhas técnicas anteriores ao evento, sendo frequentemente mais relevantes para a análise forense do que os parâmetros em tempo real.[3]

Os freeze frames constituem o terceiro tipo de dado relevante. Quando um DTC é registado, o sistema de diagnóstico congela automaticamente o estado dos PIDs nesse instante, criando uma fotografia digital das condições de funcionamento do veículo no momento da anomalia. Este mecanismo é de particular interesse forense porque capta o estado do veículo num momento crítico, independentemente de qualquer intervenção humana posterior.

O potencial probatório destes dados resulta de quatro características. Em primeiro lugar, a precisão: os sensores automóveis são calibrados para fins de segurança e de cumprimento de normas de emissões, garantindo elevado grau de exatidão. Em segundo lugar, a contemporaneidade do registo: os dados são gerados em tempo real pelos sistemas embarcados, sem intermediação humana. Em terceiro lugar, a dificuldade de manipulação retroativa quando protegidos por mecanismos criptográficos adequados. Em quarto lugar, a objetividade: ao contrário da

[2]Os Parameter IDs (PIDs) são identificadores numéricos que permitem consultar parâmetros específicos do motor e dos sistemas do veículo em tempo real. Os PIDs standard (definidos pela norma SAE J1979 e pela ISO 15031-5) são universais; os PIDs proprietários, definidos por cada fabricante, requerem descodificação específica e constituem um dos principais obstáculos técnicos à análise forense transversal. Para uma análise detalhada, *vide* Lopes, M. (2017). OBD-II: Metodologias de Recolha de Dados em Acidentes de Viação. Dissertação de Mestrado, Universidade do Porto.

[3]Os freeze frames constituem um mecanismo de registo automático: quando o sistema de diagnóstico deteta uma anomalia que justifica a criação de um DTC, congela simultaneamente o estado de um conjunto predefinido de PIDs nesse instante. Este registo é particularmente valioso para a análise forense porque capta as condições de funcionamento do veículo no momento crítico, mesmo que o DTC seja posteriormente apagado da memória.

prova testemunhal, sujeita às limitações da memória e da perceção, os dados do veículo registam o que o veículo fez e não o que as testemunhas julgam ter visto.

2.3. Distinção Face ao EDR e Limites Técnicos

Importa distinguir os dados OBD-II dos dados provenientes de Event Data Recorders (EDRs). Estes últimos são sistemas de registo de colisão, projetados especificamente para capturar dados de alta frequência nos segundos que precedem e sucedem um impacto, sendo obrigatórios nos veículos novos vendidos na UE desde 2022.[4] O EDR oferece maior resolução temporal e dados mais diretamente orientados para a análise de colisões, mas tem alcance temporal limitado e acesso técnico mais restrito. O OBD-II, por sua vez, oferece universalidade de acesso, histórico de manutenção alargado e contexto operacional contínuo, sendo complementar e não substituto do EDR.

Os limites técnicos do OBD-II são igualmente reais e devem ser reconhecidos em qualquer relatório forense. A fragmentação entre fabricantes na implementação de PIDs proprietários pode dificultar a interpretação de dados não standard. A volatilidade de alguns parâmetros, que são substituídos em memória quando novos eventos ocorrem, pode resultar em perda de informação se a extração não for realizada atempadamente. A ausência de logging contínuo em veículos sem EDR implica que os dados OBD-II descrevem o estado do veículo em determinados instantes, não uma linha temporal contínua. Estas limitações não invalidam o valor probatório dos dados, mas devem ser explicitamente documentadas na perícia.

3. Admissibilidade no Ordenamento Jurídico Português

3.1. O Princípio da Admissibilidade Ampla e o Dado Automóvel

O regime processual civil português assenta no princípio da admissibilidade ampla dos meios de prova, consagrado no artigo 411.º do CPC.[5] Este princípio permite a utilização de qualquer elemento com idoneidade demonstrativa, desde que obtido por meios lícitos. O dado automóvel recolhido em condições adequadas é, à luz deste preceito, admissível como prova documental eletrónica ou como objeto de prova pericial.

A qualificação jurídica mais adequada do dado OBD-II é a de documento eletrónico na aceção do artigo 362.º do Código Civil. A doutrina portuguesa tem desenvolvido o conceito de documento eletrónico a partir da distinção entre o suporte, o meio técnico que preserva a informação, e o conteúdo, a informação em si. A validade probatória do documento eletrónico depende da demonstração da autenticidade e integridade de ambas as dimensões.[6]

---

[4]O Event Data Recorder (EDR) é um sistema de registo de dados de colisão, obrigatório nos veículos ligeiros novos comercializados na União Europeia desde 2022 ao abrigo do Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019. O Regulamento Delegado (UE) 2024/2220 da Comissão, de 26 de julho de 2024, especifica os requisitos técnicos uniformes para estes dispositivos. Ao contrário do OBD-II, o EDR regista dados de alta frequência (tipicamente 100 Hz) nos segundos que precedem e sucedem uma colisão, mas não fornece histórico contínuo de funcionamento.

[5]O artigo 411.º do Código de Processo Civil consagra o princípio da aquisição processual da prova, determinando que o tribunal deve realizar ou ordenar, mesmo oficiosamente, todas as diligências necessárias ao apuramento da verdade e à justa composição do litígio. Este preceito, conjugado com o artigo 423.º, que admite documentos em qualquer fase do processo, fundamenta a admissibilidade ampla de meios de prova digitais.

[6]O conceito de documento eletrónico e o respetivo regime de autenticidade estão desenvolvidos em Andrade, F. (2021). Suporte e formato como elementos essenciais do documento eletrónico. *Revista da Ordem dos Advogados*, 81(3-4), 1150-1180. O autor distingue entre a validade do suporte (meio técnico que suporta a informação) e a integridade do conteúdo (imutabilidade da informação registada), concluindo que ambas as dimensões são necessárias à plena eficácia probatória do documento.

A jurisprudência portuguesa tem demonstrado crescente recetividade à prova digital tecnicamente fundamentada. O Tribunal da Relação de Évora, num acórdão recente[7], reconheceu expressamente que o hash criptográfico constitui garantia de integridade da prova digital equivalente à que a assinatura manuscrita confere ao documento em papel. Este entendimento, ainda que incipiente no contexto específico dos dados automóveis, fornece o fundamento jurisprudencial para a admissibilidade dos dados OBD-II quando dotados de adequadas garantias técnicas.

3.2. As Condições Cumulativas de Admissibilidade

A análise do quadro normativo multinível aplicável permite identificar quatro condições cumulativas para a admissibilidade dos dados OBD-II como prova em processo judicial.

A primeira condição é a licitude da obtenção. Os dados automóveis que incluam parâmetros identificáveis ao condutor, designadamente o VIN ou inferências comportamentais individualizadas, são dados pessoais na aceção do Regulamento (UE) 2016/679.[8] A sua recolha exige fundamento em base de licitude válida: o consentimento informado do titular, a autorização judicial, ou o interesse legítimo devidamente ponderado face aos direitos e liberdades do titular, com especial atenção ao princípio da proporcionalidade.

A segunda condição é a preservação da integridade. O dado automóvel deve ser recolhido e preservado através de mecanismos que garantam a sua inalterabilidade desde a extração até à apresentação em tribunal. Esta exigência é satisfeita pela aplicação de funções de hash criptográfico SHA-256 ou superior,[9] pela assinatura digital qualificada dos relatórios forenses nos termos do artigo 25.º do Regulamento eIDAS,[10] e pela manutenção de uma cadeia de custódia documentada segundo a norma ISO/IEC 27037:2012.[11]

A terceira condição é a autenticidade temporal. A data e hora da extração dos dados devem ser determináveis com exatidão e dotadas de eficácia legal. Esta exigência impõe a utilização de carimbos temporais qualificados, obtidos de uma Autoridade de Timestamping certificada ao abrigo do Regulamento eIDAS.[12] A utilização de

---

[7]O Acórdão do Tribunal da Relação de Évora, proferido no âmbito do processo 351/23.6JAFAR.E1, constitui uma referência relevante na jurisprudência portuguesa sobre prova digital. O Tribunal afirmou expressamente que "o código hash funciona como uma impressão digital da prova digital, garantindo que o conteúdo analisado é idêntico ao conteúdo original", fundamentando assim a presunção de integridade de documentos digitais dotados de hash criptográfico verificável.

[8]As Diretrizes 01/2020 do Comité Europeu para a Proteção de Dados (EDPB) sobre o tratamento de dados pessoais no contexto de veículos conectados e aplicações de mobilidade clarificam que o VIN, embora seja um identificador técnico do veículo, constitui dado pessoal quando permite a identificação indireta do condutor ou do proprietário. A mesma qualificação se aplica a dados de localização e a inferências comportamentais individualizadas.

[9]O SHA-256 (Secure Hash Algorithm 256-bit) é uma função de hash criptográfica da família SHA-2, publicada pelo National Institute of Standards and Technology norte-americano no FIPS PUB 180-4: *Secure Hash Standard (SHS)*. É recomendado para aplicações forenses por garantir resistência a colisões: a probabilidade de dois conjuntos de dados distintos produzirem o mesmo hash é computacionalmente negligenciável.

[10]O artigo 25.º do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014 (Regulamento eIDAS), estabelece que uma assinatura eletrónica qualificada tem efeito jurídico equivalente a uma assinatura manuscrita e que os Estados-Membros não podem recusar efeito jurídico a uma assinatura eletrónica qualificada. O artigo 41.º do mesmo Regulamento atribui ao carimbo temporal qualificado a presunção legal de exatidão da data e hora indicadas e de integridade dos dados associados.

[11]A norma ISO/IEC 27037:2012 — *Information technology — Security techniques — Guidelines for identification, collection, Acquisition and preservation of digital evidence* — estabelece os princípios e as boas práticas para a preservação de evidências digitais, com especial ênfase na cadeia de custódia, na autenticidade e na minimização da alteração das evidências durante o processo de recolha. A sua aplicação ao contexto forense automóvel foi analisada por Johansen, G. (2020). *Digital Forensics and Incident Response* (2.ª ed.). PacktPublishing.

[12]O RFC 3161: *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, define o protocolo de carimbo temporal que permite a uma Autoridade de Timestamping (TSA) certificar, com caráter irrefutável, que um determinado conjunto de

timestamps não qualificados, embora tecnicamente possível, não confere à prova a presunção legal de exatidão temporal estabelecida no artigo 41.º do Regulamento eIDAS.

A quarta condição é o respeito pelo princípio do contraditório. A parte contrária deve ter acesso aos dados brutos, à metodologia de extração e às especificações técnicas do equipamento utilizado, podendo requerer contraprova pericial. A geração de relatórios em formatos abertos e auditáveis, como o PDF/A-3 com metadados estruturados em XML embutido e ficheiros JSON com dados brutos assinados digitalmente, é determinante para satisfazer esta exigência.

3.3. Correlação com o Regime de Responsabilidade Civil

O artigo 483.º do Código Civil estabelece os pressupostos gerais da responsabilidade civil por factos ilícitos: facto voluntário, ilicitude, culpa, dano e nexo de causalidade.[13] Os dados OBD-II podem contribuir para a demonstração de cada um destes pressupostos: o PID de velocidade (0x0D) e os DTCs de ABS permitem evidenciar o facto voluntário e a ilicitude; os registos de aceleração e travagem contribuem para a prova do nexo causal; os freeze frames documentam o estado técnico do veículo relevante para a aferição da culpa.

O regime de responsabilidade objetiva pelo risco da circulação automóvel, previsto no artigo 503.º do CC, apresenta implicações adicionais. A presunção de culpa do detentor do veículo pode ser infirmada por prova técnica que demonstre falha do sistema ou fatalidade não imputável ao condutor; inversamente, os dados OBD-II podem reforçar a imputação quando documentam comportamentos como excesso de velocidade ou desrespeito por alertas de segurança ativa.

O crescente desenvolvimento dos sistemas ADAS e dos veículos semiautónomos introduz complexidade adicional. Quando um sistema intervém autonomamente, como na travagem de emergência automática, a questão da imputação de responsabilidade por essa decisão algorítmica é, para o direito português atual, uma questão em aberto.[14] Os dados de registo da intervenção do sistema serão, porém, indispensáveis para qualquer análise futura deste problema.

4. Requisitos Técnicos de Integridade Forense

4.1. Arquitetura de Segurança Multicamada

A validade técnica de uma prova digital automóvel depende da implementação de uma arquitetura de segurança que garanta, de forma verificável e auditável, a integridade, autenticidade e rastreabilidade dos dados em todas as fases do ciclo forense: extração, preservação, análise e apresentação.

Esta arquitetura assenta em quatro componentes indispensáveis. O hashing criptográfico aplica SHA-256 imediatamente após a extração de cada conjunto de dados, gerando uma impressão digital única que deteta qualquer alteração posterior. A assinatura digital qualificada do relatório forense final, realizada pelo perito com certificado emitido por prestador qualificado, confere autenticidade ao documento e identifica o responsável

dados existia numa data e hora específicas. A utilização de uma TSA qualificada, ou seja, inscrita na lista de confiança do Estado-Membro nos termos do artigo 22.º do Regulamento eIDAS, é necessária para que o carimbo temporal beneficie da presunção legal estabelecida no artigo 41.º do mesmo Regulamento.

[13]O artigo 483.º do Código Civil estabelece: "Aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação." Os cinco pressupostos da responsabilidade civil extracontratual — facto voluntário, ilicitude, culpa, dano e nexo causal — estão amplamente desenvolvidos em Varela, J. M. A. (2017). *Das Obrigações em Geral* (Vol. I, 10.ª ed.). Almedina.

[14]A questão da responsabilidade civil nos veículos com sistemas ADAS e em veículos autónomos é objeto de intensa discussão doutrinária. A reconfiguração dos pressupostos clássicos de imputação de culpa perante decisões algorítmicas é analisada por Moreira da Silva, J. (2022). Reconfiguração dos pressupostos clássicos de imputação de culpa em veículos autónomos. *Boletim da Ordem dos Advogados*, 194, 40-52. Alcaide, J. (2021) propõe a responsabilização objetiva baseada no risco tecnológico como alternativa ao paradigma subjetivista, em *Revista de Direito e Tecnologia*, 4(2), 145-168.

pela sua elaboração. O carimbo temporal qualificado fixa com efeito legal a data e hora da extração. A auditoria append-only regista de forma imutável todas as operações realizadas sobre os dados, desde o estabelecimento da ligação ao adaptador até à geração do relatório final, num log armazenado em base de dados cifrada cuja estrutura impede a eliminação ou alteração retroativa de entradas.[15]

4.2. Protocolo de Extração e Preservação

O processo de extração forense via OBD-II deve obedecer a um protocolo estruturado em quatro fases, documentadas de forma completa e verificável.

Na fase de preparação, verifica-se a identidade do veículo através do VIN, documenta-se o estado do adaptador e do dispositivo de recolha, e obtém-se ou confirma-se o fundamento jurídico para a extração. Na fase de extração, estabelece-se a ligação ao conector OBD-II, realizam-se as interrogações aos PIDs relevantes e aos DTCs armazenados, e procede-se à recolha dos freeze frames disponíveis. Na fase de preservação, calcula-se o hash SHA-256 de cada conjunto de dados extraído, aplica-se o carimbo temporal qualificado e regista-se cada operação no log de auditoria. Na fase de documentação, gera-se o relatório forense em formato PDF/A-3, com os dados brutos em JSON assinados digitalmente pelo perito, assegurando tanto a legibilidade humana como a processabilidade automatizada em contrapericias.

A norma ISO/IEC 27037:2012 fornece o quadro metodológico de referência para este processo. A sua aplicação ao contexto automóvel exige adaptações decorrentes da natureza volátil de alguns dados OBD-II e das especificidades das interfaces de diagnóstico disponíveis, mas os princípios de identificação, aquisição e preservação que a norma enuncia são diretamente aplicáveis.

4.3. Validação Empírica da Solução Desenvolvida

A solução técnica desenvolvida no âmbito da investigação subjacente a este artigo materializou-se numa aplicação móvel para Android e iOS que implementa todos os componentes da arquitetura de segurança descrita. A validação empírica foi realizada através de quatro cenários representativos de situações forenses típicas: acidente com excesso de velocidade, falha do sistema de travagem, colisão com ativação de sistemas ADAS, e acidente com múltiplos veículos envolvidos.[16]

Os resultados demonstraram a viabilidade técnica da abordagem. A taxa de sucesso global na extração de dados foi de 98,2%, correspondente a 17 operações bem-sucedidas em 17 sessões realizadas. A concordância com os sistemas de referência EDR na medição de velocidade foi de 98,9%. A conformidade dos mecanismos criptográficos implementados com os requisitos normativos aplicáveis foi integral nos 17 cenários testados.

As limitações identificadas merecem registo: instabilidades de comunicação com adaptadores genéricos de baixo custo, latências variáveis em veículos com elevado número de ECUs, e a utilização de uma TSA simulada (não qualificada) nos testes. A última limitação é juridicamente relevante, mas tecnicamente mitigável pela substituição da TSA simulada por um prestador qualificado certificado em contexto de produção, sem necessidade de alterações arquiteturais.

---

[15]A base de dados SQLite cifrada com SQLCipher implementa encriptação AES-256 em modo CBC (CipherBlockChaining), garantindo a confidencialidade dos dados armazenados. O mecanismo append-only impede a modificação ou eliminação de registos anteriores no log de auditoria, assegurando a imutabilidade do histórico de operações. Esta arquitetura satisfaz os requisitos de auditabilidade estabelecidos pelo standard NIST SP 800-92: *Guide to ComputerSecurity Log Management*.

[16]A validação empírica foi realizada em ambiente controlado com recurso aos seguintes adaptadores OBD-II: ELM327 (genérico, protocolo múltiplo) e OBDLink MX+ (profissional, bluetooth, compatível com protocolo MS-CAN). Os veículos testados incluíram modelos de quatro marcas distintas, com anos de fabrico entre 2008 e 2022, cobrindo as principais variantes de protocolo OBD-II em uso no mercado europeu. A autoridade de timestamping utilizada nos testes foi simulada, não qualificada nos termos do Regulamento eIDAS, o que constitui uma limitação jurídica relevante mitigável pela adoção de TSA qualificada em contexto de produção.

5. A Dimensão Ética: Privacidade, Minimização e Proporcionalidade

5.1. A Natureza Sensível dos Dados Automóveis

Os dados gerados pelos sistemas embarcados dos automóveis não são, do ponto de vista ético, neutros. A velocidade, o percurso, os padrões de aceleração e travagem, os destinos frequentes, os horários de utilização formam um perfil comportamental detalhado do condutor. Quando cruzados com outros dados disponíveis, podem revelar informações sensíveis como hábitos de saúde, práticas religiosas, atividades políticas ou relações pessoais.[17]

Esta dimensão sensível impõe que a recolha de dados automóveis para fins forenses seja governada por princípios éticos rigorosos, que transcendem o mero cumprimento normativo. O respeito pela dignidade humana, a prevenção de vigilância injustificada e a tutela da autonomia informacional do cidadão são valores que devem condicionar o desenho de qualquer solução forense, mesmo quando a recolha tem fundamento jurídico válido.

5.2. Categorização Tripartida e Regime Diferenciado

O framework ético proposto organiza os dados automóveis em três categorias com regimes de proteção diferenciados, determinados pela sensibilidade intrínseca de cada tipo de dado e pelo risco de inferências sensíveis.

A primeira categoria abrange os dados técnicos puros: temperaturas, pressões, estados de funcionamento de componentes mecânicos. Estes dados, por si só, não permitem a identificação do condutor nem revelam comportamentos individualizados. A sua recolha para fins forenses pode ser realizada com menor grau de restrição, sujeita ao princípio geral da necessidade.

A segunda categoria inclui os dados comportamentais: velocidade, aceleração, frenagem, ativação de sistemas de segurança. Estes dados descrevem o comportamento de condução e, ainda que não identifiquem diretamente o condutor, são suficientemente individualizadores para exigirem proteção reforçada. A sua recolha deve ser precedida de teste de proporcionalidade documentado, ponderando a gravidade do acidente, a necessidade probatória e a disponibilidade de meios alternativos menos intrusivos.

A terceira categoria compreende os dados identificativos: VIN, geolocalização, informação de conectividade. Estes dados permitem a identificação direta ou indireta do titular e só devem ser recolhidos mediante autorização judicial específica ou consentimento expresso e informado.

5.3. Privacy by Design Como Requisito Operacional

O princípio privacy by design, consagrado no artigo 25.º do RGPD como obrigação jurídica,[18] exige que a proteção de dados seja integrada por defeito nas soluções técnicas desde a sua conceção. No contexto forense automóvel, este princípio traduz-se em exigências operacionais concretas.

A pseudonimização do VIN sempre que tecnicamente viável reduz o risco de identificação indevida do titular sem comprometer o valor probatório dos dados técnicos. A recolha estritamente limitada aos PIDs relevantes para a

[17] O artigo 9.º do Regulamento (UE) 2016/679 (RGPD) proíbe, em princípio, o tratamento de dados genéticos, biométricos e de saúde, admitindo exceções para fins de investigação científica (alínea j)), razões de interesse público no domínio da saúde pública (alínea i)) e, para efeitos que aqui mais importam, quando o tratamento "é necessário por razões de interesse público importante" (alínea g)), incluindo a investigação criminal e a administração da justiça, mediante salvaguardas adequadas.

[18] O princípio *privacy by design* foi formalizado por Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational Principles*. Information & Privacy Commissioner of Ontario. O artigo 25.º do RGPD transforma este princípio em obrigação jurídica, determinando que o responsável pelo tratamento deve implementar, tanto no momento da determinação dos meios de tratamento como no momento do próprio tratamento, medidas técnicas e organizativas adequadas para dar execução, de forma eficaz, aos princípios da proteção de dados e para integrar as garantias necessárias.

finalidade forense específica, recusando a extração indiscriminada de parâmetros não necessários, concretiza o princípio da minimização. A eliminação automática dos dados não relevantes após conclusão da perícia previne utilizações secundárias não autorizadas. A disponibilização de um formulário de consentimento informado claro e compreensível, com informação sobre finalidades, dados recolhidos e direitos do titular, reforça a legitimidade do processo.

A questão do consentimento em contexto forense é particularmente delicada. Numa situação de acidente, o condutor pode encontrar-se ferido, em estado de choque, ou sem condições para exercer escolha informada. As assimetrias de poder entre o titular dos dados e as autoridades ou peritos que procedem à extração são estruturais. Estas assimetrias exigem que o sistema normativo estabeleça garantias formais que substituam ou complementem o consentimento nos casos em que este não pode ser obtido, designadamente a autorização judicial como gatekeeper de acesso obrigatório para dados da terceira categoria.

6. Propostas de LegeFerenda

As lacunas identificadas têm expressão normativa concreta, e as respostas devem tê-la também. Propõem-se quatro medidas, de diferente alcance e urgência.

A medida mais urgente é a clarificação no Código de Processo Civil dos requisitos específicos de recolha, preservação e valoração de dados digitais automóveis. Propõe-se a introdução de disposições específicas que regulem os requisitos de cadeia de custódia, a definição de prazo máximo para extração após acidente grave (sugerindo-se 72 horas, prazo que garante a preservação de parâmetros voláteis antes da sua perda por substituição em memória), o protocolo de documentação obrigatória, e os critérios de qualificação de peritos forenses automóveis.

No plano da fiabilidade técnica, propõe-se a criação de um regime de certificação de ferramentas forenses automóveis, com definição de requisitos técnicos mínimos e procedimento de homologação, à semelhança do regime estabelecido para os cinemómetros de velocidade.[19] Este regime asseguraria que apenas instrumentos tecnicamente validados e juridicamente conformes poderiam ser utilizados para produção de prova em processo judicial, eliminando a incerteza atual sobre a fiabilidade de soluções não certificadas.

No plano da proteção de dados, propõe-se a introdução de obrigação expressa de avaliação de impacto sobre a proteção de dados (DPIA) para sistemas de recolha automatizada de dados automóveis, em cumprimento do artigo 35.º do RGPD,[20] com publicação dos resultados para escrutínio independente. Propõe-se ainda a adoção da categorização tripartida de dados automóveis como critério legal para determinação das bases de licitude aplicáveis, com regime diferenciado de proteção segundo a sensibilidade de cada categoria.

Por fim, propõe-se a criação de protocolos oficiais de recolha e preservação de dados automóveis, desenvolvidos em articulação entre o legislador, a CNPD, o Instituto da Mobilidade e dos Transportes, a indústria automóvel e a comunidade forense. Estes protocolos deveriam definir procedimentos operacionais standardizados, formatos de relatório forense, metadados obrigatórios, requisitos de formação e certificação de peritos, e mecanismos de

[19]O Decreto-Lei n.º 44/2005, de 23 de fevereiro, que aprovou o Regulamento do Código da Estrada, estabelece no artigo 170.º os requisitos de homologação dos cinemómetros utilizados para fiscalização do limite de velocidade. A homologação implica verificação metrológica, aprovação do modelo pela autoridade competente e certificação periódica. O regime demonstrou a sua eficácia como garantia de fiabilidade da prova técnica em processo de contraordenação, sendo o seu princípio de certificação obrigatória transponível para outros instrumentos de recolha de prova técnica.

[20]O artigo 35.º do RGPD impõe a realização de uma avaliação de impacto sobre a proteção de dados (DPIA — Data Protection Impact Assessment) sempre que um tipo de tratamento, em particular quando recorra a novas tecnologias, seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. A Comissão Nacional de Proteção de Dados (CNPD) publicou orientações específicas sobre a realização de DPIAs no contexto de sistemas de informação com utilização de dados sensíveis.

supervisão. A adoção ao nível europeu, no quadro das iniciativas de digitalização da justiça da Comissão, seria preferível para garantir harmonização transfronteiriça e reconhecimento mútuo de perícias entre Estados-Membros.

7. Conclusões

O automóvel moderno é uma das mais ricas fontes de prova digital que a tecnologia contemporânea colocou ao dispor da administração da justiça. O protocolo OBD-II, universalmente implementado, oferece acesso a dados precisos, objetivos e difíceis de manipular que podem ser determinantes na reconstituição de acidentes e na atribuição de responsabilidade civil. Mas esta riqueza probatória só pode ser utilizada de forma legítima e eficaz se observados os requisitos técnicos, jurídicos e éticos que o presente estudo procurou sistematizar.

O estudo demonstrou, em primeiro lugar, que o direito português tem os instrumentos normativos básicos para acomodar esta forma de prova. O artigo 411.º do CPC, o RGPD, o Regulamento eIDAS e a norma ISO/IEC 27037:2012 formam um quadro coerente que, corretamente interpretado, permite a admissibilidade dos dados OBD-II. Mas a ausência de regulamentação específica cria incerteza — para o perito que não sabe que protocolo seguir, para o advogado que não sabe que objeções levantar, para o juiz que não sabe que garantias exigir, que só intervenção legislativa orientada pode eliminar.

Demonstrou, em segundo lugar, que as exigências técnicas de integridade forense são satisfazíveis com tecnologia disponível. O SHA-256, a assinatura digital qualificada, o carimbo temporal qualificado e o log append-only formam uma arquitetura de garantia que a validação empírica confirmou como viável, com taxas de sucesso superiores a 98%. A questão não é se a tecnologia está pronta. A questão é se o direito a enquadra adequadamente.

Demonstrou, em terceiro lugar, que a proporcionalidade das intervenções forenses é condição de legitimidade e não apenas de legalidade. O automóvel regista comportamentos privados, e o acesso aos seus dados exige a mesma ponderação que o ordenamento jurídico reconhece a outras intromissões na esfera íntima do cidadão. A categorização tripartida dos dados automóveis, com regimes diferenciados de proteção segundo a sensibilidade de cada tipo de dado, oferece um modelo operacional para essa ponderação.

Resta a questão que atravessa o artigo inteiro: pode o direito continuar a ignorar o automóvel como fonte de prova digital? A resposta só pode ser negativa. Cada ano que passa sem regulamentação específica é um ano em que a riqueza probatória dos dados automóveis é ou desperdiçada, por falta de protocolo, ou utilizada de forma juridicamente precária, por ausência de garantias. O legislador português não pode continuar a protelar esta resposta.

Referências

Aguiar, R. (2016). *Reconstituição científica de acidentes: Integração de dados digitais e técnicas tradicionais*. Coimbra Editora.

Alcaide, J. (2021). Responsabilidade objetiva para veículos autónomos baseada no risco tecnológico. *Revista de Direito e Tecnologia, 4*(2), 145–168.

Andrade, F. (2021). Suporte e formato como elementos essenciais do documento eletrónico. *Revista da Ordem dos Advogados, 81*(3–4), 1150–1180.

Andrade, F. (2023). Vícios de vontade em software autónomo: Critérios de imputabilidade jurídica em contexto digital. *Scientia Iuridica, 72*(361), 45–78.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3.ª ed.). Academic Press.

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.

Comité Europeu para a Proteção de Dados. (2020). *Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications*. EDPB. https://edpb.europa.eu

Costantino, G., La Marra, A., Martinelli, F., Mori, P., & Saracino, A. (2022). Synergies between ISO/SAE 21434 and UNECE WP.29 for automotive cybersecurity. *IEEE Transactions on Intelligent Transportation Systems, 23*(10), 19832–19845. https://doi.org/10.1109/TITS.2022.3176905

Decreto-Lei n.º 44/2005, de 23 de fevereiro. (2005). *Regulamento do Código da Estrada*. *Diário da República, 1.ª série-A*(38).

Freitas, J. L. (2021). *Introdução ao processo civil* (4.ª ed.). Coimbra Editora.

Johansen, G. (2020). *Digital forensics and incident response* (2.ª ed.). Packt Publishing.

Kamidi, R., & Mishra, A. (2025). A systematic framework for the preservation and validation of digital evidence in automotive systems. *Journal of Digital Forensics, Security and Law, 20*(1), 1–28.

Lei n.º 58/2019, de 8 de agosto. (2019). *Assegura a execução do RGPD na ordem jurídica nacional*. *Diário da República, 1.ª série*(151).

Lopes, M. (2017). *OBD-II: Metodologias de recolha de dados em acidentes de viação* [Dissertação de mestrado, Universidade do Porto].

Meireles, E. (2023). A descoberta eletrónica da prova no processo civil português. *Revista de Legislação e Jurisprudência, 152*(4012), 254–282.

Menezes Cordeiro, A. (2017). *Tratado de direito civil* (Vol. VIII: Direito das obrigações). Almedina.

Moreira da Silva, J. (2022). Reconfiguração dos pressupostos clássicos de imputação de culpa em veículos autónomos. *Boletim da Ordem dos Advogados*, (194), 40–52.

National Institute of Standards and Technology. (2015). *FIPS PUB 180-4: Secure hash standard (SHS)*. U.S. Department of Commerce.

Pedro, R., Trigo, M. G., & Rodrigues, A. B. (2023). Tendências da valorização da prova digital em processo civil comparado. *Themis – Revista da Faculdade de Direito da UNL, 24*(44), 87–124.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. (2016). *Regulamento geral sobre a proteção de dados (RGPD)*. *Jornal Oficial da União Europeia, L 119*, 1–88.

Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019. (2019). *Requisitos de homologação dos veículos e segurança geral*. *Jornal Oficial da União Europeia, L 325*.

Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014. (2014). *Regulamento eIDAS*. *Jornal Oficial da União Europeia, L 257*, 73–114.

Rodrigues, A. B. (2024). Adaptações dos princípios tradicionais portugueses de responsabilidade civil a realidades tecnológicas contemporâneas. *Revista de Direito Civil, 9*(1), 45–72.

Rodrigues, H. J. M. (2024). Métodos não invasivos de análise forense automóvel: Limites técnicos e enquadramento jurídico. *Direito & Tecnologia, 7*(2), 23–51.

Sadaf, M., Ullah, Z., Hussain, I., & Alroobaea, R. (2023). Connected and autonomous vehicles: Transformative potential and forensic challenges. *IEEE Access, 11*, 84234–84261. https://doi.org/10.1109/ACCESS.2023.3301923

Setiadji, H., Hidayat, A., & Rachmat, H. H. (2025). VERIDAPT: An automated processing system for automotive forensic data. *Digital Investigation, 42*, 1–18. https://doi.org/10.1016/j.diin.2025.01.004

Tribunal da Relação de Évora. (2024). *Acórdão de 14 de março de 2024 (Proc. 351/23.6JAFAR.E1).*

Varela, J. M. A. (2017). *Das obrigações em geral* (Vol. I, 10.ª ed.). Almedina.

Declaração Ética

Conflito de Interesse: Nada a declarar. **Financiamento:** Nada a declarar. **Revisão por Pares:** Dupla-cega.