PROTEÇÃO DE DADOS EM CARROS ELÉTRICOS CONECTADOS À REDE DE INTERNET

DATA PROTECTION IN ELECTRIC CARS CONNECTED TO THE INTERNET NETWORK

Caroline Marchesin da Silva
Faculdade de Tecnologia de Americana Ministro Ralph Biasi
caroline.silva123@fatec.sp.gov.br

Maria Fernanda Ferrante Darim
Faculdade de Tecnologia de Americana Ministro Ralph Biasi
maria.darim@fatec.sp.gov.br

Sâmela Regina Gonçalves da Silva
Faculdade de Tecnologia de Americana Ministro Ralph Biasi
samela.silva@fatec.sp.gov.br

João Emmanuel D Alkmin Neves
Faculdade de Tecnologia de Americana Ministro Ralph Biasi
joao.neves11@fatec.sp.gov.br

Resumo

Esse estudo científico abordou a intersecção entre a proteção de dados e o aumento dos carros elétricos numa era dominada pela tecnologia. Embora as empresas procurem inovar em tendências veiculares, a conectividade desses carros demostra desafios em relação a segurança dos dados utilizados e compartilhados, criando um aumento exponencial de riscos. Por meio de uma metodologia exploratória qualitativa, o artigo visa investigar os principais desafios dos carros elétricos, assim como, as regulamentações que abordam a segurança dessas informações, com objetivos de propor melhorias para garantir a disponibilidade, integridade e confidencialidade. Além disso, o estudo ressaltou a necessidade de maiores investimentos na área da segurança da informação por parte das empresas automobilísticas, as quais devem agir de forma ética e clara na coleta e uso dos dados dos titulares. Em somatória, conclui-se que é fundamental abordar sobre o valor dos dados e implementar medidas de conscientização, visando a construção de um futuro mais seguro e responsável para todos.

Palavras-chave: Carro elétrico. Segurança automotiva. Conectividade. Internet das Coisas.

Abstract

This scientific study addressed the intersection between data protection and the rise of electric cars in a technology-dominated era. While companies seek to innovate in vehicular trends, the connectivity of these cars presents challenges regarding the security of the data they utilize and share, leading to an exponential increase in risks. Through a qualitative exploratory methodology, the article aims to investigate the main challenges of electric cars, as well as the regulations addressing the security of this information, with the aim of proposing improvements to ensure availability, integrity, and confidentiality. Additionally, the study highlighted the need for greater investment in the area of information security by automotive companies, which should act ethically and transparently in the collection and use of user data. In summary, it is concluded that it is essential to address the value of data and implement awareness measures, aiming to build a safer and more responsible future for all.

Keywords: Electric car. Automotive safety. Connectivity. Internet of Things.

1. Introdução

A crescente preocupação em reduzir os impactos da poluição veicular no meio ambiente e seus efeitos, fizeram as indústrias automobilísticas passarem por grandes transformações. A sociedade tem explorado as tecnologias sustentáveis que surgiram no mercado para promover melhorias nos meios de transportes, sistemas de energias e indústrias (Brighente *et al*., 2023). Desse modo, os veículos elétricos e conectados foram adotados por diversos países e contam com defensores para sua expansão.

De acordo com um pronunciamento do diretor executivo da California Privacy Protection Agency, os veículos contemporâneos podem ser considerados como sistemas computacionais integrados sobre rodas (Ashkan, 2023), ou seja, se tornaram mais do que meios de transporte que oferecem novas tecnologias para praticidade e entretenimento das pessoas. No entanto, essas inovações também trouxeram questões críticas de segurança e privacidade, uma vez que, as empresas responsáveis por suas criações não cumprem os requisitos mínimos de proteção dos dados.

Nesse contexto, surge o seguinte problema central: até que ponto a segurança da informação será deixada como segundo plano?

Observado este ponto, o artigo tem por finalidade investigar e apresentar os desafios na proteção de dados nesses meios de transporte elétricos, entendendo sobre sua infraestrutura e pontos vulneráveis. Além disso, proporcionar métodos que garantam maior segurança dos dados dos usuários.

Para atingir esse objetivo geral, os seguintes objetivos específicos serão perseguidos:

- Identificar as tecnologias empregadas nos carros elétricos e suas vulnerabilidades.
- Expor os desafios de proteção de dados nas empresas automobilísticas.
- Sugerir medidas adicionais de segurança baseadas nas melhores práticas para mitigar os riscos associados à proteção de dados.

A justificativa deste estudo reside na crescente importância de compreender a aplicação de medidas de proteção de dados dos utilizadores dos carros elétricos, já que, em um mundo cada vez mais tecnológico, é imprescindível a conscientização sobre a segurança da informação. Ademais, a pesquisa contribuirá no debate em torno dos desafios técnicos enfrentados pelas empresas automobilísticas na busca por maior transparência e confiabilidade dos dados em relação aos seus clientes.

2. Referencial Teórico

Com o aumento da popularidade dos carros elétricos, observa-se uma interligação mais aprofundada de dispositivos conectados, visando sempre melhorar a experiência do usuário. Logo, com a crescente venda de carro elétricos e suas conexões com a Internet das Coisas (IoT), torna-se essencial realizar uma análise detalhada dos desafios relacionados à segurança dos dados compartilhados e às políticas de privacidade. Nesse contexto, o embasamento teórico deste artigo busca investigar e compreender os aspectos cruciais que envolve a interseção entre IoT, veículos elétricos e segurança cibernética, contribuindo assim para uma compreensão mais aprofundada do tema abordado.

2.1 Relação de IoT e Veículos Conectados

A conectividade permeia quase todos os aspectos da sociedade contemporânea, incluindo o setor automotivo (Moraes *et al.*, 2022). No Brasil, conforme dados da Associação Brasileira de Veículos Elétricos (ABVE, 2023), as vendas de automóveis elétricos registraram um aumento de 41% em 2022 em comparação ao ano anterior.

Os veículos elétricos conectados incentivam seus proprietários a integrarem seus smartphones ao sistema do carro, proporcionando uma experiência de usuário significativamente aprimorada. Cada um de seus componentes está interligado a um computador central, responsável por gerenciar a comunicação entre as diversas partes do veículo por meio da IoT.

De acordo com Moura e D'Alkmin Neves (2021), IoT é definida como a capacidade de estabelecer conexões físicas entre objetos e a Internet, facilitando a gestão de operações. Para que um ambiente IoT funcione de forma eficaz, é fundamental a presença de sensores para a coleta de dados, identificadores que reconheçam a origem dessas informações, software que transforme os dados em *insights* relevantes e, finalmente, uma conectividade robusta com a internet, que desempenha um papel essencial na comunicação e na notificação entre os dispositivos envolvidos (Rayes; Salam, 2016).

Assim, os dispositivos IoT inteligentes coletam uma grande quantidade de dados para garantir o cumprimento dos objetivos de proporcionar maior comodidade e praticidade no cotidiano das pessoas, por meio de sensores e dispositivos inteligentes, conectividade à Internet e comunicação com dispositivos móveis (Moura; D'Alkmin Neves, 2021).

A indústria automotiva utiliza também desse conceito na fabricação dos automóveis através de sensores e sistemas, que analisam tanto o tráfego nas estradas e informações do meio, evitando acidentes, quanto diminuindo processos complexos de fabricação, pois registram dados do funcionamento de uma máquina ou processo, monitorando continuamente e identificando possíveis falhas antes do lançamento dos veículos.

Dessa maneira, uma publicação do Grupo Internacional de empresas Knauf (2023), destacou o papel da empresa Capgemini na utilização da tecnologia para otimizar operações em diversos setores, incluindo aeroespacial e defesa, automotivo, mercados bancários, energia, entre outros. Segundo a empresa, no ano de 2023, houve um aumento de 4,4% na produtividade das fábricas que implementaram a IoT nos seus processos.

2.2 Desafios Específicos em Veículos Elétricos Conectados

Os carros elétricos apresentam diversas vulnerabilidades de segurança. Um dos principais riscos destaca-se o roubo ou violação de dados. Com a conectividade, os automóveis coletam e armazenam uma quantidade significativa de dados, que englobam localização, rotas frequentes, imagens de câmeras e até mesmo dados de dispositivos móveis. Essa ampla coleta foi evidenciada durante um processo judicial na Califórnia em 2023, conforme reportado pelo jornalista Brown (2023), envolvendo a empresa Tesla. Nesse caso, os funcionários da montadora acessaram ilegalmente imagens e vídeos armazenados no veículo do proprietário Henry Yeh infringindo sua privacidade.

Além disso, o sistema desses veículos também apresenta vulnerabilidades na infraestrutura dos equipamentos de abastecimento de veículos elétricos (EVSE), tanto em ambientes pessoais quanto públicos, que ficam expostos sem muitas medidas de segurança. Conforme estudos conduzidos por Nasr *et al* (2021), do Centro de Pesquisa de Segurança da Escola de Engenharia e Ciência da Computação Gina Cody, em 2021 foi constatado que nem sempre o *firmware* e os aplicativos usados nesses dispositivos atendem aos padrões de segurança cibernética, o que os torna suscetíveis à infecção por *malwares*.

Sendo assim, a maior parte dos sistemas de carregamento têm vulnerabilidades que vão além do controle remoto das funções. Essas falhas permitem não apenas desbloquear portas, modificar os modos de direção e navegação (coordenados por um chip central), mas também invadir outros dispositivos na mesma rede, inserindo *backdoors* que comprometem qualquer dispositivo conectado aos carregadores incluindo as estações de carregamento, os operadores dos pontos de carga e até mesmo os operadores do sistema de distribuição de energia (Gugelmin, 2021).

A adoção da tecnologia *Keyless* nos veículos também acarreta vulnerabilidades. Essa tecnologia utiliza aplicativos e chips de Identificação de Rádio Frequência (Fortra, 2023) e, quando integrada ao sistema, é responsável por destravar portas, simplesmente aproximando-se do veículo e tocando-o, uma vez que, operam por sinais que sincronizam a chave com o veículo (Jacobson, 2023). Dessa forma, hackers conseguem capturar e clonar esses sinais, facilitando o desbloqueio.

Em somatória, o grande diferencial dos automóveis equipados com sistemas de *infotainment* — termo que se refere ao conjunto de tecnologias que combinam entretenimento e informações em um único sistema integrado ao veículo (Jacobson, 2023) — é proporcionar uma experiência de direção mais sofisticada e inteligente em um painel único, com suporte de navegação GPS, streaming de música, integração de smartphone, informações do próprio carro e entre outros. Porém, pesquisas já foram desenvolvidas e demonstraram como esses sistemas ficam suscetíveis a ataques.

De acordo com um estudo de caso de um grupo de doutorandos do programa de pós-graduação da Universidade Técnica de Berlim desenvolvido em 2023 (Werling; Kühnapfel; Jacob, 2023), foi demostrado que é possível violar o sistema de *Infotainment* da Tesla, desenvolvendo o conhecido "*jailbreak*", um processo que envolve a exploração de falhas de dispositivos eletrônicos bloqueados para instalação de software não fornecido pelo fabricante para uso no dispositivo (Kaspersky, 2023).

Dessa forma, o grupo usou técnicas baseadas em pesquisas anteriores das vulnerabilidades da Unidade de Processamento Acelerado (APU) baseada na CPU AMD Zen 1. Através de um ataque de injeção de falha de tensão contra o AMD Secure Processor, alcançaram o controle absoluto do sistema, incluindo acesso a informações sensíveis e segredos das partes supostamente seguras, como a chave de autenticação que liga o carro à rede da Tesla. Isso evidencia a necessidade de que qualquer dispositivo que utilize a Internet das Coisas (IoT) implemente medidas rigorosas de segurança cibernética. Segundo Souza *et al.* (2024), a complexidade tecnológica desses sistemas os torna vulneráveis a diversas ameaças, tornando essencial a adoção de protocolos de segurança, como criptografia e autenticação, para proteger dados e garantir a privacidade dos usuários.

2.3 Políticas de Privacidade e Consentimento do Usuário

Atualmente, no Brasil, legislações como a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) conferem aos usuários escolher se autorizam ou não o compartilhamento de seus dados por parte de empresas ou concessionárias de veículos. Ao tomar essa decisão, é necessário que sejam informados como esses dados serão utilizados. Além disso, o Marco Civil da Internet (Lei n° 12 965), estabelece quais os direitos e deveres dos usuários brasileiros quando estão conectados à rede de internet, mas ainda assim, isso não impede que pessoas mal-intencionadas roubem dados e invadam esses dispositivos.

Diante desse cenário, uma medida para proteger os proprietários desses veículos elétricos é assegurar que os automóveis sejam entregues de fábrica com dispositivos de segurança integrados. Ademais, as montadoras podem elevar a confiabilidade dos produtos ao aplicar as normativas de segurança como a ISO/SAE 21434:2021 *Road vehicles — Cybersecurity engineering* (Veículos rodoviários - Engenharia de segurança cibernética), projetada para criar uma estrutura de segurança cibernética em veículos rodoviários. Essa norma é abrangente, abordando quatro principais aspectos: a avaliação e gestão de riscos dos veículos, o controle de segurança contra-ataques cibernéticos, a comunicação e troca de informações com outras organizações a fim de informar sobre riscos e incidentes de cibersegurança, e por fim o desenvolvimento de estratégias para mitigar incidentes cibernéticos.

Outra norma na temática das montadoras é a ISO 15118-20:2022 *Road vehicles — Vehicle to grid communication interface* (Veículos rodoviários - Interface de comunicação veículo-rede), aplicada em veículos rodoviários elétricos. Ela faz parte de um dos grupos de norma da Comissão Eletrotécnica Internacional (IEC). A *International Organization for*

Standardization (ISO) tem como foco a Interface de comunicação veículo-rede para carregamento e descarregamento bidirecional dos veículos elétricos, criando assim uma comunicação segura durante o carregamento, além de ter um recurso de Plug & Carga seguros, permitindo que um veículo elétrico se identifique automaticamente e se autorizando em uma estação de carregamento em nome do motorista.

2.4 Segurança de Dados e Privacidade

Atualmente, a segurança da informação e a proteção da privacidade são temas amplamente discutidos entre os profissionais da área. Esses conceitos englobam um conjunto de métodos e técnicas destinadas a garantir a integridade, a disponibilidade e a confidencialidade das informações. Portanto, é crucial entender a distinção entre esses dois termos (Barbosa; Ferreira; Neves, 2023).

A segurança de dados foca na proteção contra os ataques e as invasões, buscando evitar o roubo de informações pessoais e sensíveis. Essa situação não só gera complicações para os indivíduos afetados, mas também pode acarretar danos à reputação da empresa e resultar em penalidades legais (Tonezer *et al.*, 2024). Por outro lado, a privacidade concentra-se na aderência às leis e regulamentações, seguindo as diretrizes e políticas estabelecidas pela empresa para prevenção de perda de dados (Mcafee, 2020).

Para auxiliar nesse entendimento, a Tabela 1 apresenta uma classificação dos dados por sensibilidade, baseada na Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018. Essa classificação proporciona uma visão organizada das diferentes categorias de dados, desde informações públicas até dados confidenciais, sendo fundamental para orientar a aplicação prática de medidas de segurança e garantir uma abordagem abrangente de proteção.

Tabela 1 - Classificação dos dados por sensibilidade

Público	Informações disponíveis publicamente, sem restrições de acesso.
Interno	Dados de uso interno, compartilhados entre departamentos autorizados.
Confidencial	Informações sensíveis, restritas a pessoal autorizado.
Restrita ou Secreta	Dados altamente confidenciais, com acesso restrito a um grupo seleto de pessoas.

Fonte: Autoria própria com base na LGPD (2018)

Apesar da implementação da LGPD, a ausência de fiscalização contribui para muitas empresas não encararem seriamente essas questões, resultando em um tratamento de dados inadequado. Além disso, à irresponsabilidade demonstrada por algumas instituições e titulares, os quais não tratam as informações de maneira adequada, desconsiderando as leis e regulamentações da Autoridade Nacional de Proteção de Dados (ANPD, 2018), é uma preocupação adicional.

Diante desses desafios, torna-se indiscutível superar os diversos obstáculos para preservar a privacidade e a segurança dos dados. Recomenda-se a adoção de práticas como a utilização de senhas fortes, a implementação de autenticação, backups dos dados mais críticos e a implementação rigorosa às políticas e diretrizes estabelecidas nas empresas (LGPD News, 2023).

3. Metodologia

Esse trabalho visa a metodologia exploratória com uma abordagem qualitativa, tendo como base pesquisas que compreendem conceitos que envolvem a IoT e sua integração com os carros elétricos. Ademais, foram exploradas as vulnerabilidades recorrentes do processo de coleta, armazenamento, compartilhamento e uso de dados por parte dos fabricantes, além das normativas e regulamentações existentes sobre a temática. Para isso, foram consultadas diversas fontes como artigos científicos, sites e monografias abrangendo o período de 2015 a 2024.

Após a análise de um total de 49 trabalhos, 33 foram selecionados para servir como embasamento do artigo. Essa seleção foi levando em consideração a atualidade das informações e a qualidade metodológica para concretização da tese apresentada no trabalho.

4. Resultados e Discussões

Com base nos estudos feitos, foi evidenciado que a problemática de proteção de dados nos carros elétricos necessita de uma abordagem multifacetada, abrangendo desde os compradores desses veículos até as empresas do setor.

Em entrevista no ano de 2022, o presidente-executivo (CEO) da Upstream Security, Yoav Levy, diz acreditar que existem grandes investimentos na capacidade de abastecimento dos veículos elétricos, mas os governos devem garantir que protegerão suas redes, seus veículos e a sua infraestrutura (Gottardello, 2023).

Sendo assim, a busca constante dos países de adotar mais tecnologia e eletrificação não acompanha a preocupação com a segurança e proteção digital. Para solucionar essas

questões, requer-se uma colaboração entre os fabricantes de automóveis e as autoridades governamentais, a fim de estabelecer políticas de segurança e proteção de dados que priorizem a integridade e privacidade dos indivíduos.

Uma pesquisa divulgada pelo site da Mozilla Foundation em 2023, investigou 25 fabricantes de veículos. Os resultados revelaram deficiências preocupantes e inadequadas. Segundo o relatório, os fabricantes estão coletando e analisando dados de usuários de forma descontrolada, sendo a central multimídia a principal fonte da coleta (Caltrider; Rykov; Rykov, 2023).

Os resultados da pesquisa conduzida pela Mozilla Foundation sobre privacidade informaram que 84% das montadoras compartilham internamente os dados coletados, enquanto 76% vendem e 56% as compartilham com o governo ou com autoridades policiais em reposta a solicitações (Caltrider; Rykov; Rykov, 2023).

Os critérios considerados para a análise incluem aspectos fundamentais como o uso e controle de dados, o registro de informações, a segurança dos usuários e a aplicação da Inteligência Artificial (IA). A utilização ética e transparente dos dados é crucial para respeitar a privacidade, enquanto um registro cuidadoso permite rastrear e auditar informações, garantindo sua integridade. A segurança dos usuários se torna ainda mais relevante neste contexto, onde a IA pode ser aplicada para detectar padrões anômalos e prevenir ameaças cibernéticas (Neves, 2024). Além de oferecer proteção, a IA pode personalizar experiências, tornando o uso de dados mais responsivo e adaptado às necessidades dos usuários. No entanto, a implementação de soluções de IA deve sempre ser acompanhada de diretrizes éticas rigorosas para mitigar riscos e proteger direitos, evidenciando a importância de uma abordagem integrada entre segurança de dados e tecnologias emergentes (Neves *et al.*, 2023).

Entre os fabricantes analisados, apenas as empresas Renault e Dacia, fizeram um correto controle de dados, ambas com sede na Europa, em conformidade com o Regulamento Geral sobre a Proteção de Dados (GDPR). No entanto, outras grandes empresas como Ford, Toyota, Volkswagen, BMW e Tesla não cumpriram os padrões mínimos de privacidade (Caltrider; Rykov; Rykov, 2023).

Essas conclusões foram fundamentadas em políticas de privacidade, termos de uso, contatos diretos por e-mail ou tentativas de contato e dados fornecidos pelas montadoras. Portanto, o comprometimento da indústria automotiva é insuficiente na segurança cibernética, uma vez que, falta a especialização e maior conhecimento sobre proteção de dados.

Em suma, as maiores ameaças à proteção de dados estão relacionadas à rede interna dos veículos e aos sistemas de carregamento, uma vez que criminosos podem combinar diferentes ataques e prejudicar todo o sistema, com base na análise de alguns dos maiores fabricantes da indústria de estações de carregamento de veículos eléctricos. (Nasr *et al*., 2021).

É crucial equipar todos os componentes dos carros com capacidades de detecção de anomalias, permitindo o rastreamento e análise de dados para identificar padrões não usuais e suspeitos. Além disso, técnicas de detecção de intrusões são essenciais para prevenir e identificar ataques antes que ocorram. Por exemplo, a injeção de códigos maliciosos (malware) pode ocorrer no processo de atualização do software, seja remotamente ou via cabo de carregamento, o que pode exigir o acesso à rede do veículo. Nesse processo, para impedir que os cibercriminosos acessem a rede interna e obtenham algum tipo de controle ou acesso não autorizado, as técnicas de intrusões são cruciais para identificar tais ataques.

Em complemento, a implementação do duplo fator de autenticação (MFA) é fundamental para garantir a integridade dos dados e verificar se a fonte externa é compatível com o esperado. Essa medida ajuda a evitar o *Spoofing*, onde um invasor pode interceptar a comunicação e enviar pacotes maliciosos e falsificados, como informações sobre o estado da bateria ou dados de carregamento, através de uma camada adicional de segurança na rede física (Brighente *et al*., 2023).

Outra forma de proteger a transmissão dos dados, é por meio da criptografia, que impede qualquer modificação de conteúdo e inserção de dispositivos entre os veículos e equipamentos de carregamento, prevenindo ataques do tipo *Man-in-the-Middle* (MitM) (Brighente *et al*., 2023).

Essas medidas de segurança como detecção de intrusão e anomalias, autenticação e criptografia são essenciais para mitigar os riscos associados à interconexão dos sistemas.

Visando a necessidade do mercado em adotar práticas que transformem o setor da segurança veicular, foi desenvolvido o EVKit, uma colaboração entre a Trend Micro e o Consórcio MIH, em conjunto com o Grupo Foxconn Technology. Anunciada em outubro de 2021, o EVKit é uma plataforma de desenvolvimento de última geração, que utiliza protocolo de comunicação aberto e estabelece uma base sólida de segurança para veículos elétricos desde a fase inicial de desenvolvimento com base na abordagem *"Secure by Design"* (Foxconn, 2021).

O foco principal do projeto está na garantia de segurança e proteção cibernética, seguindo as diretrizes da norma ISO 21434-2021, que aborda a segurança cibernética em veículos automotivos e as recomendações técnicas R155 e R156 da Comissão Econômica das

Nações Unidas para a Europa (UNECE), que detalham os requisitos para lidar com as ameaças cibernéticas e homologar sistemas de segurança (MIH Consortium, 2022).

Sendo assim, essa iniciativa representa um avanço significativo no setor automotivo, considerando as crescentes preocupações com a segurança cibernética em veículos conectados. De acordo com William Wei, CTO do MIH, em 2021, destacou a importância da parceria com a Trend Micro na definição de um *framework* de segurança comum para veículos elétricos. Isso inclui suporte à detecção de intrusões na rede do veículo, proteção do sistema e defesa contra ameaças da internet. A colaboração entre as duas empresas visa não apenas fornecer segurança, mas também criar um ecossistema aberto para desenvolvedores globais participarem facilmente.

Além disso, o EVKit inclui uma série de recursos de segurança, como proteção da transmissão de dados do veículo para a nuvem, acesso seguro a dados e autenticação de identidade. Ele também oferece funcionalidades avançadas, como gerenciamento de *big data* na nuvem, permitindo o desenvolvimento de aplicativos de IA e *big data* para monitoramento remoto, manutenção preditiva e operações de segurança veicular (Trend Micro, 2021).

No geral, o EVKit vai além do software, incluindo também o aspecto do hardware, desde o projeto até a implantação (Fisita, 2021). Dessa forma, com o auxílio de uma legislação adequada, todas as organizações do setor poderiam implantar a plataforma, para analisar todo o ciclo de vida do produto e não só na venda do automóvel. Com isso, torna-se imprescindível o apoio e terceirização de empresas e iniciativas especializadas em cibersegurança, colaborando com o setor automotivo.

Ademais, ao abordar a necessidade de mudanças nas empresas, é essencial considerar quem as compõe. Ou seja, para aplicar práticas de segurança assertivas torna-se indispensável que as pessoas compreendam a razão por trás dessas melhorias. Neste contexto, a sensibilização deve ser tanto das organizações quanto da sociedade em geral sobre as implicações da interseção entre a expansão dos carros elétricos e a proteção de dados.

O estudo da Concordia University (Lejtenyi, 2022) destaca que, com o avanço da tecnologia dos veículos elétricos, os desafios de segurança dos dados aumentam significativamente. Nesse contexto, a conscientização é crucial para mitigar esses riscos, abrangendo não apenas o ambiente corporativo. É fundamental educar a sociedade sobre a importância dos dados pessoais e as implicações da conectividade dos carros elétricos. Assim, os proprietários devem estar cientes do destino dos dados e das informações utilizadas, promovendo um uso seguro dos veículos elétricos conectados.

5. Considerações Finais

Em síntese do avanço tecnológico e da popularização dos veículos elétricos, este artigo abordou sobre a interseção crítica entre a proteção de dados e o aumento desses automóveis inovadores. Explorando sobre esse assunto, foram identificados vulnerabilidades e desafios relacionados à segurança de privacidade de dados, o que gera um aumento de riscos.

A pesquisa teve por fundamento a metodologia exploratória qualitativa, focada na identificação das tecnologias utilizadas nos carros elétricos e na análise das vulnerabilidades associadas a essas inovações. Além disso, foram abordados os desafios de proteção de dados enfrentados pelas empresas automobilísticas, com objetivo de sugerir medidas adicionais de segurança que visem mitigar os riscos relacionados à proteção de dados.

Sendo assim, os resultados indicam que a segurança dos carros elétricos, especialmente no contexto da IoT e veículos conectados, enfrenta vários desafios específicos. Por exemplo, foram identificadas vulnerabilidades na infraestrutura, assim como falhas nos sistemas de entretenimento. Essas fragilidades podem permitir invasões e controle do veículo por pessoas mal-intencionadas, o que facilita o roubo de dados e informações pessoais.

Embora existam legislações que permitem aos titulares decidirem sobre o uso de seus dados, como a LGPD, e termos de consentimento oferecidos por montadoras e concessionárias no momento da aquisição de um veículo, ainda há falhas na conformidade em relação ao tratamento dos dados após a coleta. Essas falhas se refletem no compartilhamento inadequado de informações e na exposição a possíveis violações. Portanto, é fundamental uma abordagem ética e colaborativa entre os fabricantes de automóveis e as autoridades governamentais para estabelecer políticas de segurança e assegurar o cumprimento das normas de proteção de dados.

Além das regulamentações, é essencial adotar medidas específicas de segurança cibernética no tratamento de dados, como detecção de intrusões, criptografia e autenticação em duas etapas, para mitigar os riscos da interconexão dos sistemas. O EVKit, desenvolvido pela Trend Micro em colaboração com o Consórcio MIH, exemplifica uma abordagem proativa de segurança, desde o desenvolvimento até a implementação dos veículos elétricos. A pesquisa enfatiza a importância da conscientização pública sobre a proteção de dados pessoais e a necessidade de educação contínua sobre o uso seguro desses veículos. A transparência das empresas é fundamental para assegurar a confiança dos consumidores, promovendo uma harmonia entre a proteção de dados e a evolução tecnológica. Assim, o futuro dos carros elétricos deve ser não apenas inovador, mas também seguro.

Referências

ABVE. **Eletrificados fecham 2022 com novo recorde**. 3 jan. 2023. Disponível em: http://www.abve.org.br/eletrificados-fecham-2022-com-novo-recorde-de-vendas/. Acesso em: 23 out. 2023.

ANPD. **Autoridade Nacional de Proteção de Dados**. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional. Acesso em: 4 nov. 2023.

ASHKAN.S. **CPPA to Review Privacy Practices of Connected Vehicles and Related Technologies.** 31 jul. 2023. Disponível em: https://cppa.ca.gov/announcements/2023/20230731.html. Acesso em: 20 de março de 2024.

BARBOSA, P.; FERREIRA, M.; NEVES, J. E. D. **Abordagem de Segurança no Desenvolvimento de Aplicações Web.** III FatecSeg. 2023. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/107. Acesso em 3 de nov. 2024.

BRASIL. Lei 12.965, de 23 de abril de 2014**.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 nov. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018**.** Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial [da] República Federativa do Brasi**l. Redação dada pela Lei nº 13.853, de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 nov. 2023.

BRIGHENTE, A. *et al*. **Electric Vehicles Security and Privacy: Challenges, Solutions, and Future Needs**. ArXivLabs. Nova York, v.1, n. 2301.04587, p. 1-18, 11 jan. 2023. Disponível em: https://arxiv.org/abs/2301.04587/ Acesso em: 13 nov. 2023.

BROWN. C. **Tesla Slapped With Suit Over Employee Sharing of In-Car Videos.** Bloomberg Law. 11 abr. 2023. Disponível em: https://news.bloomberglaw.com/privacy-and-data-security/tesla-slapped-with-suit-over-employee-sharing-of-in-car-videos. Acesso em: 2 nov. 2023.

CALTRIDER, J; RYKOV. M; MACDONALD. Z. **It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy.** Mozzila Foundation**,** 6 set. 2023. Disponível em: https://foundation.mozilla.org/pt-BR/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/ Acesso em: 05 nov. 2023.

FISITA. **Foxconn pitches MIH open platform as "the Android of electric vehicles"**. Fisita. 19 mai. 2021. Disponível em: https://www.fisita.com/post/foxconn-pitches-mih-open-platform-as-the-android-of-electric-vehicles. Acesso em: 25 mai. 2024.

FORTRA. **ELECTRIC Vehicle Cyber Security: Are EVs Safe from Hackers?.** Fortra. 17

mai. 2023. Disponível em: https://www.terranovasecurity.com/blog/electric-vehicle-cyber-security. Acesso em: 23 out. 2023.

FOXCONN. **Open Letter from MIH CEO and EVKit**. Foxconn. 21 jan. 2021. Disponível em: https://www.foxconn.com/s3/mih/newsletter/20210131_Open_Letter_from_MIH_CEO_and_EVKit.pdf.Acesso em: 25 mai. 2024.

GOTTARDELLO, Homero. **Nova moda dos hackers é atacar estações de recarga de carros elétricos.** Mobiauto, 6 mai. 2022. Disponível em: https://www.mobiauto.com.br/revista/nova-moda-dos-hackers-e-atacar-estacoes-de-recarga-de-carros-eletricos/1840/. Acesso em: 25 out. 2023.

GUGELMIN. F. **Carregadores de carros elétricos estão vulneráveis e podem levar a apagão geral.** Canal Tech. 24 ago. 2021. Disponível em: https://canaltech.com.br/seguranca/carregadores-de-carros-eletricos-estao-vulneraveis-e-podem-levar-a-apagao-geral-193582/. Acesso em: 30 out. 2023.

ISO 15118-20:2022 - International Organization for Standardization. Disponível em: https://www.iso.org/obp/ui/en/#iso:std:iso:15118:-20:ed-1:v1:en. Acesso em: 25 out. 2023.

ISO 21434-2021: Definição, Conformidade, Ferramentas e Certificações. **Visure Solutions, Inc.** Disponível em: https://visuresolutions.com/pt/blog/automotive/iso-21434/#:~:text=A%20ISO%2021434%20descreve%20um,de%20privacidade%20e%20muito%20mais. Acesso em: 15 nov. 2023.

JACOBSON, D. **To steal today's computerized cars, thieves go high-tech.** The Conversation, 14 ago. 2023. Disponível em: https://theconversation.com/to-steal-todays-computerized-cars-thieves-go-high-tech-210358/. Acesso em: 10 nov. 2023.

KASPERSKY. **O QUE é jailbreak – definição e explicação**. Kaspersky**.** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-jailbreaking. Acesso em: 2 nov. 2023.

KNAUF. **QUAIS são as aplicações da Internet das coisas na indústria automotiva?.**19 mai. 2023. Disponível em: https://knaufautomotive.com/pt-br/quais-sao-as-aplicacoes-da-internet-das-coisas-na-industria-automotiva/. Acesso em: 8 nov. 2023.

LEJTENYI, P. **Electric vehicle charging stations are a new focus for Concordia cybersecurity researchers.** Concordia University, 15 fev. 2022. Disponível em: https://www.concordia.ca/news/stories/2022/02/15/electric-vehicle-charging-stations-are-a-new-focus-for-concordia-cybersecurity-researchers.html. Acesso em: 10 fev. 2024.

LGPD News. **Melhores práticas para proteger os dados.** LGPD News, 18 set. 2023. Disponível em: https://lgpdnews.com/2023/09/melhores-praticas-proteger-dados/. Acesso em: 20 jan. 2024

MCAFEE. **O que é privacidade de dados e como posso protegê-la? | McAfee Blog**. 01 abr. 2020. Disponível em: https://www.mcafee.com/blogs/pt-br/privacy-identity-protection/o-que-

e-privacidade-de-dados-e-como-posso-protege-la//. Acesso em: 18 nov. 2023.

MIH CONSORTIUM. **MIH's Open EV Platform for the Software-Defined Vehicle Future**. MIH Consortium. 22 jan. 2022. Disponível em: https://www.mih-ev.org/en/news-info/?id=765. Acesso em: 10 dez. 2023.

MORAES, J. M. de; QUIRINO, C.; ALMEIDA, R. M. de; NEVES, J. E. D**. Internet das Coisas (IoT)**: Casa inteligente, definições e aplicações. Revista Brasileira em Tecnologia da Informação, [S. l.], v. 4, n. 2, p. 31 - 37, 2022. Disponível em: https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/52. Acesso em: 3 de nov. 2024.

MOURA, T. M.; D'ALKMIN NEVES, J. E. **Análise de Segurança em Dispositivos Internet das Coisas**. Revista Interface Tecnológica, [S. l.], v. 18, n. 2, p. 15–27, 2021. Disponível em: https://doi.org/10.31510/infa.v18i2.1174. Acesso em: 3 de nov. 2024.

NASR, T. *et al*. **Power jacking your station: In-depth security analysis of electric vehicle charging station management systems**. Computers & Security, v. 112, p. 102511, jan. 2021. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167404821003357.Acesso em: 01 nov.2023.

NEVES, J. E. D. A. **Mineração de dados aplicada a simulação de cenários complexos em sistemas multiagentes**. Orientadores: Paulo Sérgio Martins Pedro (in memoriam), Marli de Freitas Gomes Hernandez. 2024. 237 p. Tese (Doutorado em Tecnologia) - Faculdade de Tecnologia, Universidade Estadual de Campinas (UNICAMP), Limeira, 2024. Disponível em: https://www.repositorio.unicamp.br/acervo/detalhe/1395946. Acesso em: 3 de nov. 2024.

NEVES, J. E. D. A.; PEDRO, P. S. M.; HERNANDEZ, M. F. G.; FABRI JUNIOR, L. A. **Simulation of the Implementation of Domestic Solar Systems Using Multi-agent Systems from Web Scraping. Smart Innovation, Systems and Technologies**. 1ed.: Springer International Publishing, 2023, v. 1, p. 88-96. Disponível em: https://doi.org/10.1007/978-3-031-04435-9_8. Acesso em: 3 de nov. 2024.

RAYES, A.; SALAM, S. **Internet of things-from hype to reality: The road to digitization**. Internet of Things From Hype to Reality: The Road to Digitization, Springer International Publishing, Cham, v. 32, n. 8, p. 1–328, 2016. ISSN 0970034X.

SOUZA, A. L. O.; BASTOS, C. V.; SANTOS, P. M. S.; SOARES, N. M.; NEVES, J. E. D. **Cibersegurança na Agricultura de Precisão**: Exploração à Aplicação de Medidas Preventivas. Advances in Global Innovation & Technology, v. 2, p. 61-73, 2024. Disponível em: https://doi.org/10.29327/2384439.2.2-5. Acesso em 3 de nov. 2024.

TONEZER, L. N.; SILVA, A. C. M.; ALMEIDA, A. H.; NEVES, J. E. D. **Simulações Multiagentes e Phishing: Explorando a Segurança em Ambientes de Nuvem**. Revista Tecnológica da Fatec de Americana, v. 11, p. 1-17, 2024. Disponível em: https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/393. Acesso em 3 nov. 2024.

TREND MICRO. **Trend Micro and MIH Consortium Lay the Safety Foundation for**

Electric Vehicles. Trend Micro**.** 20 out. 2021. Disponível em: https://newsroom.trendmicro.com/2021-10-22-Trend-Micro-and-MIH-Consortium-Lay-the-Safety-Foundation-for-Electric-Vehicles. Acesso em: 26 nov. 2023.

WERLING, C.; KÜHNAPFEL, N.; JACOB. H. **Jailbreaking an Electric Vehicle in 2023 or What It Means to Hotwire Tesla's x86-Based Seat Heater.** Black Hat USA, Estados Unidos, n.25, ago. 2023. Disponível em:https://www.blackhat.com/us 23/briefings/schedule/index.html#jailbreaking-an-electric-vehicle-in--or-what-it-means-to-hotwire-teslas-x-based-seat-heater-33049. Acesso em: 2 nov. 2023.