XXIV SEMEAD
Seminários em Administração
novembro de 2021
ISSN 2177-3866

GOVERNANÇA E PRIVACIDADE DE DADOS PESSOAIS: veículos conectados e as exigências da Lei Geral de Proteção de Dados (LGPD)

NIVALDO CARVALHO DA SILVA
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS (PUC MINAS) - PROGRAMA DE PÓS GRADUAÇÃO EM ADMINIST

HUMBERTO ELIAS GARCIA LOPES
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS (PUC MINAS)

RODRIGO BARONI DE CARVALHO
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS (PUC MINAS)

GOVERNANÇA E PRIVACIDADE DE DADOS PESSOAIS: veículos conectados e as exigências da Lei Geral de Proteção de Dados (LGPD)

1 INTRODUÇÃO

O uso de informações coletadas a partir de ferramentas de mídias sociais, monitoramento de consultas à Internet e dados extraídos de aparelhos pessoais conectados à Internet das Coisas (IoT – *Internet of Things*) tem sido eficaz para determinar o perfil dos consumidores e um aliado em ofertas customizadas de bens e serviços. Este cenário é resultado direto das transformações que decorrem da quarta revolução industrial, a chamada "indústria 4.0", baseada na conectividade de máquinas, digitalização, inteligência artificial e criação de redes inteligentes (Sakura & Zuchi, 2018).

Concomitantemente aos benefícios que essas tecnologias podem proporcionar ao cotidiano das pessoas, emerge a preocupação com o tratamento adequado do número substancial de informações pessoais coletadas por meio destas aplicações de IoT. Isso ocorre porque tal tratamento implica questões cruciais de privacidade que podem surgir a partir da exposição não consentida de dados sensíveis, preferências e hábitos pessoais (Baloyi & Kotzé, 2019). Dessa forma, emerge a necessidade de se proteger a privacidade por meio de requisitos técnicos de segurança da informação, por meio de ações para conscientizar os titulares dos dados sobre os riscos de privacidade em aplicações de IoT e controles sobre o que poderá ser coletado e divulgado (Ziegeldorf, Morchon & Wehrle, 2014).

Em termos mais específicos, a introdução das tecnologias de IoT nos produtos da indústria automobilística tem levado ao desenvolvimento de veículos conectados em países como Estados Unidos, Suécia, China e Coreia do Sul. Estes veículos são centrados nos usuários e não apenas na melhoria do desempenho e eficiência do automóvel tradicional (Cha, Hsu, Xiang & Yeh, 2019). Além disso, neles as preferências pessoais, hábitos de consumo e rotinas diárias ficam disponíveis para o provedor dos serviços de conectividade por meio de tecnologias de geolocalização, rastreamento, histórico das rotas, entre outras (Damjanovic-Behrendt, 2018).

Entretanto, a adoção dessa tecnologia nos veículos tem levantado questões éticas relevantes e têm estimulado as partes interessadas a buscarem respostas para dilemas nem sempre simples de lidar. Uma dessas questões mais importantes – e ainda abordada de maneira incipiente na literatura – é a manutenção da segurança e privacidade dos dados pessoais antes, durante e depois do uso de tecnologias como as utilizadas nos veículos conectados. Este assunto tem ocupado o centro das discussões de pessoas, empresas e governos nos últimos anos (Conrad, 2019). Países e organizações têm buscado tratar da proteção da privacidade por meio de leis e regulamentos aderentes às suas necessidades e realidades socioculturais (Oukemeni, Rifà-Pous & Puig, 2019). O regulamento europeu de proteção de dados (GDPR - *General Data Protection Regulation*), as comissões norte-americanas de tecnologia e a Lei Geral de Proteção de Dados brasileira - LGPD (Lei nº 13.709, 2018) são exemplos de ações governamentais que visam reforçar a proteção dos dados e criar mecanismos que permitam que os indivíduos tenham maior controle sobre os seus dados pessoais (Conrad, 2019).

Portanto, este cenário indica a relevância das questões de privacidade originadas pelas aplicações de IoT em conectividade automotiva, considerando a necessidade da implantação de modelos de governança capazes de atender aos requisitos da LGPD. Dessa forma, o objetivo deste artigo é apresentar uma proposta de modelo de governança de informações e de privacidade de dados capaz de auxiliar o controlador dos dados oriundos da conectividade automotiva a atender as questões de cunho regulatório impostas pela LGPD brasileira e assegurar a privacidade de informações pessoais dos usuários dessas tecnologias.

Para além desta introdução, o artigo está organizado da seguinte forma: a seção 2 compreende o referencial teórico que aborda os temas da governança das informações e da privacidade de dados pessoais; a seção 3 detalha a metodologia de pesquisa baseada em entrevistas em profundidade e a análise de documentos de uma indústria automobilística nacional; a seção 4 engloba análise dos resultados da pesquisa qualitativa; na seção 5 é proposto um modelo de governança de informações e privacidade de dados pessoais integrada com o modelo teórico desenvolvido na seção 2 e com uma análise crítica do modelo de governança em questão adotado pela organização estudada; o item 6 conclui o artigo evidenciando os requisitos para a aplicação do modelo.

2 REVISÃO DA LITERATURA

2.1 Governança de Informações

A governança da informação trata a informação como um ativo corporativo estratégico, maximizando seu valor comercial em detrimento do seu custo de gestão operacional. Isso ocorre por meio de mecanismos para assegurar a sua conformidade, segurança, gerenciamento de riscos e privacidade (Hulme, 2012). O sucesso de um programa de governança da informação passa por duas fases: i) mudança do modelo tradicional de atuação isolada dos departamentos de TI e ii) atribuição, aos especialistas deste setor e das áreas de negócios e jurídica, da tarefa de desenvolver e manter sistemas de informação que atendam aos clientes e às necessidades informacionais e de controle da organização (Coyne, Coyne & Walker, 2018).

O nível de desenvolvimento de um programa de governança da informação considera a capacidade de interação entre os mecanismos estruturais, processuais e relacionais de uma organização para orientar o processo de criação, coleta, armazenamento, análise, uso, distribuição e exclusão de informações relevantes para os negócios, criando valor (Borgman, Heier, Bahli & Boekamp, 2016). O objeto de atuação da governança da informação, porém, vai além da simples gestão e armazenamento dos dados. Na verdade, ele engloba aplicações para gerenciamento de registros, informações e conteúdo corporativo, gestão dos requisitos de privacidade, liberdade de informação, governança corporativa, riscos e segurança da informação e mineração eletrônica de dados (Ajis & Baharin, 2019). Portanto, programas eficazes de privacidade e segurança da informação baseiam-se em modelos sólidos de governança da informação (Briefings on HIPAA, 2017).

2.2 Privacidade de Dados

Conceituar o termo privacidade não é simples, pois ele tem significados diferentes quando confrontado com a realidade de uma sociedade, cultura ou até mesmo da forma em que é aplicado (Oukemeni *et al.,* 2019). O que deve ser mantido em sigilo e o que deve ser revelado muda de uma pessoa para outra. Na década de 1960, o surgimento das tecnologias de processamento eletrônico de dados trouxe consigo as primeiras noções de privacidade dos dados, cujos estudos encampam as teorias de privacidade dominantes até os dias atuais (Whitman, 2003; Langheinrich, 2001; Li & Palanisamy, 2019).

Smith, Dinev e Xu (2011) consideram que as definições de privacidade podem ser baseadas em valores e em cognatos. As primeiras enxergam a privacidade sob o prisma do direito humano integrado ao sistema de valores morais da sociedade e do comportamento do consumidor. Este, paradoxalmente, dispõe-se a compartilhar seus dados pessoais, dentro de uma perspectiva mercadológica, diante da percepção de algum benefício, mesmo em situações em que há preocupação com a privacidade. Por sua vez, as definições baseadas em cognatos entendem que a privacidade deve ser tratada como um estado individual e como controle do

espaço físico e da informação. Neste artigo, a privacidade de dados foi avaliada sob as quatro lentes teóricas em questão, dado o seu caráter mutuamente complementar para fins de obtenção de uma visão abrangente da privacidade.

A abordagem que considera a privacidade como um direito individual deve nortear a construção de modelos eficientes de governança de informações e de privacidade de dados, que sejam capazes de assegurar o cumprimento das exigências contidas nos marcos regulatórios globais e regionais e de resguardar os direitos individuais dos usuários das aplicações de IoT. A LGPD reconhece a privacidade enquanto um direito individual, à medida que assegura ao titular dos dados o direito à portabilidade, a ser esquecido, ao bloqueio, eliminação ou anonimização de suas informações pessoais, dentre outros.Por sua vez, a construção de um modelo justo e equilibrado de troca entre as necessidades dos usuários das aplicações de IoT e as expectativas das áreas de negócio por informações que lhe permitam ofertar novos serviços encontra amparo na perspectiva teórica da privacidade como mercadoria. Neste contexto, a LGPD reconhece a importância do uso das informações pessoais para habilitar e desenvolver transações comerciais que possibilitem a oferta de produtos e serviços aos titulares dos dados ao admitir seu tratamento para, dentre outras, execução de um contrato e apoio e promoção das atividades do controlador dos dados.

A privacidade de dados tida como um estado individual manifesta-se no processo de integração entre o usuário e o ecossistema da aplicação de IoT para assegurar que este indivíduo mantenha ou acesse uma condição de estado de privacidade sempre que julgar necessário. Neste prisma, a LGPD impõe a figura do consentimento e da escolha dos dados que poderão ser tratados como um meio de permitir que o indivíduo se mantenha em estado de isolamento ou para limitar e restringir o acesso a seus dados por terceiros em contextos específicos.

A perspectiva teórica do controle da privacidade deve ser considerada no processo de gestão do ciclo de vida da informação e na construção de barreiras sistêmicas capazes de proteger os dados pessoais dos usuários das tecnologias de IoT contra consultas não autorizadas ou acessos indesejados. Na perspectiva de controle, a LGPD está assentada sobre princípios e valores gerais que tem por objetivo garantir, de maneira transparente, o acesso, controle e segurança das informações pessoais dos indivíduos, restringindo a sua coleta a propósitos legítimos que sejam de pleno conhecimento do titular.

2.3 Estrutura de Governança para a Segurança e Privacidade de Informações

Bamberger e Mullingan (2011) afirmam que a governança de informações e a privacidade de dados estão em um processo de convergência dos modelos de regulamentação tradicional para formas mais colaborativas, experimentalistas e flexíveis de governança, o que permite que organizações regulamentadas possam atender com mais eficiência as demandas das leis de privacidade. A relevância do tema privacidade fez surgir a função de CPO - *Chief Privacy Officer*, que atende a uma necessidade crescente das organizações em manter uma orientação dos líderes de privacidade de alto nível para questões externas, confrontando incertezas decorrentes do contexto normativo dinâmico de privacidade, dos seus impactos nas relações técnicas e comerciais e da importância da existência de uma referência perante os órgãos reguladores (Bamberger & Mullingan, 2011).

Tendo por base preceitos contidos na lei de privacidade norte-americana do setor de saúde (Briefings on HIPAA, 2017), o artigo "*A privacy and information security governance model*" sugere diretrizes para organizações que queiram estabelecer um modelo de governança para a segurança e privacidade das informações. As diretrizes recomendam a seguinte linha hierárquica: Conselho de Administração, Comitê de Supervisão do Programa e CPO.

2.4 Governança de Informações, Privacidade de Dados e o Veículo Conectado (IoT)

O conceito de Internet das Coisas (IoT) foi concebido para descrever as mudanças na vida das pessoas à medida em que dispositivos, máquinas e aparelhos estivessem conectados à Internet (Cha *et al.*, 2019). A Internet das Coisas permite que os objetos utilizados pelas pessoas conectem-se com outros objetos e, simultaneamente, com os seus usuários, representando uma mudança substancial nos parâmetros globais sociais e tecnológicos (Fabiano, 2017). No setor automobilístico, a aplicação das tecnologias de IoT implica mudança conceitual importante, na qual o *design* volta-se para a perspectiva do usuário, agregando serviços inovadores aos produtos, tais como a integração do veículo com as mídias sociais dos ocupantes, o uso de ferramentas de estacionamento e navegação inteligentes, as atualizações *on-line* de mapas e softwares, o gerenciamento do consumo, o tratamento em casos de emergência, dentre outros (Cha *et al.,* 2019).

As chamadas tecnologias incrementais de privacidade (*PET – Privacy Enhancing Technologies*) e os princípios de privacidade desde a concepção da arquitetura dos sistemas (*PbD – Privacy by Desing*) inserem-se no conjunto das modernas ferramentas que podem ser utilizadas para combater as ameaças à privacidade de dados pessoais que emanam das aplicações de IoT. Cha *et al.* (2019) listam as sete seguintes Tecnologias Incrementais de Privacidade (PETs) associadas ao IoT: controle de dados; execução; anonimato e pseudônimo; proteção de dados pessoais; autorização anônima; divulgação parcial de dados; preservação holística da privacidade. A abordagem PbD (Privacidade desde a Concepção) é também baseada em sete princípios fundamentais (Cavoukian, 2011): proativo, não reativo; preventivo, não reparador; privacidade como padrão; privacidade incorporada ao design; funcionalidade total - soma positiva, não soma zero; segurança de ponta-a-ponta do ciclo de vida; visibilidade e transparência; respeito pela privacidade do usuário.

Neste ecossistema complexo do carro conectado, do qual participam diferentes tipos de indústrias (automobilística, tecnologia, comunicação), Zallone (2019) alerta para importância de se debater a função do controlador dos dados. A conclusão deste autor é que, ao menos, o vendedor do veículo e o controlador do sistema de conectividade serão responsáveis pelo controle dos dados, com iguais responsabilidades no tocante a avaliação no impacto da proteção de dados, a privacidade desde a concepção dos sistemas e as formalidades relativas à informação do usuário. O autor considera, ainda, que a segurança dos dados é uma das questões chave, senão a principal, da discussão envolvendo o veículo conectado.

A Figura 1 descreve o *framework* teórico no qual se representa a correlação de forças antagônicas que colocam, de um lado, os benefícios e a percepção de valor dos diversos agentes que compõe o ecossistema do carro conectado e, de outro, os desafios associados à governança de informações e proteção da privacidade de dados decorrente deste tipo de aplicação de IoT.

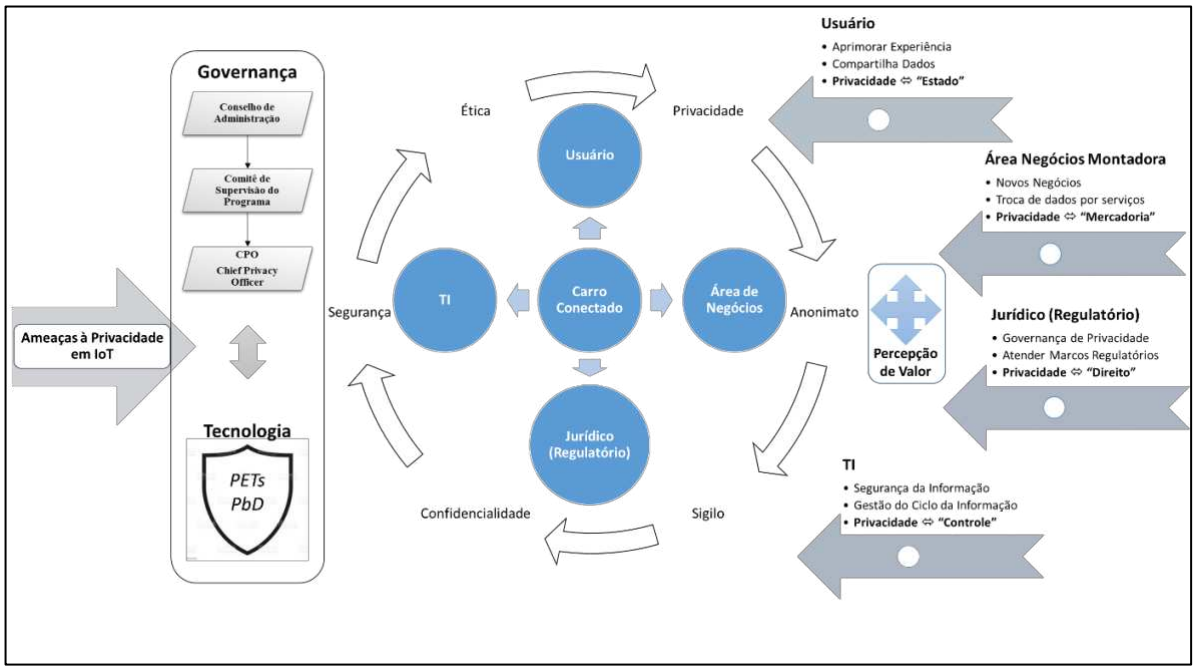

Figura 1. *Framework* teórico de governança e privacidade de dados no ecossistema do carro conectado. Fonte: elaboração dos autores

A forma como interagem o veículo, seu usuário e os demais agentes responsáveis pelo fornecimento dos serviços de conectividade, aqui representados pela figura das áreas de negócio (*business*), TI e Jurídico (Regulatório), pressupõe um ambiente novo e complexo em termos de segurança e privacidade das informações, porém com um nível de experiência e de percepção de valor associado ao uso do produto superior ao de um veículo tradicional.

O desenvolvimento de uma cultura organizacional associada à proteção da privacidade de dados e lastreada na aplicação de preceitos éticos, de anonimato, de confidencialidade, dentre outros, é peça fundamental para que se possa construir um modelo operacional de conectividade capaz de aliar, de maneira eficiente, a segurança e a privacidade das informações pessoais coletadas a partir do veículo conectado e a absorção da percepção de valor por parte das áreas de negócio e do próprio usuário do veículo.

Na perspectiva do usuário a percepção de valor materializa-se, dentre outros, pelo acesso de novos serviços, melhoria da experiência com o produto, incremento dos níveis de segurança do veículo, desde que respeitadas as condições que permitam ao usuário do veículo conectado manter ou acessar uma condição de estado de privacidade. Sob o prisma das áreas de negócio da montadora, quer estejam associadas a vendas ou a pós-vendas, a conectividade em veículos revela um cenário vasto de oportunidades de oferta de serviços e de criação de novos negócios que, certamente, irá encorajar o usuário do veículo a compartilhar suas informações pessoais em troca de benefícios proporcionais e justos, reforçando a abordagem conceitual da privacidade enquanto mercadoria.

Quando visto pela lente jurídico-regulatória, o ecossistema do carro conectado deve ser construído com base em orientações que assegurem o cumprimento dos requisitos impostos pelos marcos regulatórios globais e regionais, trazendo o equilíbrio necessário capaz de equalizar de maneira positiva as necessidades dos usuários e o apetite das áreas de negócio pela busca de informações que lhe permitam ofertar serviços diferenciados, reforçando a necessidade de desenvolvimento de estruturas formais de governança de informações e, também, os requisitos de privacidade associados a direitos individuais das pessoas.

Cumpre à área de TI a responsabilidade pela construção desse ecossistema de conectividade, tendo como premissa os anseios, necessidades e deveres associados aos

construtos de governança e de privacidade, adotando mecanismos e ferramentas capazes de proporcionar excelência no processo de gestão do ciclo de vida da informação e atender aos requisitos de controle da privacidade de dados.

Neste contexto, a criação de estruturas organizacionais dedicadas à governança de informações e privacidade de dados apresenta-se como uma medida saudável para auxiliar no processo de gestão da segurança e privacidade de informações, que associadas às estruturas multifuncionais de governança, o uso das chamadas tecnologias incrementais de privacidade (PETs) e a adoção dos princípios de *privacy by design* (PbD) na construção da arquitetura dos sistemas do veículo conectado, parecem ser um caminho viável para combater as ameaças à segurança e privacidade dos dados pessoais no ecossistema do veículo conectado (IoT). A seção seguinte detalha os procedimentos metodológicos para a investigação que foi lastreada no *framework* apresentado.

3 METODOLOGIA

Esta pesquisa é qualitativa e exploratória. Como a conectividade automotiva está em um estágio inicial de massificação no Brasil, o que reduz o número de potenciais objetos de estudo, optou-se por desenvolver a pesquisa baseada no método de estudo de caso único.

O projeto de conectividade automobilística de uma indústria de grande porte estabelecida na região Sudeste foi escolhido como unidade empírica de análise. Para os fins deste estudo, esta indústria é referida sempre como 'montadora', como forma de manter anônimos a organização e os entrevistados. Este projeto de conectividade, que ainda está em fase de desenvolvimento e deverá entrar em operação a partir do segundo trimestre de 2021, conta com uma particularidade relevante: está sendo construído concomitantemente à entrada em vigor das normas da LGPD.

Como base no *framework* teórico, os requisitos de privacidade de dados pessoais no ambiente do veículo conectado foram avaliados sob quatro categorias distintas. A primeira categoria ("Contexto Jurídico-Regulatório no Carro Conectado – LGPD") avaliou a aderência da estrutura organizacional da empresa aos requisitos de segurança e de proteção da privacidade de dados, tidos como melhores práticas pela literatura especializada. Adicionalmente, foram avaliados os requisitos de privacidade adotados pelo projeto do veículo conectado que busquem assegurar os direitos dos indivíduos à privacidade de dados.

Na segunda categoria de análise ("Novos Negócios Associados ao Carro Conectado"), foram analisados as principais funcionalidades a serem ofertadas aos usuários do veículo conectado e os aspectos mercadológicos da privacidade. A terceira categoria de análise ("Segurança dos Sistemas do Carro Conectado") abordou os requisitos de segurança dos sistemas do carro conectado que atendam às necessidades de controle da privacidade de informações pessoais e da própria LGPD.

A quarta categoria de análise ("Interações de Privacidade do Usuário com o Carro Conectado") abordou as interações de privacidade que estarão disponíveis para o usuário do veículo conectado e que lhe permitam acessar, quando julgar necessário, uma condição de estado de privacidade, compartilhando ou bloqueando o compartilhamento de seus dados pessoais.

As entrevistas foram realizadas entre setembro e novembro de 2020 por meio de um roteiro semiestruturado. Foram selecionados candidatos das áreas (i) "jurídico-regulatórias" responsáveis pelo suporte técnico de privacidade na construção dos sistemas do carro conectado e implantação do projeto de conformidade da LGPD dentro da 'montadora', (ii) "tecnologia da informação" responsáveis pela construção dos sistemas do veículo conectado e adaptações aos sistemas da 'montadora' para atendimentos dos requisitos da LGPD e de (iii) "negócios" responsáveis pelo desenvolvimento do projeto do veículo conectado no País. O roteiro

semiestruturado foi organizado para se encaixar nas categorias de análise de pesquisa, sem perder de vista a flexibilidade para tratar questões envolvendo áreas de conhecimento diferentes (jurídico, TI e negócios).

Os dados das entrevistas foram tratados pela técnica de análise de conteúdo (Silva & Fossá, 2013). Desta forma, transcreveram-se as 15 (quinze) entrevistas realizadas, que foram juntadas à entrevista respondida por *e-mail*, de modo a facilitar o processo de análise de conteúdo e garantir a fidedignidade dos dados prestados pelos respondentes. Após transcritas, as respostas foram catalogadas segundo as categorias primárias e secundárias como forma de facilitar a análise de conteúdo. A coleta de dados a partir de documentos, fonte secundária, envolveu a análise de documentos e *sites* da 'montadora' de modo a possibilitar o processo de triangulação de dados com o objetivo de confirmar, contestar e analisar os dados coletados a partir das fontes primárias (Yin, 2005).

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

4.1 Caracterização da Amostra

A coleta primária de dados baseou-se nas 15 (quinze) entrevistas em profundidade que envolveram profissionais das áreas "jurídico-regulatória" (38% dos entrevistados), de "tecnologia da informação" (24% dos entrevistados) e de "negócios" (38% dos entrevistados) ligados ao projeto de conectividade automotiva da 'montadora'. O 16a. entrevistado respondeu o roteiro por e-*mail* por dificuldade de disponibilidade de agenda.

Os entrevistados que ocupam as funções de "diretores" (18% dos entrevistados) correspondem ao segundo nível de gestão da 'montadora' e respondem pela região da América Latina. Os "gerentes" (32% dos entrevistados) e "coordenadores" (32% dos entrevistados) ocupam funções de gestão de terceiro e quarto níveis, com atuação, na maioria dos casos, restrita ao mercado brasileiro. Os demais entrevistados desempenham papéis de nível técnico especializado e não ocupam cargos de gestão (18% dos entrevistados). Os profissionais da área "jurídico-regulatória" atuam na 'montadora" a menos de 5 anos, o que coincide com a recente escalada do tema "privacidade de dados" no País, cujo principal expoente foi a publicação da LGPD. Por sua vez, os profissionais das áreas de "negócios" e "TI" atuam a mais de 10 anos na organização.

4.2 Análise Qualitativa dos Dados

O modelo de governança dos dados pessoais coletados a partir das funcionalidades do veículo conectado baseou-se nas melhores práticas de proteção de dados e na LGPD e considerou um recorte específico que considera as obrigações da 'montadora' no tocante tratamento de dados pessoais de seus clientes de conectividade. Este modelo de governança foi avaliado sob as perspectivas detalhadas e discutidas a seguir: "jurídico-regulatória", "novos negócios", "segurança dos sistemas" e "interações de privacidade entre o usuário e o veículo conectado". Os resultados estão lastreados pela análise de conteúdo das entrevistas em profundidade. Nas subseções a seguir, a análise é ilustrada com trechos literais significativos que visam elucidar como a 'montadora' está estruturada para atender os requisitos de privacidade.

4.2.1 Contexto Jurídico-Regulatório do Veículo Conectado

Avaliou-se o esforço da 'montadora' para materializar uma estrutura dedicada à governança da segurança e da privacidade de informações com foco nas questões legais e capaz de estabelecer parâmetros para uma relação equilibrada entre as necessidades de privacidade dos usuários e a demanda das áreas de negócio por informações que lhe permitam ofertar serviços diferenciados. A revisão da literatura ressalta a importância da existência de uma "Estrutura de Governança da Privacidade" dedicada. Concluiu-se que a 'montadora' possui esta estrutura formal e independente (DPO – *Data Protection Officer*) orientada às questões de segurança e privacidade de dados no âmbito da região da América Latina, composta por um time multidisciplinar formado por profissionais das áreas jurídica e de ICT (*Information Communication Technology*), conforme atestado pelo depoimento a seguir.

- *A gente hoje tem como governança um comitê técnico no Brasil (...) mantendo todos os nossos processos aderentes à LGPD.* (E2)

A 'montadora' adotou, ainda, o "Princípio da Minimização da Coleta de Dados Pessoais" requerido pela LGPD, mediante execução de mapeamento das informações pessoais coletadas pelos processos e sistemas.

- *Então é o mínimo necessário sem a exposição do cliente. Isso é base também de construção. (E5)*

Nos casos em que ocorrem "Coleta e Processamento de Dados por Terceiros" (concessionárias da marca e fornecedores de serviços de conectividade), as entrevistas evidenciaram um esforço da 'montadora' em rever as suas bases contratuais para incluir cláusulas específicas de responsabilidade inerentes ao tratamento de dados por seus concessionários e fornecedores. No entanto, a 'montadora' reconhece que as ações de conformidade legal e contratual podem não ser suficientes para evitar violações de segurança e privacidade de dados em função da capacidade limitada de ingerência da 'montadora' sobre os processos dos terceiros.

- *(...) tem normalmente algumas cláusulas reforçando e dizendo o que pode ser feito com os dados. Os dados compartilhados são só aqueles necessários para a prestação de serviço. (E15)*
- *Temos uma estrutura criada no âmbito da ('montadora') (...) para que esses comitês acompanhem e consigam dar a política e diretrizes de monitoramento adequado para as empresas parceiras. (E8)*
- *(...) a gente não tem um controle 100% sobre isso, porque eu não tenho ingerência sobre a concessionária. Inclusive a Lei Ferrari me proíbe de ter essa ingerência (...). (E2)*

No entanto, a 'montadora' declarou possui um plano formal para o tratamento de eventuais "Violações à Privacidade de Dados" que, no entanto, não pudemos ter acesso por ter sido informado tratar-se de documento restrito.

- *O plano ele tem "approaches" diferentes dependendo da gravidade da violação. (...) Plano de Ação de Incidentes. (...) Ele é um documento interno. (...) Não vai ser uma norma divulgada. (E2)*

Deve-se considerar ainda que a condução de um veículo conectado admite que sejam acessadas informações que não estão acessíveis nos veículos convencionais, que podem não ser conhecidas por um novo usuário. Apesar de não existir um "Programa de Conscientização dos Usuários" do veículo conectado, a 'montadora' salientou que o papel de conscientização do mesmo será desempenhado pela política de privacidade.

- *A política de privacidade a gente faz., Se você ver, lá está igual bula de remédio. (E2)*
- *Por exemplo, "call center", se o cliente ligar e pedir informações a respeito, ele terá a informação acessível na base de conhecimento, para que o operador possa passar para ele com detalhes. (E15)*

O acesso à "Política de Privacidade" e os termos de uso do veículo conectado poderão ser acessados pelo usuário por meio de diferentes plataformas.

- *(...) a gente vai dar os caminhos das pedras pra ele (o cliente) acessar a política de privacidade e ter conhecimento de quais dados estão sendo coletados e quais as finalidades (...). (E3)*

O processo de "Aviso de Coleta" de dados pessoais se dará por meio de vários mecanismos, tais como a própria *head unity* (rádio) do veículo, *website* e aplicativo de *smartphone.* A coleta ocorrerá em momentos diferentes do processo de interação entre o usuário e o veículo conectado.

- *(...) sempre que ocorra coleta de dados, o cliente seja avisado, ou ele tenha o direito de escolher ou não se fazer essa coleta. (E8)*

A ‘montadora’ disponibiliza também ferramentas que asseguram ao usuário em questão o acesso ao direito à “Portabilidade de Dados” prevista na LGPD. Compete ainda ao usuário de informar a ‘montadora’ acerca da venda do veículo para se cesse a coleta de dados.

- *Os dados pessoais sempre vão caminhar junto da pessoa. Os dados do veículo, quando forem importantes, vão caminhar com o veículo. (E10)*
- *É obrigação sua informar a (‘montadora’) essa venda, para que a gente faça primeiro, retire aquela vinculação daquele VIN (chassi) aos seus dados pessoais. (E3)*

Por fim, como último quesito do contexto “Jurídico-Regulatório”, concluiu-se que os dados coletados a partir dos sistemas do veículo conectado não ferem o “Princípio da Não Discriminação” previsto na LGPD, que por sua vez veda expressamente o tratamento de informações pessoais que possam causa danos ao titular por serem discriminatórios, ilícitos ou abusivos.

- *Considerando este conceito e o contexto do carro conectado, não há quaisquer serviços ou funcionalidades construídas com esse fim. (E7)*

4.2.2 Novos Negócios Associados ao Veículo Conectado

Sem perder de vista as questões regulatórias e de conformidade exigidas pela LGPD, o desenvolvimento das tecnologias de conectividade automotiva está associado aos novos negócios e à percepção de uma troca justa como o consumidor fornecendo dados pessoais em prol de uma experiência diferenciada na condução do veículo conectado. A partir das entrevistas, foi possível identificar os elementos de inovação disruptiva nas “Funcionalidades do Veículo Conectado” e a percepção da ‘montadora’ acerca do futuro deste produto.

- *A conectividade é revolucionária pra indústria. (E16)*
- *(...) à experiência do cliente, então vai desde ele entregar o carro na mão de um filho, e habilitar uma barreira virtual, aonde se o carro sair de um bairro para outro bairro, aquilo me avisa e eu posso mandar um comando pro carro ou não. (E4)*

Neste contexto, surge a preocupação com a “Coleta de Dados sem o Consentimento do Usuário”. Documentos recebidos por *e-mail* dos Entrevistados nº 03 (02/10/2020) e nº 12 e 15 (27/11/2020) indicam que o tratamento de dados será feito sem o consentimento específico do usuário somente nos casos em que há baixa exposição à privacidade de titulares e nos casos de indícios de problemas nos veículos que possam colocar em risco a integridade física de seus ocupantes (acidentes ou necessidade de *recall*). Por sua vez, as funcionalidades capazes de determinar perfis dos usuários farão a coleta apenas mediante obtenção de consentimento específico do usuário, sobretudo nos casos em que ocorre o compartilhamento de dados com terceiros.

- *(...) uma falha que pode colocar a vida dessa pessoa em risco, o carro pode acender o alerta, pode bloquear partida, pode fazer diversas coisas que o cliente não (...) precisa dar o de acordo. (E11)*
- *(...) se acontecer falhas, hoje o carro já registra falhas eletrônicas, que acontecer por exemplo. (...) E aí independente do cliente querer, é compartilhado. (E15)*

As políticas de privacidade do veículo conectado preveem a possibilidade da coleta de dados pessoais relacionados com a geolocalização, histórico de rotas, perfil de condução e dados relativos a acidentes com o veículo. Indubitavelmente, o acesso a essas informações pode levar à construção de “Perfis de Comportamento” pessoais, preferências de consumo, religiosas, sexuais, dentre outras informações de caráter sensível, que requerem um tratamento diferenciado por parte do controlador dos dados. No tratamento automatizado de informações pessoais dos usuários, a coleta será voltada para a figura dos chamados *drive score* (pontuação de direção) que, além do potencial comercial, pode ajudar os usuários a melhorar sua segurança na direção, consumo de combustível e o uso racional do veículo e que serão tratadas mediante consentimento do usuário.

- *Os sistemas provavelmente serão capazes de detectar padrões, o que não quer dizer que essas funcionalidades serão de fato utilizadas. (...) o usuário precisa ser avisado antes da coleta.. (E7)*

- *Todas as vezes que o titular se sentir prejudicado por uma decisão automatizada, que ela é tomada com base em algoritmo, ele pode pedir a revisão dessa decisão. Sempre. É um direito dele. (E2)*

Por fim, como último tópico da perspectiva de "Novos Negócios" do veículo conectado, buscou-se entender a visão da 'montadora' acerca da utilização da base de dados pessoais para a realização de "Campanhas Publicitárias" sem que se obtivesse o consentimento prévio do titular dos dados. A LGPD admite que dados pessoais sejam tratados com vistas ao "apoio e promoção das atividades comerciais do controlador dos dados", que justificariam a execução de atividades publicitárias baseadas no legítimo interesse do controlador dos dados. Restou claro que campanhas publicitárias baseada no legítimo interesse do controlador se enquadram em uma zona extremamente sensível de risco à privacidade dos usuários do veículo conectado, justamente por estar inserida em uma área controversa da legislação (LGPD).

- *O nosso entendimento é que existem, é um limiar tênue, mas existe uma diferença. (...), a análise vai ser feita no caso concreto, e esse legítimo interesse não pode ultrapassar os direitos fundamentais do titular do dado. (E2)*

4.2.3 Segurança dos Sistemas do Veículo Conectado

Nesta subseção, foram explorados os requisitos de segurança da informação e de proteção da privacidade dos usuários do veículo conectado, à luz dos princípios contidos na LGPD e dos aspectos que reforçam a abordagem conceitual de privacidade enquanto controle. Por meio do acesso à pasta de documentos disponível na rede interna da 'montadora' concedida pelos Entrevistados nº 7 e 13, foi possível ter acesso ao documento que contém as diretrizes da organização relativas à "Política de Segurança da Informação" e às políticas de privacidade desenvolvidas especificamente para clientes, fornecedores, empregados, dentre outros. A responsabilidade pela elaboração e atualização do documento é do ISSO (*–Information System Security Officer)*, estrutura operacional que se reporta diretamente ao CIO.

A adição de novas tecnologias aos veículos traz consigo um incremento da preocupação com a "Segurança dos Sistemas" e a privacidade das informações armazenadas no veículo ou em dispositivo a ele ligados. A 'montadora' se preocupa com a possibilidade de acessos indesejados aos sistemas do veículo conectado e adota este expediente de contratar empresas especializadas para identificar possíveis brechas nos seus sistemas.

- *Nós contratamos "hackers" pra atacar os nossos sistemas, pra fazerem testes. (...) você ter uma boa governança de proteção de dados, está na definição dos processos. Quem tem acesso e a que nível de informação essa pessoa tem acesso. (E8)*

Os requisitos de segurança estão separados entre o ambiente *on board* do veículo conectado, representado pelos sistemas e funcionalidades do próprio veículo, e o ambiente *off board,* que correspondea todos os sistemas externos e meios de comunicação com o referido veículo.

- *(...) hoje existe equipes de arquiteturas de "cyber security" globais. Tanto pro mundo "on board", "off board", como gestão e monitoramento vinte e quatro por sete, redundância, cobertura, a níveis máximos de segurança que a gente conhece no mercado. (E5)*

A literatura recomenda a utilização dos princípios de "Privacidade desde a Concepção" (PbD) dos sistemas como forma de assegurar a privacidade de informações pessoais no processo de construção da arquitetura dos sistemas. As entrevistas revelaram que enquanto os sistemas já existentes da 'montadora' tiverem que ser revistos para incluir regras de privacidade das informações, os sistemas do veículo conectado já nasceram com os princípios de *privacy by design* (PbD).

- *O carro conectado é o primeiro projeto, assim, "Privacy By Design. (E2)*
- *(...) grupos de discussão multidisciplinares são formados, envolvendo profissionais de TI, Jurídico, Marketing, Produto, entre outros departamentos. (E7)*

As tecnologias incrementais de privacidade (PET – *Privacy Enhancing Technologies*) apresentam alternativas para melhorar a segurança e a privacidade das informações

transacionadas a partir das tecnologias de IoT. As entrevistas sinalizaram que a 'montadora' utiliza "Ferramentas que Bloqueiam ou Dificultam a Ligação" dos dados pessoais e seus titulares por meio de técnicas de criptografia e de chaves para anonimização de dados pessoais.

- *(...) você anonimiza uma parte, usa chaves que não são correlacionáveis no outro. (E4)*
- *(...) a empresa acompanha os ataques, que por ventura tenha a esses ambientes, ou invasões, pra tentar, sem dúvida, sempre evoluir e bloquear. (E10)*

A 'montadora' utiliza também mecanismos de "Autenticação e Controle de Acesso" dos sistemas como forma de bloquear consultas indevidas que possuem potencial significativo para apresentar danos à privacidade, prejuízos ligados à perda ou roubo de dados ou até mesmo interrupção temporária da operação das empresas.

- *Existe uma política de autenticação baseada em senha forte com verificação, o que a gente chama de "two step verification" (...). (E4)*

Em se tratando do veículo conectado, surge a preocupação com a, eventual, coleta de dados pessoais de outros que não sejam o contratante dos serviços de conectividade, sobretudo em situações que envolvam o transporte de passageiros em veículos de aluguel (locadoras, táxi, Uber, dentre outros) que não contem com a ciência ou consentimento do titular dos dados. A partir das entrevistas, foi possível identificar que a coleta de dados de passageiros do veículo conectado não poderá ser realizada, a menos que o passageiro decida criar um perfil próprio para personalizar sua experiência em relação às funcionalidades disponibilizadas através dos serviços de conectividade.

- *Então se ele tiver multiusuários, ele terá que fazer todo esse processo de ativação do serviço para ele, e o consentimento especifico para ele. (E10)*

Fortemente inspirada da GDPR europeia, a LGPD contempla no seu texto limitações à transferência internacional de dados pessoais para países que não ofereçam um grau similar aos seus em termos de proteção da privacidade. Por se tratar de um projeto de veículo conectado que está sendo desenvolvido globalmente pela 'montadora' em conjunto com as suas operações na Europa e nos Estados Unidos da América, as entrevistas indicaram que haverá o tratamento de dados pessoais em outros países, dado que em sua maioria os fornecedores contratados são *players* globais do projeto e que esta transferência está em conformidade com o que dispõe a LGPD brasileira.

- *(...) um time centralizado que cuida da segurança da informação, LGPD, a particularidade de cada região junto com a gente, pra garantir que os requisitos (..) de segurança sejam atendidos. (E13)*

Como último requisito de segurança dos sistemas, observou-se que a 'montadora' disponibiliza "Canais para Denúncias", que também servem para esclarecimento de dúvidas e solicitação de informações associadas à privacidade de dados pessoais. De maneira análoga, como requisito da Política de Segurança da Informação, são realizadas auditorias periódicas como forma de se antecipar eventuais problemas de segurança e privacidade.

- *Existem, sim, mecanismos de auditoria dos sistemas de informação. (...) requisições dos titulares de dados poderão ser enviadas para o e-mail privacidade@ 'montadora'.com. (E7)*
- *(...) na estrutura do DPO, nós temos, além do canal de denúncias, a definição da pessoa, da estrutura que receberá e tratará dessas denúncias. (E8)*

4.2.4 Interações de Privacidade do Usuário com o Veículo Conectado

As questões de ordem regulatória de privacidade trazidas pela LGPD demandam que o ecossistema de conectividade deve ser dotado de ferramentas que permitam este usuário consiga manter ou acessar uma condição de estado de privacidade, sempre que julgar necessário, mesmo que isso implique em ruptura do processo de conexão veicular. Em relação ao processo de "Escolha", manifestação do "Consentimento" e eventual "Revogação do Consentimento" dado, as entrevistas indicaram que haverá momentos diferentes nos quais este usuário pode optar pela configuração de privacidade que melhor lhe atende, cuja escolha, ativação e desativação dos serviços pode ser feita diretamente na concessionária no momento da retirada do veículo novo adquirido ou posteriormente via *website* e aplicativo de *smartphone*.

- *(...) no primeiro acesso dele ele já tem a possibilidade de conhecer todas as políticas, todas as regras (...) de gerenciamento dos dados, bem como a aplicação deles como um todo. (E5)*
- *(...) o cliente fez essa ativação e em qualquer momento durante o período que ele usufrua do serviço, ele poderá mudar este consentimento. (E10)*

As entrevistas revelaram, ainda, que nos sistemas do veículo conectado estará disponível uma função denominada *privacy mode* que permitirá ao usuário do veículo conectado "Bloqueio de Acesso" a seus dados e aos serviços de conectividade, sem prejuízo das escolhas e do consentimento dado no momento da contratação dos serviços de conectividade, que serão se tornarão novamente válidos tão logo esta função seja desativada.

- *(...) o cliente quando estiver usufruindo o seu veículo, neste ambiente "on board", ou seja, de dentro do veículo, ele vai poder ter acesso a essa função "privacy mode" ativando ou desativando. (E10)*

Considerando que LGPD garante também ao titular das informações pessoais o direito à confirmação da existência de tratamento de dados e "Acesso e Correção" de seus dados pessoais, observou-se que o acesso aos dados e a correção de informações estarão disponíveis para o usuário por meios dos seguintes canais de comunicação entre a 'montadora' e seus clientes: *e-mail, website* ou *call center*.

5 PROPOSTA PARA UM MODELO DE GOVERNANÇA E PRIVACIDADE DE DADOS PESSOAIS E SÍNTISE CRÍTICA DO ESTUDO DE CASO

A Figura 2 exibe o modelo proposto de governança de dados pessoais que observa as melhores práticas de proteção de dados, os preceitos tidos como válidos pelas modernas teorias de privacidade, bem como os requisitos de cunho regulatório na LGPD brasileira. O recorte específico considera as necessidades e a visão da indústria no tocante à obrigatoriedade de se implantar medidas que assegurem a privacidade de dados pessoais de seus clientes e usuários do veículo conectado.

A avaliação que emerge da análise dos dados obtidos a partir do estudo de caso levou em consideração os seguintes fatores limitadores externos: (i) ausência de regulamentação da LGPD, o fato de os (ii) organismos de privacidade estarem em Fase de consolidação, dentre eles a ANPD (Autoridade Nacional de Proteção de Dados) e, por fim, o (iii) baixo nível de maturidade das discussões sobre privacidade associadas ao uso destas tecnologias. Os resultados da análise do modelo proposto (Figura 2) foram agrupados nas seguintes categorias:

i) **"Atende"** quando os dados coletados comprovam o atendimento aos requisitos de privacidade contidos na literatura que sustenta esta pesquisa;
ii) **"Atende com Pontos de Atenção"** quando os dados coletados comprovam o atendimento dos requisitos de privacidade, porém estão sujeitos aos fatores limitadores externos apresentados ou a limitações internas da organização estudada;
iii) **"Não Atende"** o modelo de governança nos casos em que não se comprovem ações concretas capazes de atender aos requisitos de privacidade contidos na literatura;

Na perspectiva jurídico-regulatória, destaca-se a existência de uma estrutura multidisciplinar (jurídico e TI) dedicada à governança das informações e privacidade de dados e independente das áreas de negócio (DPO – *Data Privacy Office*), subordinada à comitês regionais (América Latina) e globais de privacidade, que é aderente aos preceitos mais modernos da literatura de privacidade apresentados nessa pesquisa. Os principais desafios a serem enfrentados nesta perspectiva relacionam-se com processo de coleta e tratamento de dados realizados por terceiros, dada a capacidade limitada de ingerência da 'montadora' sobre os processos e sistemas, além da dificuldade para estruturar processos que sejam efetivos contra fatores humanos (erros ou fraudes ligadas a vazamento de dados).

Na perspectiva de novos negócios, a aplicação das tecnologias de IoT nos produtos da indústria automobilística tem potencial para redesenhar a cadeia de valores destes produtos,

mediante adição de serviços específicos e personalizados ao processo de comercialização do veículo. Todavia, deve-se observar a necessidade de se estabelecer limites para a coleta de dados baseada em padrões de comportamento do usuário do veículo conectado, justamente para que não sejam acessados dados pessoais sensíveis (preferências sexuais, religiosas, políticas, dentre outras) ou informações que possam representar algum tipo de risco à privacidade destes usuários. Adicionalmente, salvo os casos que possam se amparar na base legal de tratamento que vise assegurar a proteção da saúde e da integridade física dos usuários do veículo conectado, a indicação de que as estruturas do DPO e dos comitês de privacidade serão responsáveis se apresenta como uma solução adequada para tratar eventuais abusos em campanhas publicitárias e para também avaliar situações que justificam o tratamento de dados pessoais com base no "legítimo interesse" da 'montadora'.

Objetivo Geral	Governança da Privacidade no Veículo Conectado			Objetivo Específico	Componentes do Modelo de Governança de Segurança da Informação e da Privacidade de Dados	Análise Crítica do Estudo de Caso
	Perspectiva	Agentes Principais	Teorias de Privacidade			
Modelo de Governança de Informações e de Privacidade de Dados no Veículo Conectado	Jurídico-Regulatório	Estrutura de Governança de Privacidade ICT	Privacidade Enquanto Direito do Titular	O.E. "C"	Estrutura de Governança da Privacidade	✓
					Dados Pessoais Coletados (Princípio da Minimização da Coleta de Dados)	✓
					Coleta e Processamento de Dados por Terceiros (Concessionárias e Fornecedores)	✓ ⚠
					Violações de Privacidade (Tratamento de Incidentes)	✓
					Programa de Conscientização dos Usuários (Princípio do Livre Acesso e da Transparência)	✓
					Políticas de Privacidade	✓
					Aviso de Coleta e Portabilidade de Dados	✓
					Princípio da Não Discriminação	✓
	Novos Negócios	Áreas de Negócio Estrutura de Governança de Privacidade	Privacidade Enquanto Mercadoria	O.E. "A"	Funcionalidades do Veículo Conectado	✓
				O.E. "D"	Coleta de Dados sem o Consentimento do Usuário	✓
					Padrões de Comportamento e Tratamento de Perfis dos Usuários do Veículo Conectado	✓ ⚠
					Campanhas Publicitárias	✓ ⚠
	Segurança dos Sistemas	ICT Estrutura de Governança de Privacidade	Privacidade Enquanto Controle	O.E. "B"	Política de Segurança da Informação	✓
					Segurança dos Sistemas do Veículo Conectado	✓ ⚠
					Privacidade Desde a Concepção (*Privacy by Design* - PbD)	✓
					Ferramentas que Bloqueiem ou Dificultem a Ligação entre Dados Pessoais e os Titulares das Informações	✓
					Autenticação e Controle de Acesso	✓
					Coleta de dados de passageiros	✓
					Armazenamento e Processamento de Dados Fora do País	✓
					Auditoria e Canal de Denúncia	✓
	Interações de Privacidade do Usuário	Estrutura de Governança de Privacidade ICT	Privacidade Enquanto um Estado	O.E. "C"	Escolha, Consentimento e Revogação do Consentimento	✓
					Bloqueio de Acesso aos Dados	✓
					Acesso e Correção de Dados	✓

Legenda: ✓ Atende ✓ ⚠ Atende / Pontos de Atenção ✗ Não Atende

Figura 2. Modelo proposto de governança de informações e de privacidade de dados no veículo conectado. Fonte: dados da pesquisa.

Na perspectiva de segurança dos sistemas, observam-se os esforços da 'montadora' para assegurar a privacidade de dados e para combater eventuais consultas não autorizadas ou tentativas de ataques cibernéticos (*hackers*) no veículo conectado. Considera-se adequada a segregação dos ambientes interno (*on board*) e externo do veículo (*off board*), cuja ligação se dá por meio de chaves criptografadas e de redundância de autenticações. Todavia, como destacado pela própria 'montadora', violações de privacidade não são fruto unicamente de

brechas ou vulnerabilidades dos sistemas. O principal desafio relativo a este quesito recai exatamente sobre a necessidade de manter os sistemas seguros, mediante adoção ferramentas e técnicas modernas de segurança capazes de combater novas ameaças cibernéticas.

Por fim, na perspectiva das interações de privacidade entre o usuário e o veículo conectado, deve-se considerar o baixo nível de maturidade dos usuários em relação ao uso destas tecnologias e das questões de privacidade a ela associadas. De toda sorte, observou-se que a 'montadora' incorporou elementos ao seu modelo de governança de informações e de privacidade que permitem que o usuário possa acessar uma condição de privacidade interrompendo, ainda que temporariamente, o processo de conectividade automotiva.

6 CONCLUSÃO

Os resultados evidenciam que, se não tratadas adequadamente, sérias questões de privacidade podem surgir a partir da exposição indesejada ou não consentida de hábitos, preferências pessoais e de dados pessoais sensíveis, coletados a partir funcionalidades do veículo conectado, assim entendido como o produto resultante da aplicação das tecnologias da Internet das Coisas (IoT) no campo automotivo. Concluiu-se também que a correlação entre a conectividade automotiva e a privacidade de dados pessoais está inserida em um campo acadêmico ainda pouco explorado em termos de estudos científicos no Brasil. Isto é plenamente justificado pois a conectividade automotiva está em um processo embrionário de desenvolvimento no País, mas com uma tendência de rápida massificação. Já a privacidade, apesar da ampla literatura existente, se relaciona em termos empíricos no contexto nacional com um marco regulatório (LGPD) que entrou em vigor apenas em setembro de 2020.

Foi possível concluir ainda que a criação de mecanismos de governança de informações voltados para a privacidade de dados pessoais, no Brasil, precisa romper barreiras adicionais decorrentes do baixo nível de maturidade das discussões sobre o tema no País que, somada às ausências de uma regulamentação detalhada da LGPD e da divulgação das diretrizes da Política Nacional de Proteção de Dados Pessoais e da Privacidade pela ANPD, terminam por produzir um ambiente permeado por incertezas do ponto de vista regulatório.

Do ponto de vista teórico, constatou-se que a adoção dos princípios de governança da informação e da privacidade baseados nas tecnologias incrementais de privacidade (PETs) e nos requisitos de privacidade desde a concepção da arquitetura dos sistemas (PbD), em conjunto com a criação de uma estrutura independente dentro da organização que disponibilize recursos humanos dedicados a esse processo de governança, são capazes de gerar respostas efetivas no combate às ameaças à privacidade de dados em aplicações de IoT.

Concluiu-se que a organização estudada realizou um trabalho minucioso para associar as bases legais de tratamento de dados previstas na LGPD ao processo de coleta e tratamento de informações realizado por cada uma das funções que estarão disponíveis no veículo conectado. O modelo proposto por esta pesquisa para a governança de informações e privacidade de dados pessoais coletados a partir das funcionalidades do veículo conectado apresenta uma abrangência significativa, à medida que foi possível associar, em quatro perspectivas distintas e mutuamente complementares, os principais agentes impactados pelo ecossistema do veículo conectado com as quatro lentes teóricas sob as quais se pode entender a privacidade (direito, mercadoria, controle, estado).

Cumpre ressaltar que o enfoque desta pesquisa foi o de apresentar uma proposta de modelo de governança de informações e de privacidade de dados capaz de auxiliar o controlador dos dados oriundos da conectividade automotiva a atender as questões de cunho regulatório impostas pela LGPD brasileira e assegurar a privacidade de informações pessoais dos usuários dessas tecnologias. Desta forma, não se pode deixar de evidenciar que ainda existem diversas

lacunas a serem preenchidas no campo de estudos ora discutido, fato que abre um leque de oportunidades de estudos que poderão ser exploradas por pesquisadores no futuro.

Na perspectiva dos consumidores, usuários dos serviços de conectividade automotiva, pode-se buscar entender e avaliar qual é nível de percepção de valor desses serviços e os impactos no seu cotidiano face a introdução de tecnologias de conectividade em veículos. Em outra linha de pesquisa pode-se avaliar a percepção dos consumidores brasileiros quanto aos riscos de violação da sua privacidade comparativamente nas diversas regiões do País ou por classes sociais, ou até mesmo com o perfil dos consumidores destas tecnologias de outros países.

Por fim, na perspectiva social, de segurança e de mobilidade urbana pode-se avaliar se, de fato a conectividade em veículos será capaz de melhorar o trânsito nas cidades ou qual o impacto destas tecnologias para o transporte público. Em outra linha de pesquisa, pode-se avaliar a contribuição do uso destas tecnologias para o aumento da segurança veicular, para a redução de consumo de combustíveis e da poluição e para a redução dos acidentes e mortes no trânsito.

REFERÊNCIAS

Ajis, A. F. Md. & Baharin, S. H. (2019). Dark Data Management as frontier of Information Governance. *2019 IEEE 9th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Malaysia, pp. 34-37. doi: 10.1109/ISCAIE.2019.8743915

Baloyi, N. & Kotzé, P. (2019). Guidelines for Data Provocay Compliance: A Focus on Cyber-physical Systems and Internet of Things. *In Proceedings of ACM SAICSIT conference (SAICSIT'19), ACM*. 10 pages. https://doi.org/10.1145/3351108.3351143

Bamberger, K. A. & Mulligan, D. K. (2011). New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry. *Law & Policy*, 33, pp. 477-508. https://doi.org/10.1111/j.1467-9930.2011.00351.x

Borgman, H., Heier, H., Bahli, B. & Boekamp, T. (2016). Dotting the I and Crossing (out) the T in IT Governance: New Challenges for Information Governance. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, pp. 4901-4909. doi: 10.1109/HICSS.2016.608.

Briefings on HIPPA (2017). A privacy and information security governance model. *Briefings on HIPAA Gale Academic OneFile*, vol. 17, no. 6. Recuperado a partir de https://link.gale.com/apps/doc/A495551361/AONE?u=capes&sid=AONE&xid=4793074f.

Cavoukian, A. (2011). Privacy by Design - The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Recuperado a partir de www.ipc.on.ca/images/Resources/gps.pdf

Cha, S., Hsu, T., Xiang, Y. & Yeh, K. (2019). Privacy Enhancing Technologies in the Internet of Things: Perspectives and Challenges. *in IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2159-2187. doi: 10.1109/JIOT.2018.2878658.

Conrad, S. S. (2019). Protecting Personal Information and Data Privacy - What Students Need to Know. *Journal of Computing Sciences in Colleges*, 35(3), pp. 77-86

Coyne, E. M., Coyne, J. G. and Walker, K. B. (2018). Big Data information governance by accountants. *International Journal of Accounting & Information Management*, Vol. 26 No. 1, pp. 153-170. https://doi.org/10.1108/IJAIM-01-2017-0006

Damjanovic-Behrendt, V. (2018). A Digital Twin-based Privacy Enhancement Mechanism for the Automotive Industry. 2*018 International Conference on Intelligent Systems (IS)*, Funchal - Madeira, Portugal, pp. 272-279. doi: 10.1109/IS.2018.8710526.

Fabiano, N. (2017). The Internet of Things ecosystem: The blockchain and privacy issues. The challenge for a global privacy standard. *2017 International Conference on Internet of Things for the Global Community (IoTGC)*, Funchal, pp. 1-7. doi: 10.1109/IoTGC.2017.8008970

Hulme, T. (2012). Information Governance: Sharing the IBM approach. *Business Information Review*, 29(2), 99–104. https://doi.org/10.1177/0266382112449221

Langheinrich M. (2001) Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. *In: Abowd G.D., Brumitt B., Shafer S. (eds) Ubicomp 2001: Ubiquitous Computing. UbiComp 2001. Lecture Notes in Computer Science*, vol 2201. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45427-6_23

Lei nº 13.709 de 14 de agosto de 2018. (2018, 14 agosto). Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília

Li, C. & Palanisamy, B. (2019). Privacy in Internet of Things: From Principles to Technologies. *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 488-505. doi: 10.1109/JIOT.2018.2864168.

Oukemeni, S., Rifà-Pous, H. & Puig, J. M. M. (2019). Privacy Analysis on Microblogging Online Social Networks: A Survey. *ACM Comput. Surv.* 52(3), Article 60 (June 2019), 36 pages. https://doi.org/10.1145/3321481

Sakura, R. & Zuchi, J. D. (2018). As revoluções industriais até a indústria 4.0. *Revista Interface Tecnológica*, 15(2), pp. 480-491. doi: 10.31510/infa.v15i2.386

Silva, A. H. & Fossá, M. I. T. (2013). Análise de conteúdo: exemplo de aplicação da técnica para análise de dados qualitativos. *In Anais, IV Encontro de Ensino e Pesquisa em Administração e Contabilidade*, (pp. 1-14). Brasília. Distrito Federal: EnEpq.

Smith, H., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), 989-1015. doi:10.2307/41409970

Whitman, J. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal*, 113(6), 1151-1221. doi:10.2307/4135723

Yin, R. K. (2005). Estudo de caso: planejamento e métodos (2. ed.). *Porto Alegre: Bookman*.

Zallone, R. (2019). Connected Cars under the GDPR. *AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE)*, pp. 1-6. doi: 10.23919/EETA.2019.8804515

Ziegeldorf, J. H., Morchon, O. G. & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742.