PRODUTO & PRODUÇÃO, vol. 25, n.1, p. 64-84. 2024[*].

Implementação de Lei Geral de Proteção De Dados (LGPD) em uma Concessionária Automotiva

Ramon Siqueira
Instituto Federal de Minas Gerais (IFMG)
e-mail: ramonrsgv@gmail.com

Tatielle Menolli Longhini
Instituto Federal de Minas Gerais (IFMG)
e-mail: tatielle.longhini@gmail.com

[*] RECEBIDO em 07/02/2024. ACEITO em 23/04/2024.

Resumo

O aumento exponencial no volume de dados processados por empresas decorre do crescimento do uso de tecnologias, intensificando a geração de dados sobre os usuários. Em resposta a essa tendência, os países têm movido esforços para estabelecer aparatos legais que regulamentem o tratamento adequado dos dados pessoais. No Brasil, a Lei Geral de Proteção de Dados (LGPD), em vigor desde 2018, delineia as condições para retenção, uso, tratamento e exclusão desses dados. Neste contexto, um estudo foi conduzido em uma concessionária de veículos com mais de duas décadas de dados cadastrados, totalizando mais de 130.000 clientes registrados. Diante disso, a empresa desenvolveu um processo de implementação de proteção de dados em conformidade com os requisitos da LGPD. Para tal, foram elaborados documentos obrigatórios de adequação à legislação, incluindo políticas de privacidade para funcionários, consumidores e parceiros, políticas de execução dos direitos do titular, de cookies, de retenção de dados, além de registro de atividades de tratamento de dados pessoais (data mapping), nomeação do Encarregado de Proteção de Dados (DPO), notificação de violações de dados pessoais e formulário de consentimento para marketing. Futuramente, a empresa também planeja elaborar o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) e documentos de boas práticas após consolidar a implementação do sistema. Este estudo é de suma relevância, especialmente em um momento em que o governo nacional exige o cumprimento integral dos aspectos legais pelas empresas e os consumidores estão cada vez mais conscientes sobre a importância das condutas éticas em relação aos dados sensíveis.

Palavras-Chave: LGPD; dados sensíveis; sociedade da informação.

Abstract

With the advent of technologies, there has been an intensification in the generation of data about users. In response to this trend, countries have been making efforts to establish legal frameworks that regulate the proper handling of personal data. In Brazil, the General Data Protection Regulation (GDPR), in force since 2018, outlines the conditions for the retention, use, processing, and deletion of such data. In this context, a study was conducted at a vehicle dealership with over two decades of registered data, totaling more than 130,000 registered customers. In light of this, the company developed a data protection implementation process in compliance with LGPD requirements. To achieve this, mandatory documents for legal compliance were drafted, including privacy policies for employees, consumers, and partners, policies for the execution of data subjects' rights, cookie policies, data retention policies, as well as records of personal data processing activities (data mapping), appointment of a Data Protection Officer (DPO), notification of personal data breaches, and marketing consent forms. Additionally, the company plans to develop the Personal Data Protection Impact Report (RIPD) and best practice documents after consolidating the implementation of the system. This study is of utmost relevance, particularly at a time when the national government is demanding full compliance with legal aspects from companies, and consumers are becoming increasingly aware of the importance of ethical conduct regarding sensitive data.

Keywords: *LGPD; sensitive data; information society.*

1. Introdução.

O aumento no uso de dados influenciou os rumos que a tecnologia tomou na última década. A vida hoje se encontra *dadificada* em aplicativos *smartphones* e *apps* que facilitam bastante a nossa vida, com um fluxo intenso de dados processados e protegidos por políticas de privacidade. Até algum tempo atrás, questionava-se quais seriam os limites do mercado de aparelhos celulares; porém, com a invenção da *internet* móvel, todas as discussões se diluíram, dando espaço a um universo de possibilidades de aplicação na vida cotidiana das pessoas (BIONI, 2020).

Contudo, é de se esperar que essa mudança tão abrupta no cotidiano humano, proporcionada pelo avanço tecnológico disruptivo, também levantasse discussões quanto aos desdobramentos negativos surgidos no mercado, como o uso dos dados coletados em redes sociais e mecanismos de busca para perfilação e *marketing* direcionado (Lima, 2020). A sociedade da informação, segundo Silveira (2017), desenvolve um mundo em constante melhoria, dado que as empresas têm a oportunidade de aprimorar seus produtos e serviços. Por outro lado, percebe-se que as possibilidades não são tão otimistas assim, onde o uso do perfilamento também pode levar à "indução do comportamento social em uma sociedade articulada pelas redes digitais".

Para Silveira (2017), informação é controle e comando, e quando aborda os fundamentos da cibernética, traz a ideia de que mantemos e reproduzimos relações sociais através de um sitema de controle de informações. Onde os mais diversos dados utilizados diariamente, constituindo a base para organização de sistemas de crédito, estratificação e seleção social. Assim, são mantidos em registros dados sobre dados, onde os dados de comando geram dados de controle (metadados), onde as empresas passam a desempenhar completo sobre a vida dos indivíduos através dos dados sob sua posse.

Diante dessa realidade, os vazamentos de dados também se tornaram comuns. Por isso, a temática tem sido alvo de debates, pois os dados se tornaram bens preciosos. Surge a necessidade de uma intervenção por parte dos governos para garantir direitos fundamentais de seus cidadãos, através das leis de proteção de dados (LIMA, 2020). No Brasil, a lei geral de proteção de dados (LGPD) entrou em vigor em 2018, como um desdobramento da *General Data Protection Regulation* (GDPR) em discussão e desenvolvimento em países na Europa (BRASIL, 2018).

Desde então, as empresas têm se deparado com a dificuldade de implementação, uma vez que a regulamentação exige que sejam definidos procedimentos medidas técnicas para a proteção de dados, o que de marca uma mudança siginificativa na maneira com as empresas devem coletar e tratar os dados pessoais (Silva et al., 2023; Cairas, 2023; Bezerra, Vieira & Nascimento, 2022). Com o avanço da tecnológico, tem-se requisitado a implementação de ferramentas que otimizem processos e elevem a segurança e transparência no uso de dados pessoais (Limberger, 2022)

Segundo Monteiro *et al.* (2019), a legislação define dado pessoal toda a "informação relacionada à pessoa natural identificada ou identificável", que expande o conceito de dado pessoal a toda e qualquer informação originada por, ou atribuída à, pessoa natural. Isso veio a aumentar, entre as empresas, o escopo de aplicação da lei a não somente dados de identificação pessoal, mas a todo e qualquer dado que gere informação relativa a alguém, mesmo que este alguém não esteja identificado.

Sendo assim, as organizações devem adotar práticas de gestão de dados, em confomidade com a LGPD, como forma de evitar punições legais. Passaisso, são nomeados os responsáveis pela implementação de práticas para proteção de dados, bem comodepolíticas e processos de privacidade em todas as fases do negócio (Carvalho, Freitas & Santos, 2022; Cunha, Pinto, Timoteo, Barbosa & Almeida, 2021).

Este trabalho tem como objetivo implementar a lei geral de proteção de dados (LGPD) em uma concessionária automotiva. Trata-se de uma necessidade de se adequar aos requisitos da lei e estar em *compliance*, a concessionária, com várias empresas no ramo de vendas de automóveis, necessita de uma metodologia para fundamentar e reorganizar sua estrutura de processos com base nas exigências legais. Dessa maneira, visa-se responder a seguinte pergunta de pesquisa: "Como implementar a lei geral de proteção de dados (LGPD) em uma concessionária automotiva?".

O presente trabalho se divide em cinco seções. A primeira delas introduz e contextualiza o tema do trabalho, onde foi formulado o problema e justificada a realização do trabalho, bem como os objetivos a serem alcançados. A segunda parte expõe o referencial teórico deste estudo. A terceira parte traz a metodologia utilizada no desenvolvimento desse trabalho. A quarta parte apresenta os resultados do

desenvolvimento. A última parte aborda as considerações finais e os principais resultados alcançados, bem como as recomendações para futuros trabalhos.

2. Referencial teórico.

Neste capítulo, será definido o referencial do trabalho, sendo apresentadas as leis de proteção de dados a história e a criação, aplicação e princípios da LGPD no Brasil.

2.1. Leis de proteção de dados na história.

A Declaração Universal dos Direitos Humanos, desde 1948, já estabelecia em seu artigo 12 que a privacidade dos indivíduos é um direito universal. Monteiro *et al.* (2019), afirma que a privacidade do indivíduo é um direito que se associa com o campo pessoal, garantindo assim a proteção dos ideais e valores da vida individual.

Ainda, segundo este autor, com o avanço da tecnologia da informação nas décadas de 60 e 70, começaram, na Europa, a serem criadas as primeiras leis regulamentando o tratamento de dados pessoais de forma automatizada. Com a primeira lei estadual de garantia da proteção de dados sendo criada em 1970, no estado alemão de Hesse, e no âmbito nacional, com a primeira lei de proteção de dados aprovada em 1973 na Suécia. Ao longo dos anos 70, outros países europeus seguirão essa tendência, com leis ainda bem genéricas, bem distantes das sólidas e estruturadas leis atuais.

No ano de 1981, foi aprovada pelo Conselho da Europa o tratado n° 108, sendo o primeiro ato para proteção de dados que abarcava toda a Europa e seus fluxos de dados transnacionais.

> "Esta Convenção é o primeiro instrumento internacional vinculativo que protege o indivíduo contra abusos que podem acompanhar a recolha e tratamento de dados pessoais e que visa regular ao mesmo tempo o fluxo transfronteiriço de dados pessoais. Além de fornecer garantias em relação à coleta e processamento de dados pessoais, ele proíbe o processamento de dados "sensíveis" sobre a raça, política, saúde, religião, vida sexual, antecedentes criminais, etc. de uma pessoa, na ausência de salvaguardas legais. A Convenção também consagra o direito do indivíduo de saber que as informações sobre ele armazenadas e, se necessário, de fazer com que sejam corrigidas" (COUNCIL OF EUROPE, 1985).

Segundo Monteiro *et al.* (2019), o tratado 108 serviu de base para a Diretiva 95/46/CE8 em 1995, que vigorou "até maio de 2018, quando foi substituída pelo Regulamento n° 2016/679, de 27 abril de 2016, popularmente conhecido como General Data Protection Regulation (GDPR), a nova lei geral de proteção de dados da União Europeia".

Enquanto a Europa se estruturava diante do novo cenário introduzido pelas transformações tecnológicas, o Brasil permanecia incauto quanto a essa questão, detendo, segundo Lima (2020), algumas leis que abordam a proteção da privacidade dos cidadãos e seus dados pessoais, como a Constituição Federal de 1988, o Código de Defesa do Consumidor de 1990, o Código Civil de 2002, a Lei do Cadastro Positivo de 2011, o Marco Civil da Internet de 2014, entre outras legislações que não são específicas para o assunto.

De acordo com Garcia *et al.* (2020), a privacidade abordada nas leis citadas, não é a mesma que a proteção de dados pessoais, tendo este um escopo muito mais amplo, fez surgir em agosto de 2018 a lei que abordasse tal escopo de forma específica. Com alterações pela Medida Provisória 869/2018 e pela Lei n. 13.853/2019, nasce a Lei Geral de Proteção de Dados (LGPD), inovando "ao criar sanções direcionadas, além de uma governança que inclui um novo órgão da presidência da República", fazendo com que qualquer empresa, organização, instituição pública ou privada que coleta ou que utiliza dados de pessoas físicas se adaptassem a ela.

2.2. Criação, aplicação e princípios da Lei Geral de Proteção de Dados (LGDP) no Brasil.

No ano de 2018 entrou em vigor na Europa a mais completa legislação de proteção de dados do mundo, a GDPR. Esta legislação foi uma evolução da Diretiva 95/46/EC, fruto de um longo processo de criação desde as primeiras leis que abordavam a proteção de dados na década de 70. Seu escopo de aplicação inclui como deve ser a utilização de dados pessoais naturais localizados tanto na União Europeia, como em outros países ao redor do mundo (MONTEIRO, et al, 2019). Tendo em vista a

criação da GDPR, o Brasil visou regulamentação parecida, pois o país também seria afetado pela transferência internacional de dados, sendo que a lei envolvia o relacionamento comercial dos países da União Europeia com estrangeiros (PANEK, 2019).

Outros fatores contribuíram para que o Brasil formulasse uma legislação que abordasse a proteção dos dados. Por ser signatário de alguns acordos internacionais que já possuem considerações, sobre a proteção de dados pessoais, como a Convenção de Berna de 1886 e o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual relacionados ao Comércio e o anseio pela entrada na OCDE - Organização para a Cooperação e Desenvolvimento Econômico (PANEK, 2019).

Diante disso, o Brasil aprovou em 14 de agosto de 2018 a Lei Geral de Proteção de Dados (LGPD). A Lei nº 13.709, que trata da proteção dos dados no Brasil, estabelece em seu artigo 1°:

> Art. 1 °. A lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Neste sentido, a lei é aplicável à pessoa física ou jurídica que armazene e trate bases de dados com fins econômicos; dados coletados e/ou tratados dentro do território nacional, independentemente do meio aplicado; e dados usados para fornecimento de bens ou serviços (PANEK, 2019).

Já o artigo 2º apresenta os fundamentos da LGPD que, segundo Garcia *et al*. (2020), devem preceder a qualquer interpretação e aplicação da lei, abordando a privacidade do indivíduo como um objetivo fundamental na sociedade, mas que não deve se sobrepor ao interesse coletivo de desenvolvimento e progresso. Sendo estes:

> "I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - à inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais." (BRASIL, 2018).

Definidas as exclusões de aplicação da lei, todo o restante se enquadra em seu escopo, dessa forma é apresentado então os dez princípios a serem observados antes do tratamento de um dado pessoal. De acordo com a LGPD, os princípios de aplicação da mesma são:

> I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X – Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Ressalta-se que a LGPD não se aplica para fins jornalísticos e artísticos, de segurança pública, de defesa nacional, de segurança do Estado, de investigação e repressão de infrações penais, e para o

uso particular, sem interesses econômicos envolvidos. Ao longo de todo o primeiro capítulo, é bem definido o escopo da lei, trazendo clareza sobre todas as partes envolvidas ou não.

De acordo com Silva (2021), a gestão de dados colhidos e usados passam a ter processos de manuseio mais rigorosos e transparentes quanto ao tratamento, armazenagem e descarte, sendo que as empresas que não cumprirem tais passos, estarão sujeitas a penalidades e sanções. Estas são aplicadas Autoridade Nacional de Proteção de Dados (ANPD), responsável pela fiscalização, rientação e aplicação de notificações, sendo que as multas variam de acordo com o nível de descumprimento e inconformidade com a lei (NASCIMENTO, 2018).

3. Metodologia.

A metodologia de um estudo visa desdobrar os passos de análise e compreensão de diferentes técnicas e métodos com a finalidade de coletar dados e processar informações de determinado assunto. A finalidade é resolver problemas a partir de uma lógica devidamente fundamentada. Esta seção apresentará os passos formais e aplicados para a realização do presente trabalho.

A metologia de pesquisa estabelece o caminho para abordagem e estudo realidade em análise frente às concepções teóricas que as refletem (MINAYO, 2001). O presente estudo se configura como uma pesquisa aplicada que, segundo Fonseca (2002), visa o desenvolvimento de conhecimento a partir de uma aplicação prática, voltada a problemas específicos. Exatamente o que se propõe neste trabalho, onde requisitos da LGPD serão atendidos pela empresa em estudo.

A natureza do estudo é qualitativa, uma vez que se aborda uam realidade não quantificada, baseada em significados e motivos, bem como no entendimento de processos e fenômenos sociais (MINAYO, 2001). Para isso, nesta pesquisa, foram levantadas informações por observação direta e participante. Quanto ao objetivo, este tranalho se configura pelo seu caráter descritivo, uma vez que busca a descrição do fenômeno, possibilitando o conehcimento e interpretação da realidade em análise (GIL, 2007; TRIVIÑOS, 1987). Para o caso específico, foram descritos os passos e adequações que a empresa passou a adotar em atendimento às prescrições da LGPD.

O objeto é um estudo de caso em que, segundo Gil (2007) e Yin (2001), visa o entendimento profundo de um ou poucos objetos para compreensão detalhada da sua configuração. No presente trabalho, estudo de caso foi realizado em um grupo de empresas concessionárias, que necessitam aplicar os aspectos da LGPD em seus processos. Finalmente, os dados do trabalho foram coletados por observação direta, observação participante, estudos de relatórios e pesquisa-ação. Estes permitem a descrição do fenômento em análise e, por sua vez, uma investigação social mediante embasamento empírico e ação dos demais participantes, com relação direta entre a ação do pesquisa e a resolução do problema (FONSECA, 2002; THIOLLENT, 1988). O desevolvimento do estudo foi realizado em 2020, a partir da participação direta do responsável pela implementação das etapas exigidas pela lgpd. para isso, foram desenvolvidos, com participação direta de setores envolvidos no processo, os documentos referentes a: (1) política de privacidade para funcionários, (2) política de privacidade para consumidores e parceiros, (3) política de execução dos direitos do titular, (4) política de cookies, (5) política de retenção de dados, (6) registro de atividades de tratamento de dados pessoais (data mapping), (7) carta nomeação do data protection officer (dpo), (8) notificação de violação de dados pessoais, (9) formulário de consentimento para marketing.

Com isso, os aspectos de direitos aos consumidos e titulares dos dados serão resguardados, conforme indicados pela LGPD (CUNHA *et al.*, 2021). Assim, serão mantidos: (i) confirmação de existência de tratamento; (ii) acesso aos dados; (iii) correção dos dados; (vi) anonimização, bloqueio ou eliminação de dados; (v) portabilidade dos dados; (vi) eliminação dos dados tratados com consentimento; (vii) informações sobre o compartilhamento de dados; (viii) informação sobre a possibilidade de não fornecer consentimento; (ix) revogação do consentimento.

4. Resultados e discussões.

A organizaçao em estudo é um grupo de empresas localizadas nos estados de Minas Gerais e Espírito Santo, com seis empresas somando dezesseis concessionárias de veículos, contando com cerca de quatrocentos colaboradores. Seu principal ramo de atividade é a venda de veículos, novos e semi-

novos multimarcas, mas trabalha também com a venda de peças e acessórios automotivos, fisicamente e pela internet, prestação de serviços de oficina, e locação de veículos. Atualmente, o Grupo conta em seu banco de dados principal com cerca de cento e trinta mil clientes cadastrados, entre pessoas físicas e pessoas jurídicas, contando com pelo menos sete bases de dados digitais para a área comercial. São quase 20 anos de dados cadastrados e acumulados.

A LGPD consiste no tratamento de dados pessoais. Nesse contexto, todas as empresas que tratam e armazenam esse tipo de dados, precisa se adequar aos novos moldes legais. A concessionária possui dados de funcionários e de clientes do tipo pessoa física, sendo que o volume de clientes, colaboradores e bases de dados existentes é significativo, e a complexidade e o risco de gerenciá-los aumentam proporcionalmente com o crescimento destas três variáveis. O fato da empresa representar importantes marcas de veículos no Brasil, também foi uma justificativa a mais para acelerar o processo de implementação. Houve a necessidade dada a representatividade das marcas e pelo volume de clientes e dados processados. Para que a empresa se adeque às condições de tratamento, uso e descarte de dados pessoais, conforme prescrito por Brasil (2018), elaborou-se dez documentos listados no Quadro 1.

Quadro 1 - Documentos desenvolvidos.

Documento	**Informações mantidas**
1 POLÍTICA DE PRIVACIDADE PARA FUNCIONÁRIOS	1. Objetivo 2. Dados Pessoais 3. Dados pessoais sensíveis 4. Compartilhar e transferir dados pessoais 5. Consentimento 6. Direitos de acesso, retificação, cancelamento e oposição 7. Revogação do consentimento para processamento de dados pessoais 8. Modificações no aviso de privacidade 9. Tratamento inadequado de seus dados 10. Validade e gestão do documento
2 POLÍTICA DE PRIVACIDADE PARA CONSUMIDORES E PARCEIROS	1. Quem somos 2. Informações que coletamos a. Tipos de cookies que coletamos em nossos sites eletrônicos 3. Política de cookies 4. Como usamos seus dados pessoais 5. Seus direitos a. Medidas de salvaguarda b. Transferências internacionais 7. Consequências de não fornecer seus dados a. Interesses legítimos 8. Por quanto tempo mantemos seus dados a. Dados sensíveis 9. Consentimentos para marketing 10. Isenção de responsabilidades 11. Direito de fazer uma reclamação a. Alterações deste aviso de privacidade
3 POLÍTICA DE EXECUÇÃO DOS DIREITOS DO TITULAR	1. Entenda o papel da organização dentro de uma determinada atividade de tratamento 2. Verifique a identidade do titular. 3. Torne o procedimento gratuito. 4. Tempo de Resposta. 5. Obs.: os prazos podem vir a ser regulamentados setorialmente, por autoridade nacional. 6. Impossibilidade de Atender a Requisição 7. Fluxo de cumprimento/recusa à solicitação 8. Informe outros Agentes 9. Evidências
POLÍTICA DE *COOKIES*	O que são e as finalidades de uso.

POLÍTICA DE RETENÇÃO DE DADOS	1. Finalidade, âmbito e destinatários 2. Regras de retenção 3. Princípio geral da retenção 4. Programa gera da retenção 5. Backup dos dados durante o período de retenção 6. Destruição dos dados 7. Violação, execução e conformidade 8. Calendarização da rotina de destruição 9. Método de destruição 10. Anexo
REGISTRO DE ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS (DATA MAPPING)	1. Identificação dos serviços / processo de negócio de tratamento de dados pessoais 2. Agentes de Tratamento e Encarregado 3. Fases do Ciclo de Vida do Tratamento Dados Pessoais 4. De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados 5. Escopo e Natureza dos Dados Pessoais 6. Finalidade do Tratamento de Dados Pessoais 7. Categoria de Dados Pessoais 8. Categorias de Dados Pessoais Sensíveis 9. Frequência e totalização das categorias de dados pessoais tratados 10. Categorias dos titulares de dados pessoais 11. Compartilhamento de Dados Pessoais 12. Medidas de Segurança/Privacidade 13. Transferência Internacional de Dados Pessoais 14. Contrato (s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio
CARTA NOMEAÇÃO DO DATA PROTECTION OFFICER (DPO)	Modelo de documento a ser preenchido.
NOTIFICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS	Modelo de documento a ser preenchido.
FORMULÁRIO DE CONSENTIMENTO PARA *MARKETING*	Modelo de documento a ser preenchido.

Fonte: autoria própria (2024).

Houve a prestação de serviço de consultoria de implementação da LGPD por uma empresa terceira. Para a concessionára se adequar à lei, foi feito um mapeamento dos processos, sendo que as estruturas foram mudadas continuamente para se adequar às exigências. Também foram definidas atividades e conteúdos recomendados nos padrões de boas práticas na implantação dos programas de adequação à LGPD (Figura 1).

14 ETAPAS DE IMPLANTAÇÃO	REALIZAÇÃO	OBJETIVO > ENTREGA
Definição do grupo de trabalho (*)	o	ficha com definição e dados de titular/diretor - gerentes - DPO
Medição da aderência atual à LGPD	o	mapa de avaliação geral de sistemas e processos atuais
Mapeamento de todos os dados relacionados à pessoa natural	o	mapa com sistemas e locais de arquivos avulsos
Mapeamento dos processos atuais de coleta de dados	o	fluxogramas das áreas críticas
Avaliação da necessidade de tratamento do agente	o	roteiro de providências para o DPO
Revisões contratuais em âmbito geral	o	modelos documentação e contratual
Eliminação de riscos desnecessário (*)	o	roteiro de providências para o DPO
Cadeia de custódia dos dados	o	mapa com especificação da segurança para o DPO
Mecanismos de interação com o titular (*)	o	roteiro para a produção e/ou adoção da aplicação de consentimento
Plano de contingência para o caso de incidente	o	roteiro com recomendações para o DPO
Plano de manutenção da conformidade	o	indicação de treinamentos para o DPO
Designação do encarregado (DPO) (*)	o	indicação para definições de vínculo ou contratação
Contratação do Cyber seguro	o	indicações para DPO
Engajamento público interno e parceiros	o	apresentação engajamento equipes - roteiro de tarefas
EMERGENCIAL INDICADO COM (*)		

Figura 1 - Etapas de implementação e relação entre objetivos e entregas. Fonte: autoria própria (2024).

Foram desenvolvidos referenciais e modelos básicos de boas práticas, de modo que a empresa viesse a apresentar a documentação de adequação à lei geral de proteção de dados. A adequação inclui a obrigatoriedade de elaboração, manutenção e revisão de documentos. Destaca-se o conceito

"*accountability* ", que é a conduta e obrigação em prestar contas de forma transparente – art. 6, incisos VI e X da LGPD. A empresa visa o desenvolvimento de sistema de documentação eficiente que poderá fundamentar melhor eventuais defesas processuais futuras, e forma o que se denomina de provas pré-constituídas. As documentações (Figura 2) deverão ser revistas e atualizadas regularmente para atender a dinâmica das atividades e alterações na lei. O *Data Protection Officer* (DPO) e o controlador devem se reportar às exigências presentes na legislação.

DOCUMENTOS DE ADEQUAÇÃO À LGPD	
Documentos obrigatórios = 12	
DOC 01 - Política de Privacidade para funcionários-V1	• Art. 46 LGPD
DOC 02 - Política de Privacidade Consumidor e Parceiros-V1	• Art. 9 LGPD
DOC 03 - Política de Execução dos Direitos do Titular-V1	• Art. 9 LGPD
DOC 04 - Política de cookies (inserida na política pública de privacidade)	inserida no DOOC 1
DOC 05 - Política de Retenção de Dados-V1	Arts. 6/II/III/IV, 9/II, 40
DOC 06 -Registros das Atividades de Tratamento (ROPA)	• Art. 37 LGPD
DOC 07 - Carta de nomeação DPO-V1	• Art. 41 LGPD
DOC 08 - Notificação de Violação de Dados Pessoais (controlador-autoridade)-V1	• Art. 48 LGPD
DOC 09 - Formulário de Consentimentos para Marketing-V1	• Arts. 7/I, 8, 11/I, 14 LGPD
Documentos importantes em situações específicas = 1	
Política para RIPD, incluindo modelo	• Arts. 10/§ 3º, 38
Documentos de Boas Práticas = 4 (não inclusos)	
Cláusulas em contratos com operadores e com terceiros (incluindo transferências internacionais)	• Arts. 33, 34, 35, 39, 42, 44,45
Política de violação de dados pessoais	• Art. 50/§ 2º/g
Notificação de violação de dados (operador para controlador)	
Registro de violação de dados pessoais	
	ago/21

Figura 2 - Grade de documentos de adequação à LGPD. Fonte: autoria própria (2024).

Os próximos subtópicos desdobrarão o conteúdo dos documentos elaborados pela empresa, em resposta às exigências da LGPD: 1. Política de privacidade para funcionários; 2. Política de privacidade para consumidores e parceiros; 3. Política de execução dos direitos do titular; 4. Política de *cookies*; 5. Política de retenção de dados; 6. Registro de atividades de tratamento de dados pessoais (*data mapping*); 7. Carta de nomeação do *Data Protection Officer* (DPO); 8. Notificação de violação de dados pessoais; 9. Formulário de consentimento para *marketing*.

4.1. Política de privacidade para funcionários.

A política objetiva manter os dados pessoais do titular, recolhidos pela empresa. Os mesmos são tratados e protegidos sob estrita confidencialidade pela EMPRESA CONTROLADORA e utilizados para avaliação e participação em processos de recrutamento e seleção, fornecer treinamento, cumprir obrigações contratuais, cumprir obrigações em matéria trabalhista, previdenciária, tramitar seguro saúde (se aplicável ao cargo), seguro de vida (se aplicável ao cargo), solicitar referências e cadastro de vínculo, cadastrar funcionários nos sistemas internos e acompanhar obrigações contratuais. Os mesmos não são mantidos em caso de indicação contrária do titular através dos meios descritos neste Aviso de Privacidade.

Os dados pessoais recolhidos são de identificação, contato, situação laboral, condição acadêmica, evoluções patrimoniais e características físicas dos colaboradores. São classificados como dados sensíveis aqueles relacionados com a saúde dos funcionários. A base legal de tratamento se dá com a execução de contrato e, em alguns casos, por consentimento.

Definiu-se que os dados pessoais podem ser compartilhados e/ou transferidos e processados por pessoas físicas e/ou jurídicas que não a EMPRESA CONTROLADORA. Neste sentido, as informações podem ser compartilhadas com (i) seguradoras com as quais o colaborador mantém relacionamento jurídico; (ii) assessores jurídicos, contábeis e administrativos externos e auditores; (iii) algum tipo de *software* e qualquer infraestrutura de computador que sirva para manter seus dados atualizados e protegidos; (iv) fornecedores que salvaguardam documentos e informações em arquivos eletrônicos e impressos; (v) instituições bancárias (vi) prestadores de serviços jurídicos para defender a EMPRESA CONTROLADORA de qualquer controvérsia jurídica que possa surgir. A EMPRESA

CONTROLADORA tomará medidas para que terceiros que recebam dados pessoais sigam o cumprimento deste aviso de privacidade.

No caso de não se obter uma oposição contrária expressa do colaborador, a empresa entende que o mesmo foi devidamente informado, e que entendeu que as bases legais de tratamento dos seus dados pessoais está na execução de contrato de trabalho, sendo que em alguns casos específicos a base será o CONSENTIMENTO. Em caso de não autorização de compartilhamento de dados pessoais com terceiros, o funcionário deve escrever por conta própria as entidades para as quais não deseja que seus dados pessoais sejam transferidos. O funcionário tem o direito de saber quais dados pessoais a empresa possui, para o quê são usados e as condições de uso feitas. Da mesma forma, é direito do colaborador:

- solicitar a correção de seus dados pessoais se estiverem desatualizados, inexatos ou incompletos (Retificação);
- a eliminação dos nossos registos ou bases de dados quando se considerar que não está a ser utilizado de acordo com os princípios, deveres e obrigações previstos na regulamentação (Cancelamento);
- opor-se à utilização dos seus dados pessoais para fins específicos (Oposição). Basta que enviem um e-mail para [inserir e-mail de contato do responsável pelos dados pessoais], explicando o que deseja.

Diante de tais manifestações, a EMPRESA CONTROLADORA deverá entrar em contato com os colaboradores que se opuserem, no prazo máximo de dois dias úteis (48 horas), contados a partir da data da recepção do pedido de acesso, retificação, cancelamento ou oposição, para o informar decisão adotada. Além disso, a qualquer momento, o colaborador pode revogar o consentimento dado para o processamento de seus dados pessoais, para que deixem de ser usados. Para tal, é necessário que submeta o seu pedido por escrito, para o *e-mail* de contato do encarregado pelo dados pessoais da empresa. No entanto, é importante que tenha em atenção que nem em todos os casos poderão ser respondidos ou encerrar imediatamente a utilização, pois é possível que devido a alguma obrigação legal a emrpesa tenha de continuar a tratar os seus dados pessoais (consultar tabela de retenção de dados pessoais com o setor de Recursos Humanos). No prazo máximo de dois dias úteis (48 horas) o pedido é retornado.

A empresa se reserva ao direito de fazer modificações ou atualizações ao Aviso de Privacidade a qualquer momento, para atender a nova legislação, políticas internas ou novos requisitos para o fornecimento ou oferta de nossos serviços. Ass modificações estarão disponíveis nos seguintes meios:

- Anúncios visíveis na empresa;
- No site da empresa, seção Aviso de Privacidade;
- Ou enviará para o último e-mail fornecido.

Caso o colaborador considere que o seu direito à proteção dos dados pessoais foi prejudicado por qualquer conduta da EMPRESA CONTROLADORA, ou por suas ações ou respostas, presume-se que no processamento de seus dados pessoais houve alguma violação das disposições da Lei Federal sobre Proteção de Dados Pessoais na Posse de Pessoas Físicas, poderá apresentar a respectiva reclamação ou reclamação junto do Autoridade Nacional de Proteção de Dados (ANPD).

4.2. Política de privacidade para consumidores e parceiros.

A EMPRESA CONTROLADORA trata as informações pessoais para cumprir suas obrigações legais contratuais e fornecer-lhe nossos produtos e serviços. Nunca são coletados dados pessoais desnecessários e não são tratadas informações de quaisquer outras formas que não as especificadas nesta Politica. Os dados pessoais de identificação coletados são, entre pessoas físicas: nome; data de nascimento; endereço; *e-mails*; número do Cadastro de Pessoa Física (CPF) e Registro Geral (RG); número de telefones; número da carteira de motorista. As informações são coletadas por:

- Uso de *cookies* em *websites* e aplicativos;
- Ferramentas de redes sociais como *WhatsApp, Facebook e Google*;
- Formulários eletrônicos em nossos *sites* e aplicativos;
- Formulários impressos em nossa loja física;
- Formulários eletrônicos com Ordem de Compra, Ordem de Serviços e Notas Fiscais;
- Sistemas de gestão de dados e operações da Concessionária, como sistema DMS (gestão da operação do concessionário) e sistema CRM (gestão dos relacionamentos e jornadas de compra e uso dos nossos produtos);

- Formulário para Currículos e informações de emprego;
- Câmeras de segurança em nossas lojas captam imagens do trânsito de pessoas.

Os consumidores e parceiros têm o direito de acessar qualquer informação pessoal que a empresa trata a seu respeito, e pode também solicitar informações sobre:

- Quais dados pessoais mantidos;
- As finalidades do tratamento;
- As categorias de dados pessoais em causa;
- Os destinatários a quem os dados pessoais foram/serão divulgados;
- Quanto tempo a empresa pretende armazenar os dados pessoais;
- Se não os dados não são coletados diretamente do usuário, o mesmo terá informações sobre a fonte.

Caso o cliente acredite que há dados incompletos ou imprecisos sobre ele, o mesmo tem o direito de solicitar correção e/ou preenchimento das informações, o mais rapidamente possível, a menos que haja uma razão válida para não fazê-lo - caso ocorra, o usuário é devidamente notificado. Os consumidores e parceiros têm o direito de solicitar a exclusão dos dados pessoais ou de restringir o tratamento (quando aplicável) de acordo com a legislação de proteção de dados, bem como o direito de se opor a qualquer *marketing* direto (*e-mails*, mensagens eletrônicas, dentre outros). Quando aplicável, há o direito à portabilidade de dados de suas informações e o direito de ser informado sobre qualquer tomada de decisão automatizada que pode ser usada.

Os dados pessoais não são compartilhados ou divulgados sem o devido consentimento, exceto para os fins especificados neste Aviso ou quando houver uma exigência legal. A Empresa Controladora usa como parceiros Google, Facebook, WhatsApp, Linkedin, Agência de Propaganda e Agências e sistemas de CRM para fornecer os serviços abaixo indicados, cumprindo integralmente o Aviso de Privacidade da empresa, bem como as legislações de proteção de dados e quaisquer outras medidas de confidencialidade e segurança apropriadas:

- Google – publicidade e buscas dos produtos e serviços;
- Facebook – publicidade e buscas dos produtos e serviços;
- Portais de Automóveis – publicidade e buscas dos nossos produtos e serviços.
- Portais de Serviços – publicidade e buscas dos produtos e serviços;
- Whatsapp – atendimento e prestação de serviços diversos;
- LinkedIn – processos de busca e seleção de candidatos para serem nossos colaboradores e divulgação da marca e dos produtos;
- Agência Propaganda – tratamento de dados pessoais para analíticos, planos de comunicação e ações de marca, vendas e serviços;
- Agência CRM – tratamento de dados pessoais para analíticos, planos de comunicação e ações de marca, vendas e serviços;
- Sistemas de operação e CRM – tratamento de dados pessoais para analíticos, planos de comunicação e ações de marca, vendas e serviços.

Alguns produtos ou serviços (ou parte deles) da empresa estão hospedados em servidores localizados nos Estados Unidos da América e Reino Unido. O que significa que há a possibilidade de transferência de qualquer informação do consumidor para fora do território brasileiro para as finalidades de Google, Facebook, Portais de Automóveis, Portais de Serviços, WhatsApp, LinkedIn e Sistemas de Operação e CRM. As coletas de dados são sempre minimizadas, de modo a pseudonimizar ou anonimizar. Há uma conduta contra acesso não autorizado, alteração acidental ou ilícita, divulgação ou destruição de seus dados pessoais, e temos várias camadas de medidas de segurança em vigor, como acesso restrito, SSL, TLS, criptografia, pseudonimização, acesso restrito, autenticação de dois fatores, *firewalls*, antivírus/*malware*.

Cabe ressaltar que os usuários não são obrigados a fornecer os dados pessoais. No entanto, como essas informações são necessárias para o fornecimento de serviços e produtos, a empresa pode não ser capaz de oferecer alguns/todos os serviços e produtos.

Os dados pessoais são mantidos apenas pelo tempo que for necessário para que as finalidades da empresa sejam atingidas (pesquisa de compra de produtos e serviços, contratos de compra de produtos

e suporte de assistência técnica). Para isso, há rigorosas políticas de revisão e retenção em vigor para cumprir essas obrigações. A lei tributária do Brasil obriga a manutneção dos dados pessoais básicos (nome, endereço, detalhes de contato e do contrato) por um mínimo de cinco anos, em garantia, e permanente nos registros fiscais, sendo que após tais períodos os dados serão apagados e/ou mantidos.

Embora a empresa adote elevados padrões de segurança, a fim de evitar incidentes, não há nenhuma página virtual inteiramente livre de riscos. Nesse sentido, a empresa não se responsabiliza por:

- Quaisquer consequências decorrentes da negligência, imprudência ou imperícia dos TITULARES em relação a seus dados individuais. Há a garantia e responsabilização da empresa apenas pela segurança dos processos de tratamento de dados e do cumprimento das finalidades descritas no presente instrumento;
- Ações maliciosas de terceiros, como ataques de *hackers*, exceto se comprovada conduta culposa ou deliberada da nossa Empresa Controladora;
- Inveracidade das informações inseridas pelo usuário/cliente nos registros necessários para a utilização dos nossos serviços; a empresa sempre atuacom medidas para coletar e armazenar os dados pessoais com qualidade e atualizados. Caso, mesmo assim, ocorra erro ou má fé de parte do cliente, quaisquer consequências decorrentes de informações falsas ou inseridas de má fé são de inteiramente responsabilidade do usuário/cliente.

A EMPRESA CONTROLADORA apenas trata os dados pessoais em conformidade com este Aviso de Privacidade e de acordo com a legislação de proteção de dados relevante. Se, no entanto, o usuário/cliente deseja fazer uma reclamação sobre nossas atividades de tratamento em relação aos seus dados pessoais ou estiver insatisfeito com a forma como lidamos com suas informações, há o direito de apresentar uma reclamação à autoridade de controle responsável.

A empresa se reserva ao direito de modificar esse Aviso de Privacidade a qualquer tempo, principalmente em função da adequação a eventuais alterações feitas no *site* ou em âmbito legislativo. Eventuais alterações entraram em vigor a partir de sua publicação no *site*. Ao utilizar nossos serviços e fornecer seus dados pessoais após tais modificações, o usuário/cliente consente.

4.3. Política de execução dos direitos do titular de dados pessoais.

Para atender os direitos dos titulares de dados regulamentados através da Lei 13.709, que trata da Proteção de Dados Pessoais, a empresa considera:

- A função da Concessionária no processamento de uma atividade de tratamento;
- Confirmação de identidade do titular requisitante, devendo ser representante legal atestado por processo interno de verificação e confirmação de identidade;
- Tempo de Resposta à requisição do titular devendo ser imediata (em até 48h), se o acesso for simplicado, ou em até 15 dias, caso a declaração seja completa;
- Impedimentos para que a requisição do titular seja atendida, principalmente em situações que são aplicados princípios de razoabilidade e proporcionalidade do requerimento quanto ao esforço demandado e também deve-se considerar obrigações legais setoriais, sindicais e associativas que influenciam no tratamento de dados realizado;
- A distribuição da requisição para agentes e operadores, de modo que os agentes de tratamento repliquem a requisição para todos os controladores e operadores com que compartilha aqueles dados;
- Evidências dos procedimentos, atitudes e processos da Concessionária são mantidas como provas pré-constituídas fundamentais para demonstrar à ANPD em situações de auditoria ou intimação. Assim, deverão ser armazenados e prontos para disponibilização e consulta, todo e qualquer histórico que trate das requisições dos titulares (e também de todas as atividades da Concessionária ligadas à LGPD) como e-mails, correspondências mensagens trocadas ou outras, registros dos processos para atender ao titular e das análises e motivos de divisão no atendimento ou na impossibilidade.

Tipos de direitos dos titulares e respectivas respostas

Os titulares têm direito à: Confirmação de existência do tratamento; Acesso; Correção de dados incompletos, inexatos ou desatualizados; Anonimização, bloqueio ou eliminação de dados desnecessários; Eliminação de dados pessoais tratados com base no consentimento; Portabilidade de dados a outro fornecedor de serviço ou produto; Revisão das decisões automatizadas. Os direitos e as

respostas encontram-se no Quadro 2.

Quadro 2 - Direitos dos titulares e as respectivas respostas.

Direito	Respostas
Confirmação de existência do tratamento	Confirmar se a Concessionária trata ou não os dados daquele titular, sendo que o prazo de resposta deve ser em até 48 horas para relatórios simplificados e até 15 dias corridos para relatórios de dados completos. As respostas e confirmações da concessionária devem ser encaminhadas pode forma segura e comprobatória, lembrando que cabe ao titular definir o formato do arquivo que receberá.
Acesso	É o direito dos titulares de obter cópias de seus dados pessoais e informações sobre si. A resposta deve ser imediata ou no máximo em 15 dias corridos e as informações somente podem ser fornecidas com a devida confirmação da identidade do titular. É fundamental guardar o histórico para comprovação dos fatos. A confirmação pode ser por qualquer canal, ou na preferência do titular, sendo que as informações devem ser objetivas adequadas e ostensivas.
Correção de dados incompletos, inexatos ou desatualizados	Deve-se considerar uma prioridade nas ações requisitadas pelo titular, como por exemplo, dados sensíveis, dados de perfil comportamental, decisões automatizadas de sistemas. Em situações assim é recomendável interromper imediatamente o tratamento dos dados do titular requerente. E informar a operadores ou co-controladores para que executem as mesmas ações de mitigação. É tarefa do titular a correção ou atualização de seus dados pessoais.
Anonimização, bloqueio ou eliminação de dados desnecessários	A base de dados de leads e clientes da concessionária deve ser mapeada e os registros classificados em grupos que considerem: dados com bases legais (dados válidos ativos e inativos e dados caducos) e dados sem bases legais (dados ativos e inativos). As ações devem ser objetivas no gerenciamento do ciclo de retenção dos dados, conforme grupos acima indicados, com registros de eliminações, anonimizações ou bloqueio (considerar também os processos de backup). Todos os co-controladores e operadores devem ser comunicados para que executem as ações requisitadas, lembrando que os mapeamentos dos tratamentos que as empresas devem executar, será a referência para estas ações.
Eliminação de dados pessoais tratados com base no consentimento	O direito ao esquecimento é uma prerrogativa da LGPD para os titulares de dados. Assim, um titular mesmo fornecendo consentimento pode solicitar que seus dados sejam excluídos a qualquer tempo e hora que solicitar, em exceção a situações que sejam regidas por leis setoriais, federais, estaduais que exijam a guarda de dados por determinado período.
Portabilidade de dados a outro fornecedor de serviço ou produto	É o direito do titular de receber seus dados em formato eletrônico que permita guardar ou transferir para outro controlador. A Concessionária deve preparar seus sistemas para exportação de dados em formatos CSV, TXT, XML e JSON, de modo a poder executar a portabilidade.
Revisão de decisões automatizadas	Qualquer decisão automatizada de sistemas integrados, o que facilita processos e reduz esforços da Concessionária, deve ser revista. O titular deve ser informado com antecedência da automação de decisões, por exemplo, de compartilhamento de seus dados ou outras empresas.

Fonte: autoria própria (2024).

Esta política se baseia nas boas práticas e nas empresas que são referências na prática da LGPD. O texto pode ser distribuído internamente, ou ser utilizado para elaboração de guias ou cartilhas para as equipes e funcionários da concessionária. É também um documento importante para fortalecer e demonstrar as iniciativas e esforços da Concessionária na implantação e implementação da Lei Geral de Proteção de Dados Pessoais.

4.4. Política de *cookies.*

O site eletrônico da empresa faz uso de *Cookies*, que são arquivos de texto enviados pela plataforma ao seu computador e que nele se armazenam, que contém informações relacionadas à navegação do site. Em suma, os c*ookies* são utilizados para aprimorar a experiência de uso. Ao acessar o site e consentir o uso de *cookies*, o usuário deve manifestar conhecer e aceitar a utilização de um sistema de coleta de dados de navegação com o uso de *cookies* em seu dispositivo.

A partir dos *cookies*, o usuário é reconhecido mais rapidamente nos sites, outros analisam estatísticas e/ou comportamento de navegação para gerar dados para serem utilizados como ferramentas de *marketing*, promoções e serviços na customização e personalização de relacionamento. Os dados pessoais dos consumidores são usados sob o consentimento e os mesmos não são divulgados, compartilhados ou vendidos sem a devida autorização prévia, a menos que seja necessário fazê-lo por lei. Os dados são mantidos por período necessário para que possam ser atingidas as finalidades especificadas. Se o cliente, em algum momento, consentiu receber ofertas promocionais e de *marketing* da empresa, o mesmo poderá revogar este consentimento a qualquer momento. As finalidades e as razões

para o tratamento dos dados pessoais estão detalhadas:

- Na pesquisa de compra dos produtos: os dados pessoais são coletados para atender os interesses de compra e venda de veículos, prestar informações técnicas, financeiras e econômicas, realizar *test-drives*, apresentar propostas e pacotes de vendas e serviços (seguros, blindagem, financiamentos, personalização de produto) durante os ciclos de pesquisa de compra que podem ser imediatos, de curto ou médio prazos nas nossas práticas e objetivos de vendas, e nos seus interesses diretos de compra dos nossos produtos ou serviços.
- Na jornada de compra dos nossos produtos ou serviços: os dados pessoais são coletados e armazenados como parte da obrigação legal para fins de contabilidade Empresa Controladoria e tributária (emissão de notas fiscais, controles fiscais, controles financeiros, balanço e relatórios contábeis, garantias de produto).
- No contrato de compra e uso de produtos sob nossa responsabilidade: a empresa tem a temos a obrigação legal de compartilhar os dados pessoais com órgãos federais e estaduais do Governo como Denatran, Detran, assim como com o sistema bancário para as operações financeiras envolvidas no contrato de compra e venda, incluindo uma agência de referência de crédito que nos fornece verificações de antecedentes financeiros para liberação de crédito na aquisição de produtos e serviços de assistência (garantia, peças, serviços de revisão e oportunidades promocionais de troca do veículo).
- Para as atividades de marketing, propaganda e promoção de marca e produtos: ocasionalmente, informações de *marketing* serão enviadas, de modo que pode ser benéfico ao consumidor. Tais informações não são intrusivas e são tratadas com base em nossos interesses legítimos, podendo o usuário optar, a qualquer momento, por não receber estas informações.

4.5. Política de retenção de dados.

Esta política define os períodos de retenção necessários para todas as categorias específicas de dados pessoais e define os padrões mínimos a serem aplicados ao destruir certas informações dentro da Sintética, doravante denominada “Empresa”. Aplica-se a todas as unidades de negócios, processos e sistemas nos quais a Empresa conduz negócios e possui negócios ou outras relações comerciais com terceiros, a todos os executivos, diretores, trabalhadores, agentes, afiliadas, contratados, consultores ou prestadores de serviços da Empresa que possam recolher, processar ou ter acesso a dados pessoais.

É responsabilidade de todos se familiarizarem com a Política e garantir o cumprimento adequado. Aplica-se a todas as informações usadas na empresa, sendo exemplos de documentos incluídos: endereços eletrônicos; documentos impressos; documentos digitais; vídeo e áudio; dados gerados por sistemas de controle de ponto.

Regras de Retenção

No caso de qualquer categoria de documentos não especificamente definidos em outra parte desta Política (e em particular, no Calendário de Retenção de Dados) e a menos que exigido de outra forma pela lei aplicável, o período de retenção exigido para esse documento será de 05 anos a partir da data de criação dos documentos. Para isso, são definidos: (i) Programa Geral de Retenção; (ii) *Backup* dos Dados durante o Período de Retenção; (iii) Destruição de Dados; (iv) Violação, Execução e Conformidade; (v) Calendarização da Rotina de Destruição; (vi) Método de Destruição.

<u>(i) Programa Geral de Retenção</u>

A Equipe de Proteção de Dados define o período de tempo durante o qual os documentos e registros eletrônicos devem ser retidos por meio do Calendário de Retenção de Dados. Poderão existir exceções aos períodos de retenção no Calendário de Retenção de Dados nos seguintes casos:

- Investigações em andamento das autoridades dos Estados Membros, se houver uma necessidade de registos de dados pessoais serem necessários pela Empresa para comprovar o cumprimento de quaisquer requisitos legais; ou
- Quando exercem direitos legais em casos de processos judiciais pela legislação local.

(ii) *Backup* dos Dados durante o Período de Retenção

A possibilidade de que os meios de dados usados para backup se desgastem deve ser considerada. Se forem escolhidos meios de *backup* eletrônicos, todos os procedimentos e sistemas que garantem o acesso à informação durante o período de retenção (tanto no que diz respeito ao portador da informação quanto na legibilidade dos formatos) também serão guardados de maneira a proteger as informações contra perdas como resultado de futuras mudanças tecnológicas. A responsabilidade pelo armazenamento é da Equipe de Proteção de Dados.

(iii) Destruição de Dados

A Empresa e os seus funcionários devem regularmente rever todos os dados, sejam eles mantidos eletronicamente ou em papel, para decidir eliminar ou excluir quaisquer dados, uma vez que a finalidade para a qual esses documentos foram criados já não são mais relevantes. A responsabilidade geral pela destruição de dados é da Equipe de Proteção de Dados. Uma vez tomada a decisão de eliminar de acordo com o Calendário de Retenção, os dados devem ser excluídos, triturados ou destruídos tendo em atenção se é papel ou em formato eletrônico dependendo da sua forma e tendo em conta sempre o grau equivalente ao seu valor para os outros e o seu nível de confidencialidade. O método de destruição varia e depende da natureza do documento.

O processo específico de eliminação ou destruição pode ser realizado por um trabalhador ou por um prestador de serviços interno ou externo que a Equipe de Proteção de Dados subcontrate para este fim. Quaisquer disposições gerais aplicáveis ao abrigo das leis de proteção de dados relevantes e da Política Geral de Proteção de Dados Pessoais da Empresa devem ser cumpridas. Devem existir controles apropriados que impeçam a perda permanente de informações essenciais da empresa como resultado da destruição maliciosa ou não intencional de informações.

A Equipe de Proteção de Dados deve documentar e aprovar totalmente o processo de destruição. Os requisitos legais aplicáveis para a destruição de informações, particularmente os requisitos sob as leis de proteção de dados aplicáveis devem ser integralmente observados.

(iv) Violação, Execução e Conformidade

A pessoa designada com responsabilidade pela Proteção de Dados e a Equipe de Proteção de Dados, tem a responsabilidade de garantir que a Empresa cumpra esta Política. É também da responsabilidade deste auxiliar a Empresa com perguntas de qualquer proteção de dados local ou autoridades governamentais. Qualquer suspeita de violação desta Política deve ser reportada imediatamente à Equipe de Proteção de Dados. Todos os casos de suspeita de violações desta Política devem ser investigados e tomadas as medidas apropriadas.

O não cumprimento desta Política pode resultar em consequências adversas, incluindo, mas não limitado a perda de confiança do cliente, litígio e perda de vantagem competitiva, perda financeira e danos à reputação da Empresa, danos pessoais, danos ou perdas. O não cumprimento desta Política pelos trabalhadores permanentes, temporários ou contratados, ou quaisquer terceiros, que tenham tido acesso às instalações ou informações da Empresa, pode, portanto, resultar em processos disciplinares ou no término de seu contrato de trabalho. Tal não conformidade também pode levar a ação(ões) legal(ais) contra as partes envolvidas em tais atividades.

(v) Calendarização da Rotina de Destruição

Os registros que podem ser regularmente destruídos, a menos que sujeitos a uma investigação legal ou regulatória em andamento, são os seguintes:

- Anúncios e avisos de reuniões diárias e outros eventos, incluindo aceitações e pedidos de desculpas;
- Solicitações de informações comuns, como rotas de viagem;
- Reservas para reuniões internas sem cobranças/custos externos;
- Transmissão de documentos, tais como cartas, mensagens de correio eletrônico ou postal, folhetos e itens semelhantes que acompanham documentos, mas não adicionam qualquer valor;
- Recados de mensagens;
- Lista de endereços substituída, listas de distribuição, etc.
- Duplicação documentos como cópias de documentação de identificação pessoal, rascunhos

inalterados, impressões de Snapshots ou extratos de bancos de dados e arquivos diários;

- Publicações internas de stock(s) obsoletas
- Revistas comerciais, catálogos de fornecedores, folhetos e boletins informativos de fornecedores ou outras organizações externas.

Em todos os casos, a eliminação encontra-se sempre sujeita a quaisquer requisitos que possam existir no contexto de um litígio.

(vi) Método de Destruição

Os documentos de Nível I são aqueles que contêm informações de mais alta segurança e confidencialidade e aquelas que incluem dados pessoais. Estes documentos devem ser eliminados como lixo confidencial (triturado transversalmente) e sujeitos a uma eliminação eletrônica segura. A destruição dos documentos deve incluir prova de destruição.

Os documentos de nível II são aqueles que não contêm informações confidenciais ou dados pessoais e são documentos da empresa publicados. Estes devem ser triturados ou descartados através de uma empresa de reciclagem e incluir, entre outras coisas, anúncios, catálogos, panfletos e boletins informativos. A destruição dos documentos não necessita incluir prova de destruição.

4.6. Registros das atividades de tratamento.

O inventário consiste em uma lista dos serviços/processos de negócios inventariados (Lista Inventário) e, pelo menos, em um formulário de inventário (Template). Deve-se criar uma guia para cada serviço/processo de negócio a ser inventariado com base no Template. A partir deles, atividades sao tratadas à face da LGPD.

- Lista inventário: proprociona uma lista geral dos serviços/processos de negócio institucionais que realizam o tratamento de dados pessoais (Figura 3).

Listagem geral do inventário dos serviços/processos de négocio que tratam dados pessoais						
Controlador	Nome:		E-mail:		Endereço:	
	CEP:		Cidade:		Telefone:	
Encarregado	Nome:		E-mail:		Endereço:	
	CEP:		Cidade:		Telefone:	

Nome do serviço/processo de negócio	Nº Ref / ID	Data de Criação do Inventário	Data de Atualização do Inventário	Finalidade do tratamento dos dados pessoais	Trata Dados Pessoais Sensíveis?

Figura 3 - Listagem de inventário. Fonte: autoria própria (2024).

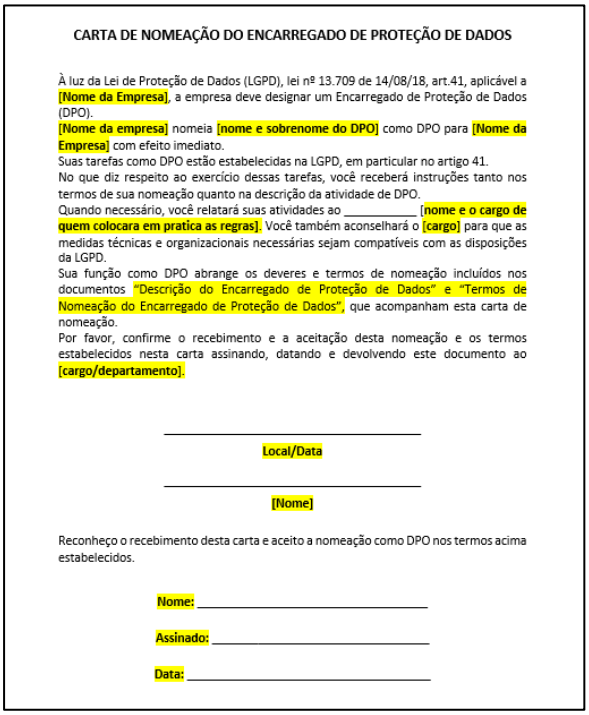
- *Template*: modelo de formulário de inventário de dados pessoais. Essa guia deve ser replicada e preenchida quantas vezes for necessário para documentar todos os serviços/processos de negócios que tratam dados pessoais na instituição (Apêndice A). Para isso, são mantidas informações sobre:

1 - Identificação dos serviços / processo de negócio de tratamento de dados pessoais
2 - Agentes de Tratamento e Encarregado
3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais
4 - De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados
5 - Escopo e Natureza dos Dados Pessoais
6 - Finalidade do Tratamento de Dados Pessoais
7 - Categoria de Dados Pessoais
8 - Categorias de Dados Pessoais Sensíveis
9 - Frequência e totalização das categorias de dados pessoais tratados
10 - Categorias dos titulares de dados pessoais

11 - Compartilhamento de Dados Pessoais
12 - Medidas de Segurança/Privacidade
13 - Transferência Internacional de Dados Pessoais
14 - Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio

4.7. Carta de nomeação de DPO.

Trata-se do documento o qual a empresa usa para definir qual o colaborador responsável por conduzir as atividades de proteção de dados (Figura 4).



CARTA DE NOMEAÇÃO DO ENCARREGADO DE PROTEÇÃO DE DADOS

À luz da Lei de Proteção de Dados (LGPD), lei nº 13.709 de 14/08/18, art.41, aplicável a **[Nome da Empresa]**, a empresa deve designar um Encarregado de Proteção de Dados (DPO).
[Nome da empresa] nomeia **[nome e sobrenome do DPO]** como DPO para **[Nome da Empresa]** com efeito imediato.
Suas tarefas como DPO estão estabelecidas na LGPD, em particular no artigo 41.
No que diz respeito ao exercício dessas tarefas, você receberá instruções tanto nos termos de sua nomeação quanto na descrição da atividade de DPO.
Quando necessário, você relatará suas atividades ao _____ [**nome e o cargo de quem colocara em pratica as regras**]. Você também aconselhará o **[cargo]** para que as medidas técnicas e organizacionais necessárias sejam compatíveis com as disposições da LGPD.
Sua função como DPO abrange os deveres e termos de nomeação incluídos nos documentos "Descrição do Encarregado de Proteção de Dados" e "Termos de Nomeação do Encarregado de Proteção de Dados", que acompanham esta carta de nomeação.
Por favor, confirme o recebimento e a aceitação desta nomeação e os termos estabelecidos nesta carta assinando, datando e devolvendo este documento ao **[cargo/departamento]**.

_____
Local/Data

_____
[Nome]

Reconheço o recebimento desta carta e aceito a nomeação como DPO nos termos acima estabelecidos.

Nome: _____

Assinado: _____

Data: _____

Figura 4 - Carta de nomeação do encarregado de proteção de dados. Fonte: autoria própria (2024).

4.8. Notificação de violação de dados pessoais.

Trata-se de um formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD). Nele, são apontadas informações sobre:

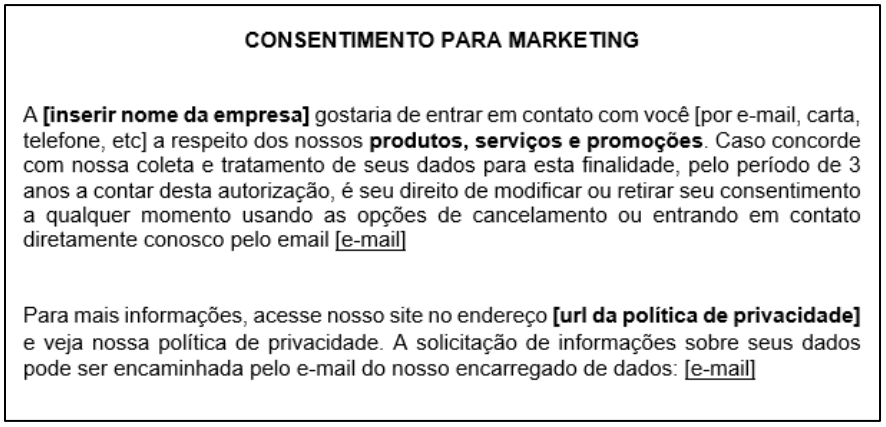
- Comunicação: tipo de comunicação e critério para a comunicação.
- Agente de tratamento: caracterização do notificante; dados do agente de tratamento; dados do notificante; e dados do encarregado.
- Incidente de segurança: descrição do incidente de segurança com os dados pesssoais; quando o incidente aconteceu; quando a organização teve ciência do incidente de segurança; como a organização teve ciência do incidente de segurança; motivos da comunicação do incidente não ter sido feita em dois das úteis, natureza dos dados afetados; quantidade de titulares afetados; e categoria dos titulares afetados.
- Medidas de segurança utilizadas para a proteção dos dados: quais medidas de seguranças foram tomadas para prevenir o incidente de segurança; quais medidas de seguranças foram tomadas após o incidente de segurança; quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados; registrar se foi feito relatório de impacto à proteção de dados pessoais.
- Riscos relacionados ao incidene de segurança: prováveis consequências do incidente de segurança para os titulares afetados; se o incidente pode trazer consequências transfronteiriças aos titulares

afetados.

- Comunicação aos titulares de dados: se os titulares foram comunicados sobre o incidente de segurança com dados pessoais.

4.9. Formulário de consentimento para *marketing*.

Trata-se de um documento onde o usuário aponta a concordância (ou não) quanto à oferta e produtos, serviços e promoções (Figura 5).



CONSENTIMENTO PARA MARKETING

A **[inserir nome da empresa]** gostaria de entrar em contato com você [por e-mail, carta, telefone, etc] a respeito dos nossos **produtos, serviços e promoções**. Caso concorde com nossa coleta e tratamento de seus dados para esta finalidade, pelo período de 3 anos a contar desta autorização, é seu direito de modificar ou retirar seu consentimento a qualquer momento usando as opções de cancelamento ou entrando em contato diretamente conosco pelo email [e-mail]

Para mais informações, acesse nosso site no endereço **[url da política de privacidade]** e veja nossa política de privacidade. A solicitação de informações sobre seus dados pode ser encaminhada pelo e-mail do nosso encarregado de dados: [e-mail]

Figura 5 - Formulário de consentimento para o marketing. Fonte: autoria própria (2024).

O consentimento é válido por 3 (três) anos, podendo ser revogado ou modificado.

4.10. Dificuldades de implementação da LGPD na empresa.

Implementar os requisitos da LGPD requer um rabalho contínuo dentro da empresa. É importante ressaltar que a adequação quanto aos pontos da lei não acontece de maneira repentina, pois envolve mudança de cultura corporativa. A limitação de acesso de dados pessoais gerou uma disputa de interesses nos setores da empresa. Houve uma rejeição, por parte dos responsáveis das área comercial e de *marketing*, quanto à alteração dos processos em resposta à LGPD. Isso porque, com menos informações disponíveis, pode-se limitar o trabalho desenvolvido pelos setores nas atividades de vendas.

Fato este que tem justificado constantes questionamentos sobre os limites da LGPD, sobre o que é tratado, o que é requisitado, o que abrange, bem como se dará o processo de fiscalização. Frisa-se que o projeto ainda não foi implementado em sua totalidade, especialmente em função do enfraquecimento da fiscalização de LGPD no Brasil.

Para a sua finalização, faltam alterações e implementações de processos no setor de tecnologia de informação. As áreas responsáveis precisam reconhecer a importância do avanço e execução do projeto - ressalta-se que, depois do mapeamento de processos, as ações de adequação pouco avançaram. Falando especificamente do setor de marketing, é necessário o desenvolvimento de estratégias para o controle de contatos ativos e de ações de modo que não se diminua a capacidade de trabalho realizada pelo setor.

A empresa, para a continuidade do projeto, precisa manter o grupo de trabalho unido, de modo que o mesmo acompanhe periodicamente o percentual de aderência da empresa a aspectos da LGPD. É preciso que os processos sejam sempre revisados como forma de se manter a conformidade da empresa, em relação aos requisitos da lei, bem como haja segurança e ações que antevenham riscos de uso dos dados pessoais.

5. Considerações finais.

Este estudo teve como finalidade a implementação da Lei Geral de Proteção de Dados (LGPD) em uma concessionária automotiva. Para isso, desenvolveu os documentos indicados para o

cumprimento dos requisitos da Lei 13.709/2018

Dessa maneira, o estudo desenvolveu: 1. Política de privacidade para funcionários; 2. Política de privacidade para consumidores e parceiros; 3. Política de execução dos direitos do titular; 4. Política de cookies; 5. Política de retenção de dados; 6. Registro de atividades de tratamento de dados pessoais (*data mapping*); 7. Carta de nomeação do *Data Protection Officer* (DPO); 8. Notificação de violação de dados pessoais; 9. Formulário de consentimento para *marketing*.

Para operacionalizar as ações da LGPD é fundamental um trabalho profundo com a equipe, uma vez que repercutirá em mudanças na cultura corporativa da empresa. Além disso, como relatado anteriormente, tais adaptações também geram conflitos internos, que precisam ser monitorados e resolvidos.

Para estudos futuros, sugere-se o desenvolvimento do Relatório de Impacto de Proteção de dados pessoais (RIPD), documento importante em situações específicas, e de documentos de boas práticas, como cláusulas em contratos com operadores e com terceiros (incluindo transferências internacionais), política de violação de dados pessoais, notificação de violação de dados e registro de violação de dados pessoais. Para isso, a empresa precisa consolidar o sistema em desenvolvimento, de modo a amadurecer.

Ressalta-se que o desenvolvimento de estudos na área de proteção de dados é indispensável às empresas e aos seus usuários. Isso porque deve-se assegurar o uso adequados dos dados pessoais, em consonância com a percepção dos clientes, que estão cada vez mais conscientes quanto às consequências negativas do mal uso por parte das empresas.

Referências.

BEZERRA, I. H. G.; VIEIRA, L. F. C.; NASCIMENTO, P. A. Adequação e a execução da LGPD 13.709/18 em face as empresas, e sua proteção dos dados pessoais. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 7, 2022. p. 875-883.

BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento**. Imprenta: Rio de Janeiro: Forense, 2020.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

CAIRES, K. A. **A proteção dos dados e a LGPD: desafios na implementação da LGPD**. Trabalho de Conclusão de Curso. Pontifícia Universidade Católica de Goiás. 2023.

CARVALHO, H. E. R. H.; FREITAS, A. E. B.; SANTOS, D. R. Impactos da implantação da Lei Geral de proteção de dados pessoais no brasil: uma análise bibliométrica: Impacts of the implementation of the General Law for the protection of personal data in brazil: a bibliometric analysis. **Revista de Gestão e Secretariado**, v. 13, n. 3, 2022. p. 1398-1411.

COUNCIL OF EUROPE. **Detalhes do Tratado No. 108**. 1985. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 03 jun. 2023.

CUNHA, B. E. M.; PINTO, E. D.; TIMOTEO, G.; BARBOSA, J. V. A.; ALMEIDA, M. E. M. AS DIFICULDADES DA IMPLEMENTAÇÃO DA LGPD NO BRASIL. **Revista Projetos Extensionistas**,v.1, n. 2, jul./dez. 2021. p. 39-47.

FONSECA, J. J. S. **Metodologia da pesquisa científica.** Fortaleza: UEC, 2002. Apostila.

GARCIA, L. R.; AGUILERA-FERNANDES, E.; GONÇALVES, R. A. M.; PEREIRA-

BARRETO, M. R. **Lei Geral de Proteção de Dados Pessoais (LGPD):** guia de implantação. Editora Edgard Blücher, 2020.

GIL, A. C. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2007.

PANEK, Lin Cristina Tung. **Lei Geral de Proteção de Dados n° 13.709/2018:** Uma análise dos principais aspectos e do conceito de privacidade na sociedade informacional. 2019. 50 f. Monografia (Graduação). Universidade Federal do Paraná, Curitiba, 2019.

LIMA, A. P. M. C. **LGPD – Lei Geral de Proteção de dados [recurso eletrônico]:** sua empresa está pronta? São Paulo: Literare Books International, 2020.

LIMBERGER, T. Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação Pública (LAI): um diálogo (im) possível? As influências do direito europeu. **Revista de Direito Administrativo**, v. 281, n. 1, 2022. p. 113-144.

MONTEIRO, L.R, et al. **Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos**. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em: 03 jun. 2023.

MINAYO, M. C. S. (Org.). **Pesquisa social:** teoria, método e criatividade. Petrópolis: Vozes, 2001.

NASCIMENTO, Luciano. **Governo publica MP que cria órgão para proteção de dados**. AgênciaBrasil, Brasília, 28 dez. 2018. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2018-12/governo-publica-mp-que-cria-orgao-para-protecao-de-dados. Acesso em 12 ago. 2023.

SILVA, Itapoã Fortunato da. **Proteção de Dados Pessoais**: o processo de implementação da LGPD em uma Universidade Pública Federal. Trabalho de Conclusão de Curso (Graduação) – Universidade Federal de Pernambuco. Centro de Artes e Comunicação. Departamento de Ciência da Informação. Curso de Gestão da Informação, 2021.

SILVA, S. L. P.; COSTA., W. P. L.B.; PAULA, G. R.; SILVA, J. D. Lei Geral de Proteção de Dados (LGPD): implementação nos escritórios de contabilidade **Revista de Contabilidade da UFBA**, v.17, e2313, 2023. p. 1-16.

SILVEIRA, Sergio Amadeu da.**Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais**. São Paulo: Edições Sesc, 2017.

THIOLLENT, M. Metodologia da pesquisa-ação. São Paulo: Cortez & Autores Associados, 1988.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais:** a pesquisa qualitativa em educação. São Paulo: Atlas, 1987.

YIN, R. K. **Estudo de caso:** planejamento e métodos. Trad. de Daniel Grassi. Porto Alegre: Bookman, 2001.