Estudo para adequação de um provedor de internet a LGPD

Vinicius Cassis De Mello[1], Marcos Juares Vissoto Corino[1]

[1]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS), Campus Veranópolis – RS – Brasil

sh4rkrs@yahoo.com.br, marcos.corino@veranopolis.ifrs.edu.br

Abstract. *In 2018, the General Law for the Protection of Personal Data (LGPD, Law n. 13.709/2018) was approved, which brings challenges for companies that need to comply and comply with legal requirements. Thus, this study sought to identify compliance with LGPD requirements in a telecommunications service provider company in Nova Prata, Rio Grande do Sul. For this, the company's data, the implementation methods used and the planning for Future actions having this analysis aim at the company's internal processes in relation to its customers' data. Thus, it was found that the company's processes show a certain degree of maturity. However, it still needs to improve some procedures, so it was suggested the preparation of a Personal Data Protection Impact Report (RIPD) and the design of a data protection officer (DPO), suggestions that are intended to help the company's maturation in its process of compliance with the law.*

Resumo. *Em 2018, foi aprovada a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei n. 13.709/2018), que traz desafios para as empresas que precisam estar em conformidade e cumprir as exigências legais. Deste modo, esse estudo buscou identificar o atendimento aos requisitos da LGPD em uma empresa provedora de serviço de telecomunicações de Nova Prata, Rio Grande do Sul. Para isso, analisou-se os dados da empresa, os métodos de implementação utilizados e o planejamento para ações futuras tendo esta análise tem como objetivo os processos internos da empresa em relação aos dados de seus clientes. Com isso verificou-se que os processos da empresa mostram certo grau de maturidade. Contudo ainda precisa aprimorar alguns procedimentos, sendo assim sugeriu-se a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e a concepção de um oficial de proteção de dados (DPO), sugestões que pretendem auxiliar no amadurecimento da empresa em seu processo de adequação à lei.*

1. Introdução

O vazamento de dados da população brasileira em 2021, rotulado de Vazamento de Dados do Fim do Mundo, revelou dados de brasileiros, vivos e mortos, expondo CPFs, e-mails, telefones de mais de 223,7 milhões de indivíduos. Esse episódio somente foi descoberto após os dados terem sido colocados à venda na internet. O que ainda não se tem conhecimento é a fonte onde esses dados foram obtidos, porém sabe-se que alguns fazem referências a empresas e serviços, assim é possível que sua origem pode ser de diversas fontes.

A privacidade digital torna-se uma necessidade da sociedade moderna. Essa privacidade é uma garantia constitucional assegurada por mecanismos legais de proteção, como o Marco Civil da Internet (Lei n. 12.965/2014) e a Lei do Consumidor (Lei n.

8.078/1990). Cabe ressaltar que a privacidade se diferencia de proteção de dados, e que mesmo um dado público deve ser protegido [Garcia et al. 2020]. Por este motivo, em 2018, sancionada Lei Geral de Proteção de Dados Pessoais (a LGPD, Lei n. 13.709/2018), para estabelecer uma estrutura legal com objetivo exclusivo na proteção de dados. Essa lei também institui a criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP), subordinadas à presidência da República e unicamente dedicadas ao tema.

Baseada nos direitos fundamentais de liberdade e privacidade, a LGPD define normas e regras rigorosas para a proteção de dados pessoais, regulando seu tratamento, que é entendido como "qualquer ação realizada desde a coleta, cópia, edição, armazenamento, publicação, impressão, transmissão, processamento e compartilhamento de dados pessoais" [Marinho 2020, p.8]. Essa regulamentação busca robustecer o direito à privacidade dos titulares de dados, protegendo os direitos fundamentais dos indivíduos, por meio do fortalecimento da segurança da informação no que diz respeito à privacidade, transparência, desenvolvimento, padronização, proteção do mercado e livre concorrência [Marinho 2020].

Esse instrumento regulatório traz diversos desafios e oportunidades positivas para a segurança da informação. Empresas, independentemente do porte, que oferecem produtos e serviços ao mercado brasileiro, que coletam e tratam dados de pessoas que estejam no país precisam se preparar para estarem em conformidade e cumprir as exigências legais da lei [Donda 2020] e para isso será necessária uma extensa mudança nos sistemas de gestão de dados no Brasil. Será preciso regulamentar a maneira que as instituições irão utilizar esses dados, estabelecendo limites e normas para todas as empresas em território nacional ou empresas nacionais em território estrangeiro [Marinho 2020]. Todas as atividades que realizam o processamento de dados pessoais, sejam próprios ou de terceiros serão afetadas em suas "relações comerciais e de consumo, relações de trabalho e emprego, tecnologia e processos, políticas corporativas de privacidade, ética e segurança de dados, bem como na capacitação e no treinamento de pessoal (público interno e externo)" [Marinho 2020, p8].

Neste sentido, é necessário realizar um diagnóstico situacional da empresa e seus processos em relação aos requisitos de conformidade da LGPD para identificar possíveis brechas e assim definir escopo, planejamento, investimento e esforço necessário para o desenvolvimento das atividades de adequação. Para as empresas que já possuem dados armazenados se faz necessário fazer um levantamento desses dados e colocá-los em conformidade com a LGPD, assim como revisar toda a política de privacidade e verificar a adequação das empresas parceiras de coleta e tratamento de dados [Panek 2019]. Assim, as empresas precisarão tomar algumas medidas básicas e essenciais para se prepararem e se adaptarem às conformidades legais como, por exemplo, o tratamento dos dados.

Deste modo, esse estudo buscou identificar o atendimento aos requisitos da LGPD em uma empresa provedora de serviço de telecomunicações de Nova Prata, Rio Grande do Sul. Da mesma forma, foram propostas adequações para os processos a fim de torná-los alinhados com as exigências da lei. Para isso, analisou-se os dados da empresa desde a coleta, processamento, armazenamento até o compartilhamento de dados pessoais na empresa, os métodos de implementação utilizados e o planejamento para ações futuras. Cabe ressaltar que esta análise tem como objetivo os processos internos da empresa em

relação aos dados de seus clientes, excetuando-se destes qualquer informação oriunda a dados de conexão como conteúdo, horário, acessos, entre outros do tipo.

O trabalho será estruturado conforme as seguintes seções: na seção 2 uma revisão da literatura a respeito da LGPD e trabalhos relacionados, na sequência na seção 3 a metodologia utilizada e o mapeamento dos dados, na seção 4 a apresentação e discussão dos resultados, na seção 5 as considerações finais e na seção 6 as referências bibliográficas.

2. Revisão da literatura

A LGPD dispõe sobre o tratamento de dados pessoais, por meio digital ou não, por pessoas físicas ou jurídicas, visando proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural [Brasil 2018]. Para isso a lei se fundamenta em alguns princípios como (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; e (vii) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais[Brasil 2018]. Esse instrumento é aplicado a qualquer operação de tratamento, independentemente do tipo de entidade, do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que eles tenham sido coletados ou o tratamento seja realizado no território nacional [Brasil 2018].

As organizações e seus sistemas de informação e redes enfrentam ameaças de segurança provenientes de um amplo leque de fontes. As causas de danos, como códigos maliciosos, atividades de *hacking* em computadores e ataques de negação de serviço (ou *denial-of-service*) se tornaram mais comuns, mais ambiciosas e cada vez mais sofisticadas, portanto a segurança da informação é muito importante tanto para os negócios públicos quanto para o setor privado, e para proteger infraestruturas críticas.

Na norma ISO 27001 estão presentes três pilares da segurança da informação, também conhecidos como os princípios mais significativos em todos os programas de segurança que são a integridade, a confidencialidade e a disponibilidade. Esta norma trabalha em conjunto com a ISO 27002 que auxilia a segurança da informação. O nível de segurança requisitado para executar esses princípios é diferente para cada empresa, pois cada uma tem as suas finalidades e seus requisitos de negócios e de segurança. Todos os mecanismos e proteções são implementados para abastar um ou mais desses princípios, e todos os riscos, ameaças e vulnerabilidades são avaliados pela sua capacidade potencial de comprometer um ou todos os princípios.

De acordo com [Baars et al. 2018] a confidencialidade refere aos limites em termos de quem pode obter que tipo de informação. Já a integridade se refere a ser correto e consistente com o estado ou a informação pretendida, sendo que qualquer modificação não autorizada de dados é uma violação da integridade dos dados. E a disponibilidade garante que os sistemas estão ativos e funcionando quando necessário.

Segundo Teffé e Viola (2020) na LGPD parte-se da ideia de que todo dado pessoal tem valor e importância. Dados que pareçam não relevantes em um momento ou que não façam referência a alguém diretamente, uma vez transferidos, cruzados ou organizados, podem resultar em dados bastante específicos sobre determinada pessoa, trazendo

informações inclusive de caráter sensível a seu respeito. Uma informação pode possuir vínculo objetivo com um indivíduo, mostrando algo sobre ela, ou seja, a informação se refere às características ou ações desta pessoa, ou então que são informações nativas de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações [Doneda 2011].

Em sua redação a lei define conceitos norteadores para seu entendimento e aplicação, entre eles destacam-se os conceitos de (i) dado pessoal como a informação relacionada a pessoa natural identificada ou identificável; (ii) dado pessoal sensível pode ser um elemento pessoal sobre raça ou etnia, religião, posição política, dados referentes à saúde ou à vida sexual, informação genética ou biométrica, se vinculado a uma pessoa natural; (iii) dado anonimizado são dados relativos a alguém que não possa ser identificado, através de cruzamentos e/ou técnicas específicas em seu tratamento; (iv) titular pessoa a quem se referem os dados pessoais que são objeto de tratamento; (v) controlador, a quem competem as decisões referentes ao tratamento de dados pessoais;(vi) operador, que realiza o tratamento de dados pessoais em nome do controlador; (vii) O tratamento é tido como toda operação realizada com dados pessoais, desde a coleta, produção, recepção, classificação, utilização, acesso, processamento, arquivamento, armazenamento, até a eliminação, modificação, ou transferência; outro ponto importante e que segundo a lei deve ser imperativo é o (viii) consentimento onde por meio de sua: manifestação livre, informada e inequívoca, o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada e por último o (ix) relatório de impacto à proteção de dados pessoais(RIPD): documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Seguindo o objetivo principal da LGPD, a proteção da intimidade e da privacidade possui importância essencial no contexto do Estado Democrático de Direito e a sua inviolabilidade constitui direito fundamental da pessoa humana, plenamente reconhecido em todo o mundo democrático. [Maichaki 2018].

Uma obrigação imposta pela LGPD para as organizações é a de emitir um Relatório de Impacto de Proteção de Dados (RIPD). Como afirma Pinheiro (2020), os RIPD são documentos em que há a descrição dos procedimentos adotados pela organização no que diz respeito aos aspectos que podem gerar riscos às liberdades civis e ao tratamento de dados pessoais. Como Donda (2020) explica, este documento precisa detalhar todos os processos de tratamento que os dados pessoais sofrem durante o ciclo de vida. Além de conter os riscos e controles de segurança aplicados. O RIPD além de essencial, ajuda a identificar pontos de atenção necessários no processo de conformidade. Assim é possível garantir que os processos legais sejam cumpridos enquanto é feito o processo de conformidade. Devido a esses fatores percebe-se que a utilização desse documento seria de grande relevância para a organização. Portanto, pesquisou-se sobre os procedimentos necessários para a sua elaboração pela empresa, demonstrando quais os responsáveis pelos processos assim como as etapas para a sua construção.

Além disso, aderir a implementação de um *Data Protection* Officer (DPO), tal como também recomenda Pinheiro (2021), para mensurar o processo de conformidade com a lei, se faz de extrema importância. Este profissional tem conhecimento no que concerne ao entendimento de como deve ser feita a proteção dos dados pessoais e sobre regras e os regulamentos brasileiros que condizem com a privacidade e proteção dos dados em ambientes corporativos.

É fundamental entender que ao manipular dados, é possível realizar associações entre estes, gerando como produto diversas outras informações que podem ferir a intimidade e privacidade de uma pessoa. Assim a atividade de tratamento de dados deve respeitar os dez princípios estabelecidos na lei [Brasil 2018, Art 6º]:

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;
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.

Diversos métodos são aplicados na implementação da LGPD, em suma seu reconhecimento a respeito de como será feita a adaptação e após é feito um mapeamento para verificar quais fluxos de dados seriam tratados em seu embasamento. Posteriormente é feita uma análise a respeito dos riscos e impactos relacionados à privacidade até como será feita a sua implementação, os processos são definidos e aplicados e assim a última etapa da aplicação consiste na monitoria dos dados [Brandão 2021].

2.1 Trabalhos relacionados

Foi realizada uma pesquisa em trabalhos que tratassem sobre a implantação da LGPD em empresas. Pode-se observar que os trabalhos encontrados na área ainda são bastante recentes. O artigo de Silva e Lima (2020) trata sobre o armazenamento de dados clínicos em consonância com a LGPD. Nesse estudo os autores fizeram uma pesquisa no Instituto Sobral e Fuzzeto, onde foi constatado que havia pouca informação da parte dos Gestores a respeito do LGPD. Tendo isso em vista foi elaborado um cenário propício para a implementação da LGPD com o objetivo de sugerir métodos de backup que contemplem a segurança.

No trabalho de Viana et al. (2020) foi realizada uma análise do gerenciamento de riscos para compreender os riscos da aplicação da LGPD através de um estudo de caso na empresa Telecom. Os autores concluíram que a implementação da lei iria alterar toda a estrutura e a cultura organizacional da empresa de forma significativa. Ainda, citam que para uma implementação adequada da LGPD é necessário a aderência aos requisitos do escopo da LGPD, o gerenciamento dos riscos, a adesão de todos os agentes envolvidos, além de apoio financeiro e da execução por parte dos patrocinadores do projeto de respostas aos riscos.

3. Metodologia

Por ser uma etapa importante e necessária para realmente entender o processo do ciclo de vida dos dados na empresa, foi feita uma visita técnica a fim de conhecer os processos de atendimento ao cliente no setor de vendas, financeiro e suporte. Da mesma forma verificou-se os dados que cada setor/atendente tem acesso e o fluxo de cada solicitação. Também foi analisado o sistema de ERP utilizado para informatização dos processos com o objetivo de verificar os dados solicitados, tal como nome, endereço, telefone, e-mail e outros dados informados para cadastro ou consulta de serviços além da estrutura de funcionamento, de que forma os dados são armazenados, entre outros. Este sistema tem por principal objetivo cadastrar os dados do cliente e mostrar suas informações, nele é possível também gerenciar os dados de acordo com a atribuição de cada setor. Assim a coleta de dados foi facilitada pelo software de gerenciamento da empresa que possui os elementos de estudo junto ao seu próprio banco de dados. Como a empresa possui muitos clientes, a fim de não estender o processo de classificação e seleção individual do tratamento de dados, foi feita a coleta de dados usando o software de gerenciamento da empresa que possui os dados cadastrais dos clientes junto ao seu próprio banco de dados. Com o uso do ERP foi possível analisar se um dado foi atualizado recentemente ou se ele precisa ser atualizado, qual será a denominação para este dado, se pessoal ou sensível, quem acessa o dado e qual seu ciclo de vida. Posteriormente foi realizada uma reunião com os responsáveis pela TI, segurança e direção da empresa para conhecer um pouco mais sobre o sistema de gestão, os processos implantados e em vias de implantação para reunir mais conhecimento sobre o panorama atual da empresa e assim melhor embasar esse diagnóstico.

Com os dados obtidos na coleta, foi realizado um estudo de campo sobre quais seriam os procedimentos adequados da lei para se implementar a fim de utilizar nas ações futuras de regularização da empresa. Para isso foram utilizadas referências da própria lei e de guias de implementação da mesma. Para iniciar o desenvolvimento deste trabalho foi necessário realizar o processo de levantamento e análise dos dados para investigar a fim de entender como é o fluxo de tratamento de dados da empresa. A tarefa de mapeamento precisa ser capaz de identificar dados sensíveis e as operações por eles sofridas, para posterior adoção de controles de proteção desses dados [Donda 2020]. Esta etapa é a mais importante e complexa no processo de adequação da LGPD, já que os dados são o produto para o tratamento correto e deve-se saber onde estão localizados para definir mecanismos de proteção no tratamento. Para facilitar esta etapa as ações foram divididas da seguinte forma: identificar o fluxo de tratamento de dados (ciclo de vida de dados), identificação e controle de acessos; monitoramento do tratamento dos dados, quem está acessando e de onde, quais ações estão acontecendo, a fim de detectar atividades suspeitas ou acessos não autorizados.

3.1 Mapeamento dos dados

A realização deste processo tem a complexidade e o esforço necessário definidos pelo nível de documentação dos processos da empresa em análise, uma vez que é necessário mapear todos os processos e identificar quais dados são utilizados em cada etapa [Kohls et al. 2021]. Para isso foi adaptado uma planilha tendo como base o modelo de Kohls et al. (2021, p.114), que prevê vários pontos da LGPD que precisam ser levantados e avaliados e que podem ser adaptados às necessidades de cada realidade. Neste processo é indispensável que o conteúdo desta planilha descreva o processo e o tratamento de dados com o maior número de detalhes possíveis, já que servirá de entrada em uma posterior análise de riscos. Neste estudo foram mapeados os processos de cadastro de clientes, instalação, manutenção, suporte e faturamento da empresa, descritos abaixo.

Tabela 1 – Mapeamento do processo de cadastro de clientes. Próprio.

Identificação da atividade de tratamento	
Nome do processo	Cadastro de cliente
Departamento	Comercial
Categorias titulares	Colaboradores
Responsável	Omitido
Última atualização	20/05/2021
Identificação dos dados pessoais tratados	
Dados pessoais tratados	Nome Completo, endereço completo, CPF, RG, telefone e e-mail.
Dados pessoais sensíveis	Não se aplica
Como os dados são obtidos	Telefone.
Onde os dados são armazenados	ERP da empresa com backup da base de dados
Descrição da atividade de tratamento	
Finalidade e fluxo do tratamento	Esta atividade tem por objetivo inserir o titular em na carteira de clientes e realizar sua adesão aos serviços prestados pela empresa por meio da assinatura de contrato. Os dados coletados pelo telefone são inseridos no ERP sem a necessidade de envio de qualquer documentação física ou digital por parte do cliente. Estes dados estarão disponíveis aos setores de manutenção e suporte técnico, financeiro, TI, marketing e direção. Também serão usados para vendas e informações relacionadas à aquisição ou alteração de planos ou produtos
Hipótese legal para tratamento de dados pessoais	Execução dos serviços contratados pelo titular bem como atividades de suporte e manutenção por solicitação ou não do mesmo.
Hipótese legal para tratamento de dados pessoais sensíveis	Não se aplica.
Método de obtenção/revogação do consentimento	Consentimento por meio de assinatura de contrato. Revogação não há definição.
Os dados são compartilhados com outro controlador	Não
Dados anonimizados	Não
Definição do término do tratamento	
Período do tratamento de dados	Não há definição
Ações tomadas após o fim do período de tratamento	Não há definição

Identificação dos operadores de tratamento	
Operador interno	Departamentos Comercial
Responsabilidades do operador interno	Coletar as informações para cadastro de novos clientes, atualização dos existentes e repassar para o setor técnico para instalação dos serviços.
Operador externo	Prestadores de serviços terceirizados
Responsabilidades do operador externo	Realizar a instalação dos serviços contratados no domicílio do cliente.

Tabela 2 – Mapeamento do processo de Instalação, manutenção e suporte. Próprio.

Identificação da atividade de tratamento	
Nome do processo	Instalação, manutenção e suporte
Departamento	Técnico
Categorias titulares	Colaboradores e prestadores de serviço
Responsável	Omitido
Última atualização	20/05/2021
Identificação dos dados pessoais tratados	
Dados pessoais tratados	Nome Completo, endereço completo, CPF, RG, telefone e e-mail.
Dados pessoais sensíveis	Não se aplica
Como os dados são obtidos	Através do ERP da empresa
Onde os dados são armazenados	ERP da empresa com backup da base de dados
Descrição da atividade de tratamento	
Finalidade e fluxo do tratamento	Esta atividade tem por objetivo instalar, manter e dar suporte aos serviços contratados pelo titular. O processo se inicia através da verificação dos dados cadastrais do titular e se estes estão atualizados com base nas informações disponíveis no ERP. Após identificação do problema o atendente N1 busca uma solução para o problema remotamente ou encaminha a uma equipe para realizar uma visita ao domicílio do cliente, caso ainda não se encontre uma solução este encaminha ao suporte N2 para resolução do problema.
Hipótese legal para tratamento de dados pessoais	Execução dos serviços contratados pelo titular bem como atividades de suporte e manutenção por solicitação ou não do mesmo.
Hipótese legal para tratamento de dados pessoais sensíveis	Não se aplica.
Método de obtenção/revogação do consentimento	Consentimento por meio de assinatura de contrato. Revogação não há definição.
Os dados são compartilhados com outro controlador	Não
Dados anonimizados	Não
Definição do término do tratamento	
Período do tratamento de dados	Não há definição
Ações tomadas após o fim do período de tratamento	Não há definição
Identificação dos operadores de tratamento	

Operador interno	Departamento Técnico Interno, N1 e N2
Responsabilidades do operador interno	Realizar a instalação dos serviços contratados bem como a manutenção e o suporte aos mesmos.
Operador externo	Prestadores de serviços terceirizados
Responsabilidades do operador externo	Realizar a instalação dos serviços contratados bem como sua manutenção no domicílio do cliente.

Tabela 3 – Mapeamento do processo de faturamento. Próprio.

Identificação da atividade de tratamento	
Nome do processo	Faturamento
Departamento	Financeiros
Categorias titulares	Colaboradores
Responsável	Omitido
Última atualização	20/05/2021
Identificação dos dados pessoais tratados	
Dados pessoais tratados	Nome Completo, endereço completo, CPF, RG, telefone e e-mail.
Dados pessoais sensíveis	Não se aplica
Como os dados são obtidos	Através do ERP da empresa
Onde os dados são armazenados	ERP da empresa com backup da base de dados
Descrição da atividade de tratamento	
Finalidade e fluxo do tratamento	Esta atividade tem por objetivo arrecadar os valores devidos pelos serviços contratados pelo titular. O processo se inicia através da verificação dos dados cadastrais do titular com base nas informações disponíveis no ERP. Após é feita a emissão do documento de cobrança que é enviado ao domicílio do cliente ou então por meio digital em seu e-mail. Já a cobrança ocorre através da verificação dos pagamentos por parte dos clientes, caso exista um registro de dívida, é realizado contato com o cliente por meio de e-mail, telefone ou SMS.
Hipótese legal para tratamento de dados pessoais	Faturamento dos serviços contratados pelo titular e atividades de cobrança por inadimplência.
Hipótese legal para tratamento de dados pessoais sensíveis	Não se aplica.
Método de obtenção/revogação do consentimento	Consentimento por meio de assinatura de contrato. Revogação não há definição.
Os dados são compartilhados com outro controlador	Não
Dados anonimizados	Não
Definição do término do tratamento	
Período do tratamento de dados	Não há definição
Ações tomadas após o fim do período de tratamento	Não há definição
Identificação dos operadores de tratamento	
Operador interno	Departamento Financeiro

Responsabilidades do operador interno	Acessar e atualizar se necessário os dados para a emissão de documentos de cobrança pelos serviços prestados ao titular.
Operador externo	Operadores bancários
Responsabilidades do operador externo	Realizar o registro dos documentos de cobrança emitidos pelo operador interno.

Após a conclusão da etapa de mapeamento foi realizada a análise desse material, o que possibilitou identificar finalidade adequação e necessidade de determinado dado no processo permitindo realizar considerações e sugestões de mudança a empresa para alinhar sua operação as diretrizes da LGPD, expondo desta forma um diagnóstico situacional da empresa e de seus processos em relação aos requisitos de conformidade a LGPD, identificando possíveis brechas, sugerindo, planejamento, investimento e esforço necessário para o desenvolvimento das atividades de adequação.

4. Apresentação e discussão dos resultados

Como trata-se de uma empresa em processo de adequação à Lei Geral de Proteção de Dados, os processos estudados mostram certo grau de maturidade. Assim a empresa tem buscado se aprimorar e alinhar sua operação ao que dispõe a lei. A partir da análise realizada nos processos de cadastro de clientes, instalação, manutenção, suporte e faturamento da empresa, pode-se constatar que já são adotados processos importantes no sentido do tratamento dos dados e mitigação de riscos, um deles seria um sistema de criptografia integrado com o servidor de dados protege o seu armazenamento, onde são realizados backups diários para garantir a sua segurança. Outro ponto positivo e que deixa o processo menos complexo é a não utilização de dados sensíveis por parte da empresa já que não apresenta a necessidade de tal dado.

Contudo, mediante as demais análises realizadas no desenvolvimento do trabalho alguns pontos no processo de adequação da lei na empresa precisaram ser ajustados. Existe uma lacuna no que diz respeito ao ciclo de vida dos dados e seu tratamento, ou seja, não existe uma previsão definida do término desse ciclo e quais ações são tomadas ao fim deste ciclo.

Outro ponto que carece de atenção diz respeito ao consentimento do titular, não existe um procedimento claro de consentimento e revogação dele. Subentende-se que o consentimento se dá pela assinatura do contrato e que este deve durar durante sua vigência, entretanto, sugere-se que este seja mais bem esclarecido. Pois de acordo com [Brasil 2018] o consentimento precisa ser manifestado livremente por escrito, inequivocamente onde o titular concorda com o tratamento de seus dados para uma finalidade específica. Aqui também cabe uma referência ao apontamento anterior, devendo ser indicado ao titular as ações tomadas após a revogação deste consentimento no que diz respeito à eliminação dos seus dados, uma vez que a lei determina que se faça.

Encerrada as considerações acerca de modificações dos processos existentes passaremos a indicar agora adoções de medidas ainda não realizadas pela empresa. Entre elas destacam-se a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e a concepção de um oficial de proteção de dados (DPO), pontos importantes sugeridos por Pinheiro (2021) e reforçado por Donda (2020).

O DPO deve procurar liderar um comitê de modo que organize as ações relacionadas à proteção e análise dos dados. Sua estruturação pode ser essencial para regulamentar junto com a aplicação do RIPD além de diminuir a carga de trabalho imposta sobre um colaborador com muitas atribuições. Algumas das principais funções onde o DPO se faz responsável segundo Ribeiro (2020):

i. Interagir com os titulares dos dados pessoais, inclusive prestando esclarecimentos, e adotando medidas necessárias referente a tais contatos ou reclamações dos titulares;
ii. Interagir com a Autoridade Nacional de Proteção de Dados (ANPD), sendo com ponto de contato quanto ao contato e o recebimento de comunicações da ANPD.
iii. Orientar os colaboradores da entidade, no que diz respeito às práticas relacionadas à proteção dos dados.
iv. Executar todas as atribuições determinadas em normas complementares, da ANPD e outras autoridades.
v. Assessorar os responsáveis pelo tratamento dos dados pessoais na emissão de RIPD.
vi. Recomendar a realização do RIPD, inclusive acerca da metodologia de sua realização.
vii. Recomendar salvaguardas para mitigar riscos aos direitos dos titulares, além de medidas e técnicas organizacionais.

Levando em conta como vai ser feita a estruturação do DPO para Donda (2020) os agentes de tratamento de dados, ficam sujeitos a sanções administrativas aplicadas pela ANPD em razão das infrações cometidas às normas previstas na lei. Assim é essencial definir bem quem serão os agentes responsáveis para não haver brechas que possam comprometer o tratamento dos dados.

Já no que diz respeito sobre o RIPD pode ser elaborado no início no projeto ou com um projeto já em andamento, este consiste na definição de três partes atuantes. O encarregado, o responsável pela elaboração e o controlador. Segundo Pinheiro (2021), a elaboração do RIPD na empresa pode ser feita de acordo com cada projeto, seguidos dos riscos envolvidos na operação do mesmo. Uma empresa que elabora o RIPD, ou seja, realiza uma avaliação da conformidade de suas operações quanto ao tratamento de dados, está um passo a mais de sua adequação, além de assegurar os direitos dos titulares dos dados quanto à sua proteção.

Ainda nas considerações sobre os processos da empresa em relação a LGPD e a bibliografia estudada para o embasamento deste trabalho, sugere-se que a empresa crie um grupo para análise e tomada de decisões sobre os processos que envolvem dados, e que este realize um mapeamento do ciclo de vida dos dados para facilitar seu entendimento. Também é importante a adoção de padrões de segurança da informação e de processos de auditoria bem como planos de ação para emergências.

5. Considerações Finais

Apesar do fato de a LGPD já estar em vigor, empresas ainda estão se adequando aos processos. A empresa estudada neste trabalho está um passo à frente das outras por já ter iniciado o processo e adequado alguns de seus parâmetros. Contudo a total adequação ainda necessita passar por diversos processos.

Este estudo permitiu identificar os tipos de dados utilizados pela empresa nos processos de relacionamento com o cliente e verificar qual o grau de adequação aos princípios da LGPD. A utilização planilha como ferramenta para mapeamento dos dados e seu tratamento torna o processo mais fácil de ser conduzido pois os relacionamentos estão todos descritos no mesmo documento, permitindo a visualização de possíveis pontos de atenção de forma mais eficiente.

As sugestões apresentadas neste trabalho, pretendem auxiliar no amadurecimento da empresa em seu processo de adequação à lei, contribuindo para os próximos passos a serem realizados nesta caminhada. Visando trabalhos futuros a intenção é de junto com a empresa acompanhar a aplicação das sugestões apontadas por este estudo.

6. Referências Bibliográficas

Brandão, G. (2021) O que é mapeamento de dados. Disponível em: https://blconsultoriadigital.com.br/mapeamento-de-dados/ , Abril.

BRASIL. Lei Federal Nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Senado Federal.

BRASIL. Lei Federal Nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Senado Federal.

Kohls C. et al. (2021). LGPD: Da teoria à implementação nas empresas. Editora Rideel.

Donda D. (2020) Guia prático de implementação da LGPD. São Paulo, Editora Labrador.

Doneda, D. (2011) "A proteção dos dados pessoais como um direito fundamental". Espaço Jurídico. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez.

Garcia, R. C. de C. (2020) "Proteção de dados pessoais no Brasil: uma análise da Lei nº 13.709/2018 sob a perspectiva da Teoria da Regulação Responsiva". Revista de Direito Setorial e Regulatório, Brasília, v. 6, nº 2, p. 45-58.

Baars. H. et al. (2018). Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Editora Brasport

Marinho, F. (2020) "Os 10 mandamentos da LGPD como implementar a Lei Geral de Proteção de Dados em 14 passos" São Paulo, Atlas.

Maichaki, M. R. (2018) "Herança Digital: O Precedente Alemão e os Direitos Fundamentais À Intimidade e Privacidade." Revista Brasileira de Direito Civil em Perspectiva. Porto Alegre v. 4 n. 2 p. 136 – 155.

Panek, L. C. T. (2019), "Lei Geral De Proteção De Dados Nº 13.709/2018: Uma Análise Dos Principais Aspectos E Do Conceito Privacidade Na Sociedade Informacional". Universidade Federal do Paraná. Setor De Ciências Jurídicas, Curitiba. (Trabalho de conclusão de curso).

Pinheiro, P. P. (2018) "Proteção de dados pessoais comentários à Lei n. 13.709/2018 (LGPD)." 3. São Paulo Saraiva Jur.

Pinheiro, P. P. (2020) "Segurança digital proteção de dados nas empresas", São Paulo, Atlas.

Ribeiro, J. F. (2020) “Implantação da lei geral de proteção de dados na companhia de tecnologia da informação do Estado de Minas Gerais - PRODEMGE”. Fundação João Pinheiro, Belo Horizonte. (Trabalho de conclusão de curso).

Silva A. N., Lima J. N. (2020) “Armazenamento de dados clínicos em consonância com a LGPD”. Revista Inovação Tecnológica, São Paulo, v. 10, n. 2, p. 24-42.

Teffé, C. S. de, e Viola, M. (2020) “Tratamento de dados pessoais na LGPD: estudo sobre as bases legais”. Civilistica.com. Rio de Janeiro, a. 9, n. 1.

Viana, C. da S. et al. (2020) “Gerenciamento de riscos na implementação de LGPD pessoais: Estudo de caso”. Engenharia no Século XXI - Volume 19. Belo Horizonte, Editora Poisson.