DOI: 10.5748/18CONTECSI/PSE/AUD/6847

IMPLEMENTATION OF LGPD AND ITS IMPACTS ON A HOLDING COMPANY IN THE HEAVY MACHINERY SECTOR

Rodrigo Alexandre Ciriaco - PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS - Orcid: https://orcid.org/0000-0003-0984-0703

Adriane Maria Arantes Carvalho - PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS - Orcid: https://orcid.org/0000-0001-6754-8116

This research aims to describe the adaptation project of a multinational company from the heavy machinery production sector to the LGPD. Approved in 2018, the Law No. 13.709, known as the General Data Protection Law (LGPD), aims to guarantee protection to all citizens residing in Brazilian territory through transparent practices of companies during the data collection process. The research is descriptive with a qualitative approach. It was showed how the principles of good faith provided by law were mostly contemplated in the ticket system and in the company's data privacy policy, and what could be improved was pointed out. Through a case study, it was possible to describe the company's adequacy project using the main ticket opening system as a study tool, and to analyze its data privacy policy and the solutions adopted by the company. A survey of lessons learned by project members was also carried out.

Keywords: Data privacy, IT Governance, LGPD, Personal data, Data protection

IMPLANTAÇÃO DA LGPD E SEUS IMPACTOS EM UMA HOLDING DO SETOR DE MAQUINÁRIO PESADO

O estudo tem como objetivo descrever o projeto de adaptação de uma empresa multinacional do setor de produção de máquinas pesadas à LGPD. Aprovada em 2018, a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), visa garantir proteção a todos os cidadãos residentes em território brasileiro por meio de práticas transparentes das empresas durante o processo de coleta de dados. A pesquisa é descritiva com abordagem qualitativa. Constatou-se que os princípios da boa-fé previstos em lei foram contemplados majoritariamente no sistema de tickets e na política de privacidade de dados da empresa e foi apontado o que poderia ser aprimorado. Por meio de um estudo de caso foi possível descrever o projeto de adequação da empresa utilizando o principal sistema de abertura de tickets como ferramenta de estudo, assim como realizar a análise da sua política de privacidade de dados e das soluções adotadas pela empresa. Também foi realizado o levantamento das lições aprendidas pelos membros do projeto.

Palavras-chave: Privacidade de dados, Governança de TI, LGPD, Dados Pessoais, Proteção de dados

IMPLANTAÇÃO DA LGPD E SEUS IMPACTOS EM UMA *HOLDING* DO SETOR DE MAQUINÁRIO PESADO

Aprovada em 2018, a Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), visa garantir proteção a todos os cidadãos residentes em território brasileiro por meio de práticas transparentes das empresas durante o processo de coleta de dados. O estudo tem como objetivo descrever o projeto de adaptação de uma empresa multinacional do setor de produção de máquinas pesadas à LGPD. A pesquisa é descritiva com abordagem qualitativa. Por meio de um estudo de caso foi possível descrever o projeto de adequação da empresa utilizando o principal sistema de abertura de *tickets* como ferramenta de estudo, assim como realizar a análise da sua política de privacidade de dados e das soluções adotadas pela empresa. Constatou-se que os princípios da boa-fé previstos em lei foram contemplados majoritariamente no sistema de *tickets* e na política de privacidade de dados da empresa e foi apontado o que poderia ser aprimorado. Também foi realizado o levantamento das lições aprendidas pelos membros do projeto.

Palavras-chave: Privacidade de dados. Governança de TI. LGPD. Dados pessoais. Proteção de dados.

IMPLEMENTATION OF LGPD AND ITS IMPACTS ON A HOLDING COMPANY IN THE HEAVY MACHINERY SECTOR

Approved in 2018, the Law No. 13.709, known as the General Data Protection Law (LGPD), aims to guarantee protection to all citizens residing in Brazilian territory through transparent practices of companies during the data collection process. This research aims to describe the adaptation project of a multinational company from the heavy machinery production sector to the LGPD. The research is descriptive with a qualitative approach. Through a case study, it was possible to describe the company's adequacy project using the main ticket opening system as a study tool, and to analyze its data privacy policy and the solutions adopted by the company. It was showed how the principles of good faith provided by law were mostly contemplated in the ticket system and in the company's data privacy policy, and what could be improved was pointed out. A survey of lessons learned by project members was also carried out.

Keywords: Data privacy. IT Governance. LGPD. Personal data. Data protection.

1 INTRODUÇÃO

A informação é hoje um dos ativos mais valorizados das empresas que a utilizam na busca de melhor produtividade, redução de custos, ganho de espaço no mercado (*market share*) e de lucratividade. De um supermercado a uma empresa multinacional, a informação é essencial nos processos de tomada de decisão e está presente em todos os processos e setores de uma empresa.

Há a necessidade de realizar a gestão de um ativo que é intangível, a própria informação. Segundo Sêmola (2014):

> A primeira década do século XXI tornou-se pródiga em expressões e aplicações comerciais que passaram a utilizar-se da moderna infraestrutura de rede e computacional como *business-to-business*, *business-to-consumer*, *business-to-government*, *e-commerce*, *e-procurement*, e os sistemas integrados de gestão ERP (*Enterprise Resource Planning*), que prometiam melhor organização dos processos de negócio, e passaram a representar um dos principais pilares de sustentação da empresa [...]. (Sêmola, 2014, pg. 4).

Com o passar do tempo vê-se que as empresas reconhecem a importância da informação, seja ela digitalizada, compartilhada ou distribuída, para fornecer seus serviços personalizados aos consumidores finais. Devido ao aumento crescente dessa dependência, em 2012 a Comissão Europeia definiu planos para uma reforma na proteção de dados com o *General Data Protection Regulation* (GDPR), uma regulamentação (em tradução livre, GDPR significa "Regulamento Geral sobre Privacidade de Dados") que tem por objetivo dar aos cidadãos e residentes de países europeus formas de controlar seus dados pessoais armazenados em bancos de dados nas organizações empresariais.

O GDPR entrou em vigor em 25 de maio de 2018 e, desde então, outros países adotaram estratégias semelhantes. Em 14 de agosto de 2018, foi sancionada no Brasil a Lei nº 13.709, Lei Geral de Proteção de Dados (LGPD), segundo a qual todas as empresas presentes em solo nacional que tratem dados pessoais, sejam elas sediadas dentro ou fora do país, devem atender uma série de requisitos a fim de garantir as principais exigências previstas pelos artigos da lei para maior proteção dos usuários. A LGPD possuía previsão para entrar em vigor em agosto de 2020, porém com a crise provocada pela pandemia mundial de COVID-19, o Senado aprovou a o Projeto de Lei nº 1.179/2020 que adiou o início da vigência para janeiro de 2021.

A LGPD não descreve o que deve ser feito e somente define os objetivos a serem cumpridos pelas empresas. Diante disso, as organizações devem encontrar os meios e maneiras que melhor se adequam ao seu cenário, desde que estes sejam legais para realizar a implementação da lei em seus ambientes. Porém, por não ser definido, o processo de implementação da LGPD em uma organização levanta inúmeras questões sobre como isto deve ser realizado.

A empresa Duosun (nome fictício) é uma multinacional do setor de produção de maquinário pesado. A empresa conta com um quadro de funcionários global de 64,4 mil pessoas em suas unidades que, por sua vez, possuem gestão descentralizada para agilidade nos processos de tomada de decisão, além de um escopo de 2217 sistemas ativos globalmente, dentre estes, aproximadamente 200 sistemas estão em atuação no Brasil e na Argentina. A adequação à lei é vista como um grande desafio internamente, visto o número elevado de sistemas e funcionários, localizações e legislações distintas, descentralização de atividades, orçamento, bem como a árdua interpretação dos pormenores da lei.

Diante deste cenário, este estudo tem como objetivo geral analisar o projeto de adequação à LGPD da multinacional do setor de produção de maquinário pesado. Os objetivos específicos deste estudo são: identificar na política de segurança da empresa as principais mudanças para adequação da lei; compreender quais foram as principais ações desencadeadas

para adequação do principal sistema de abertura de *tickets* da empresa; e detalhar os problemas e dificuldades enfrentados para adequar a empresa à LGPD.

Como o processo de adequação é recente e tem-se poucos relatos sobre como as empresas tem lidado com ele, espera-se que o estudo contribua para auxiliar outras organizações a se adequarem à nova legislação.

2 REFERENCIAL TEÓRICO

Tem-se que "dado é qualquer elemento identificado em sua forma bruta que, por si só, não conduz a compreensão de determinado fato ou situação" (Oliveira, 2006, p. 24). Partindo dessa afirmação, define-se como sendo um dado, qualquer registro ou indício que pode ser relacionado a algum evento ou entidade. É importante ressaltar que um dado é uma informação bruta e que ainda não foi processada ou, como destaca Davenport, "dados são observações do mundo" ou "entidades quantificáveis" (Davenport, 1998, p.19).

Define-se então que "informação é o dado trabalhado que permite ao executivo tomar uma decisão" (Oliveira, 2006, p. 24). A informação então, é um conjunto de dados que faça sentido para um ser humano permitindo que ele consiga entender suas relações e realizar comparações neste conjunto. Mas, além disso, "a informação precisa de análise" (Davenport, 1998, p. 20), ou seja, precisa que as pessoas façam o processo de transformar dados em informações atribuindo sentido e significado.

Atualmente a coleta de dados dos clientes, por exemplo, não se limita apenas ao escopo de seus dados pessoas, tais como nome e endereço dentre outros. As empresas também coletam dados comportamentais de seus usuários. Para Zuboff (2020), inicialmente os dados comportamentais eram utilizados a favor dos usuários, porque eram empregados para aperfeiçoar a oferta de serviços e elaborar novos produtos. A autora dá a essa fase o nome de ciclo de reinvestimento do valor comportamental. No contexto do chamado capitalismo de vigilância, ela destaca que os novos produtos são derivados do comportamento dos usuários. Desta maneira, a captura dos dados comportamentais permite a criação de produtos que "estão relacionados a predizer sobre nós sem de fato se importar com o que fazemos ou o que é feito a nós" (Zuboff, 2020, p.88).

Parte significativa dos dados comportamentais é adquirida por meio da utilização de um pacote de dados denominado *cookie*. *Cookies* são informações coletadas quando se visita um *website*, tais como local e idioma da página, para quando houver um novo acesso, ela esteja de forma personalizada para cada usuário. Contudo, estes *cookies* também podem armazenar informações altamente sensíveis, como nome, endereço, e-mail, CPF ou telefone (caso fornecidos previamente, como em cadastros em *e-commerces*, por exemplo).

Nesse contexto a gestão dos dados e informações de uma empresa exige novas responsabilidades. Para Sêmola (2014), o ciclo de vida da informação possui quatro estágios, sendo eles:

- **Manuseio:** estágio de criação e manipulação da informação;
- **Armazenamento:** estágio em que a informação é armazenada, desde *pen-drives* até a *data centers* gigantescos usados pelas empresas que detém a maior parte do mercado;
- **Transporte:** estágio em que a informação é transportada, como por exemplo, ao enviar um e-mail para cadastro de um novo concessionário em um sistema de vendas;
- **Descarte:** estágio em que a informação é descartada pela empresa.

Para Sêmola (2014), todas as etapas acima são sustentadas quando os ativos de uma empresa - tecnológicos ou humanos - fazem uso da informação sustentando seus processos que, por sua vez, mantém a empresa em funcionamento. É importante notar que Sêmola conceitua a

informação quase como um sinônimo de dado, e para os fins deste estudo, o ciclo de vida da informação retratado no parágrafo anterior deve ser entendido como um ciclo de vida do dado.

2.1 Legislação antecedente à Lei Geral de Proteção de Dados

Apesar da LGPD ser uma lei recente, o assunto de proteção de dados é antigo no Brasil, presente em leis setoriais que serão incrementadas com a vigência da nova lei. Estas leis setoriais englobam principalmente a confirmação da existência do tratamento de informações pessoais; acesso aos dados por parte do usuário; e a correção de dados desatualizados. Como exemplo, pode-se citar a lei nº. 12.527/2011 – Lei de Acesso à Informação (LAI), que trata do acesso às informações públicas e direcionada somente a entidades públicas, que visa garantir uma gestão segura, transparente e íntegra da informação pessoal, propiciando amplo acesso a ela e sua divulgação através de uma linguagem clara e de fácil compreensão através da internet (Soares, Jardim e Hermont, 2013).

Outra lei presente em território nacional, é de nº 12.737/2012, apelidada de Lei Carolina Dieckmann devido ao escândalo envolvendo a divulgação em larga escala de imagens íntimas da referida atriz na internet. Ela provocou a alteração no Código Penal para tipificação dos crimes cibernéticos propriamente ditos, tal como a invasão de dispositivos pessoais visando utilizar seu conteúdo para denegrir ou chantagear alguém. Outra novidade da lei foi a equiparação de cartões de crédito e débito com documentos particulares, transformando-os em objetos de crime de falsidade ideológica (São Paulo, 2012).

Por último, o Brasil também possui a lei nº 12.965/2014, intitulada de Marco Civil da Internet, que estabelece diretrizes para o uso da internet em solo brasileiro e tem como objetivo central, regulamentar a relação entre as empresas operadoras de serviços de internet e os seus respectivos clientes. (Brasil, 2014). O princípio de neutralidade da rede, presente no Marco Civil da Internet, visa garantir que as empresas provedoras de acesso não pratiquem ações abusivas na prestação de seus serviços e proporciona um tratamento igualitário entre todos os seus clientes, sem distinção de origem, destino, serviço, conteúdo ou dispositivo (computador ou aparelho celular).

Como alertam Bezerra e Waltz (2014), apesar da privacidade e da intimidade serem considerados direitos fundamentais presentes na Declaração Universal dos Direitos Humanos e na Constituição Federal de 1988, o uso das tecnologias digitais implicou numa gradual restrição à proteção desses direitos, pois

> O fluxo e o armazenamento de comunicações e informações pessoais na rede abrem brechas à vigilância estatal indevida, uso impróprio de dados de clientes por empresas, ataque de *hackers* a *data centers* e a dispositivos pessoais, vazamento de informações sigilosas por pessoas mal-intencionadas a fim de denegrir a imagem de terceiros, entre outros (Bezerra e Waltz, 2014, p.162).

Se por um lado o Marco Civil também regulamenta a privacidade na internet, garantindo a inviolabilidade das comunicações dos usuários, atribuindo o dever de sigilo das informações de cada usuário ao seu provedor de internet. (CHC Advocacia, 2019). Por outro, segundo Thompson (2012), não permite a responsabilização dos "provedores de serviço que ajam com negligência - ou até mesmo com malícia – na manutenção de conteúdo de cuja existência têm ciência [...], senão pelo descumprimento de ordem judicial extemporânea e, muitas vezes, jurisdicionalmente distante", o que acaba por não contribuir para a promoção de boas práticas de direito (Thompson, 2012, p.214).

2.2 Lei Geral de Proteção de Dados

Neste cenário surge então a Lei Geral de Proteção de Dados (LGPD) brasileira, visando a conformidade das empresas atuantes em solo nacional, sejam suas matrizes sediadas dentro ou fora do país. Se uma empresa realiza processamento de dados de brasileiros ou não-brasileiros residentes no país, ela deve estar de acordo com lei nº 13.709.

A LGPD tem como objetivo trazer proteção à privacidade da informação pessoal do usuário através de práticas transparentes e seguras pelas empresas. A lei também padroniza as regras sobre tratamento de dados pessoais para todos os agentes que realizam coleta de dados para fins jornalísticos, artísticos ou para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação penal, conforme art. 4º (Brasil, 2018).

Para entender a LGPD, é necessário primeiro definir o conceito de dados pessoais. De acordo com o art. 5º da lei nº 13.709, tem-se:

> I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...]. (Brasil, 2018).

De acordo com a *European Comission* e, para comparação, o GDPR define como dado pessoal sensível qualquer dado que possua:

- Dado pessoal revelando origem étnica ou racial, opiniões políticas, religiosas ou filosóficas;
- Filiação sindical;
- Dados genéticos ou biométricos tratados exclusivamente para identificar um ser humano;
- Dados relacionados à saúde de um ser humano;
- Dados relativos à vida sexual ou orientação sexual de um ser humano. (European Comission, 2016).

Assim como explicado no tópico anterior, dados pessoais isolados também não são significativos, e sim a informação pessoal aplicada em um contexto. Isolados, os dados podem fornecer somente a geolocalização de um comprador de *e-commerce*, porém, quando em conjunto, como uma lista de nomes, cidade e opinião política, podem se tornar uma ferramenta muito poderosa. Um exemplo foi o ocorrido durante as eleições presidenciais norte-americanas no escândalo da empresa britânica *Cambridge Analytica*, que usou a informação pessoal do *Facebook* como meio para atingir os usuários com a campanha do então candidato, posteriormente eleito, Donald J. Trump (Confessore, 2018). A informação pessoal fornecida em simples cadastros de uma rede social, adquirida por meio de *cookies*, pode ser crucial para definir o que o usuário final vai ler, ver, ouvir e/ou comprar.

O art. 6º da LGPD define os princípios de boa-fé para atividades de coleta de dados em solo nacional, sendo estes:

> 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. [..]. (Brasil, 2018).

Percebe-se que a LGPD tem grande impacto em relações comerciais e de consumo que demandam coleta de dados, principalmente para empresas que coletam informações pessoais de clientes/consumidores para traçarem perfil de pagador, visando hábitos de consumo e condições financeiras.

Porém, é importante pontuar que até mesmo as relações trabalhistas irão sofrer alterações com a nova lei. Embora a LGPD autorize que as empresas usem os dados pessoais dos seus empregados para execução de contratos em prol do trabalhador, também será preciso estar atento à LGPD para os atos praticados durante a vigência do contrato e nas rescisões. Para as terceirizações de serviços, será necessário obter consentimento do trabalhador para fornecer suas informações pessoais a outra empresa, conforme visto no art. 7º (Brasil, 2018).

A LGPD visa garantir que não só a internet seja um local seguro para navegação, abrangendo também os bancos de dados e aplicações responsáveis por armazenar as informações pessoais de todas as pessoas, garantindo que eles possuam segurança independentemente de serem provedores de internet ou não.

Fortemente inspirada na sua contraparte europeia, o GDPR, a lei brasileira possui diferenças e semelhanças, não sendo somente uma tradução literal da lei europeia. De acordo com Alleasy (2020), alguns dos principais pontos são:

- **Âmbito territorial:** Tanto a LGPD quanto a GDPR são semelhantes neste ponto e "são aplicáveis a todas as empresas que prestam serviços a cidadãos localizados na União Europeia ou no Brasil, independentemente de onde estejam localizadas", sendo a LGPD ainda mais abrangente em relação a aplicabilidade dos dados coletados em solo nacional.
- **Sanções:** As sanções aplicadas tanto pela lei quanto pelo regulamento seguem a mesma abordagem. O GDPR determina que, em caso de incidente de violação de dados, a empresa pode ser multada entre 10 a 20 milhões de euros ou de 2% a 4% do faturamento anual total, o que for maior. Já a LGPD, define que as empresas poderão ser multadas em 2% do faturamento total, mas limitado até 50 milhões de reais.
- **Solicitação do acesso pelos titulares:** ambas garantem o acesso aos dados coletados pelas empresas pelos seus titulares, diferindo apenas no prazo que as empresas possuem para responder as solicitações: no GDPR são 30 dias, enquanto a lei brasileira oferece apenas 15 dias.

Então, apesar de existirem muitos pontos semelhantes entre as duas leis, há também muitos outros pontos em que há diferenças notórias, sendo importante ressaltar que o GDPR é apenas um regulamento e é mais objetivo em seus termos. Enquanto isso, por outro lado a LGPD é uma lei federal, tendo cláusulas abertas e subjetivas, permitindo interpretações diferentes em alguns pontos que deverão ser consolidados pela jurisprudência e consolidados

pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD) quando finalizado seu processo de formação.

2.3 *Compliance,* Governança de TI e Governança de Dados

Segundo Assi (2013, p.19), "*compliance* é a ferramenta da governança corporativa, no que se refere a sistemas, processos, regras e procedimentos adotados para gerenciar os negócios da instituição [...]". Ainda, uma empresa estar em *compliance* é estar em conformidade com leis e regulamentos além do dever de cada colaborador dentro dela (Assi, 2013). Conclui-se então que o *compliance* é o cumprimento de leis externas e internas, políticas e procedimentos, objetivando mitigar riscos e falhas inerentes à atividade da empresa.

A governança de TI é "a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização da TI" (Weill e Ross, 2006, p.31). Pode-se dizer então que é um ramo da governança corporativa que atua como uma ferramenta de controle da tecnologia de informação, estabelecendo políticas e regras que direcionam os processos de TI. O monitoramento dessas normas garante que a TI do negócio esteja fazendo o que é necessário para alcançar os objetivos estratégicos da organização, diminuindo as chances de riscos ao negócio (Corrêa, 2018). É extremamente importante que uma organização esteja alinhada com seus processos de TI, estando em constante inovação tecnológica.

A governança de TI é vista como um diferencial competitivo no mercado, pois pode trazer bons resultados, expandindo as possibilidades de negócio da empresa através da tecnologia, tornando-a mais atraente ao mercado. Entre os mais famosos *frameworks* da governança de TI destaca-se o uso das principais, *Control Objectives for Information and Related Technology* (COBIT) e *Information Technology Infrastructure Library* (ITIL). O modelo corporativo de Governança do COBIT 5 traz a seguinte definição de governança de TI:

> A governança garante que as necessidades, condições e opções das Partes Interessadas sejam avaliadas a fim de determinar objetivos corporativos acordados e equilibrados; definindo a direção através de priorizações e tomadas de decisão; e monitorando o desempenho e a conformidade com a direção e os objetivos estabelecidos. (ISACA, 2012).

Essa relação entre governança de TI e processos de tomadas de decisão (governança corporativa), surge quando os processos físicos se tornam digitais e a TI deixa de ser apenas a provedora de serviços e soluções tornando-se um parceiro de negócio da organização. A companhia que tiver uma boa gestão da governança de TI, possuindo meios otimizados de gerenciar e controlar seus ativos informacionais, terá uma maior facilidade na adequação de seus processos à LGPD.

Por sua vez, governança de dados é a parte da governança responsável por gerenciar o controle de dados e informações de uma organização. A Governança de Dados "É um conceito em evolução, que envolve o cruzamento de diversas disciplinas, com foco em qualidade de dados, passando por avaliação, gerência, melhoria, monitoração de seu uso, além de aspectos de segurança e privacidade associados a eles" (Barbieri, 2013, p.7).

A governança de dados, além de atuar nas normas, padrões e controles de acessos de uma organização, atua também como uma visão apurada sobre os dados estratégicos da mesma, definindo e analisando todos os processos que produzem e se alimentam destes dados (Rêgo, 2013). Ainda segundo Rêgo, a governança de dados é vista como uma das mais importantes funções de gestão de dados e existem diversos *frameworks* e modelos de maturidade disponíveis no mercado.

Observa-se então, conceitos fortemente pertinentes à LGPD, já que são ferramentas de controle da TI de uma empresa, para garantir a conformidade em os processos que tratem

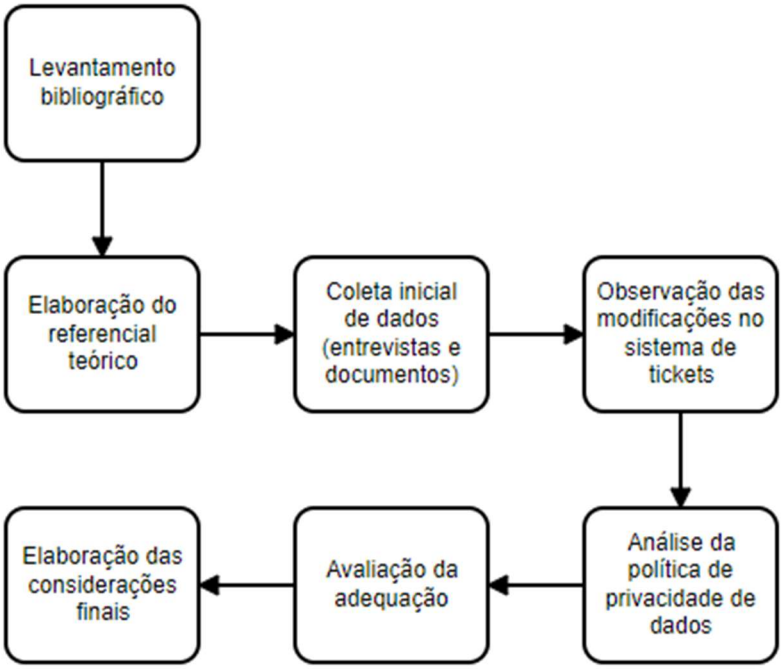
informações pessoais, evitando assim, possíveis sanções administrativas previstas pela lei em seu capítulo VIII, art. 52.

3 PROCEDIMENTOS METODOLÓGICOS

A pesquisa é do tipo descritiva com uma abordagem qualitativa. O método utilizado para o desenvolvimento deste estudo foi o estudo de caso. O estudo de caso "é o tipo de pesquisa cujo procedimento volta-se para um caso específico com o objetivo de conhecer suas causas de modo abrangente e completo" (Carvalho et al., 2019, p.44). Também foi utilizada a observação participante pelo fato de um dos pesquisadores estar presente no dia a dia dos envolvidos na adequação do projeto e utilizar o sistema estudado como ferramenta principal de trabalho.

Atendo-se ao fato de que este é um assunto muito recente, em maio de 2021, foi feito um levantamento bibliográfico no Portal de Periódicos CAPES, com as palavras-chave "adequação LGPD", e foram obtidos somente 9 resultados. Dentre estes 9 resultados, 6 referiam-se a estudos pertencentes à área de Direito. Os estudos restantes referiam-se à área de tecnologia, mas não são pertinentes à proposta deste estudo. A partir daí foi elaborado o referencial teórico. A Figura 1 ilustra o percurso metodológico adotado.

Figura 1 – Percurso metodológico do estudo de caso



Fonte: Elaborado pelos autores.

Para a coleta inicial de dados, foram realizadas duas entrevistas virtuais não-estruturadas em julho/2020, através da plataforma de comunicação da empresa, o *Microsoft Teams*. A primeira entrevista foi realizada com o gestor do time de *Access Management* e a segunda, com um analista do time *CyberSecurity*, responsável pela realização da adequação no âmbito da América Latina. Elas visaram o entendimento geral do projeto realizado pela empresa, quem são os envolvidos diretamente no mesmo, quais são suas funções e, também, entender quais dificuldades estão sendo enfrentadas para uma mudança tão grande quanto a que é solicitada pela lei.

Através da observação-participativa foi possível observar o ambiente de trabalho com uma nova percepção, a fim de entender melhor o impacto da lei para os empregados que trabalham diretamente com o atendimento de *tickets* e avaliar como o principal sistema de *tickets* foi alterado para atender aos requisitos da lei.

O estudo também fez uso da análise documental da política de privacidade da empresa para comparação com os princípios de boa-fé previstos na lei, para verificar como a empresa se preparou para atender à adequação. Outros documentos utilizados foram: diretrizes para acessos a sistemas internos, diretrizes para dados armazenados em dispositivos corporativos e a política de segurança interna.

Foram realizadas novas entrevistas com o gestor do time de *Access Management* e com o analista do time *CyberSecurity* em maio/2021, após a adequação do sistema de *tickets*, também através da plataforma de comunicação da empresa (*Microsoft Teams*), para entender do ponto de vista gerencial, os desafios enfrentados e lições aprendidas durante o projeto de adequação até o presente momento.

4 APRESENTAÇÃO E ANÁLISE DOS DADOS

Nesta seção são apresentadas as análises dos dados obtidos durante a observação do projeto de adequação da empresa à LGPD, tais como os requisitos e a análise da política de privacidade de dados.

4.1. Caracterização da organização

Este estudo foi desenvolvido em uma organização multinacional presente em 180 países onde atua, por meio de suas marcas, na produção de máquinas agrícolas, equipamentos de construção, veículos especiais e comerciais, motores, eixos, transmissões e serviços de pós-venda e financiamento.

O principal sistema de gestão integrado *(Enterprise Resource Planning* – ERP), que permite acesso fácil, integrado e confiável aos dados da empresa, é o *SAP*[1]. Ele engloba a maior parte dos processos centrais desde movimentação de peças de estoque e compras no centro de custo até contas a receber e expedição de máquinas. Para que todos os fluxos tenham seu funcionamento normal, a empresa possui um alto número de sistemas, além do ERP, visando atender subprocessos, gerando uma redundância alta de dados, pois os usuários precisam ter seus acessos criados em cada aplicação. Um destes sistemas é a principal ferramenta de abertura de *tickets* na empresa, objeto de análise do estudo.

4.2. A gestão de usuários de sistemas

A gestão dos usuários em aplicações geradas pela área de sistemas é realizada por um único departamento de *Access Management* seguindo a matriz *segregation of duties*[2] (SOD) visando a liberação de permissões pertinentes à área do usuário final durante o atendimento de um *ticket*. Este atendimento só ocorre mediante a aprovação do titular da área, sinalizando que o usuário está autorizado a receber as permissões solicitadas.

[1] SAP que vem do alemão *Systeme, Anwendungen und Produkte in der Datenverarbeitung*, podendo ser traduzido como Sistemas, Aplicativos e Produtos para Processamento de Dados.

[2] Os mecanismos de segregação de funções (SoD) são projetados para gerenciar relacionamentos conflitantes entre determinadas entidades de modelo. (IBM, 2021).

O time de *Access Management* possui diversos processos auditados internamente, e externamente, por auditores contratados, que visam garantir a segurança dos dados de usuários cadastrados nos sistemas. Dentre esses processos, existem alguns que são realizados mensalmente, como a verificação do centro de custo de um usuário a fim de garantir a conformidade dos acessos por área, até o desligamento dos usuários, realizado semanalmente, de acordo com a política de segurança interna da empresa.

Estes pontos ajudam na construção de um cenário favorável para implantação da LGPD na empresa, mostrando que a empresa possui diversos processos críticos mapeados com rotinas bem definidas. Porém em contrapartida, a gestão dos usuários em aplicações geridas pela área de negócios não possui atuação do time *Access Management*, o que cria um obstáculo por estes sistemas não possuírem um controle centralizado.

A cultura da empresa de possuir uma gestão descentralizada é vista como um dos maiores desafios para o sucesso do projeto de implantação, pois somente em território nacional a empresa totaliza mais de 500 processos e cerca de 30 setores de trabalho distintos. Destes processos, muitos são somente rotina local dos times e não possuem documentação como rotinas de execução ou listas de usuários, enquanto os demais possuem políticas internas e procedimentos detalhados para execuções, sendo estes aprovados pelos responsáveis locais e globais da área antes da implantação do sistema.

Outro fator extremamente importante que compõe o cenário da empresa no que diz respeito às aplicações, é que dentre os sistemas utilizados no Brasil, existem alguns sistemas *web* que são usados por agentes externos à empresa, como *dealers* ou fornecedores de serviços, contendo bases de informações de clientes e produtos da empresa. Cada área da empresa pode realizar a contratação de agentes externos para realização de diversos serviços, com consultorias, auditorias, manutenções ou serviços de propaganda.

Conforme já exposto, o sistema de abertura de *tickets* usado pelo time *Access Management* é o objeto de avaliação e análise dos dados. Este sistema é uma centralização de todas as solicitações referentes aos mais de 100 sistemas que estão na gestão do time de *Access* Management. Seu funcionamento se dá da seguinte forma:

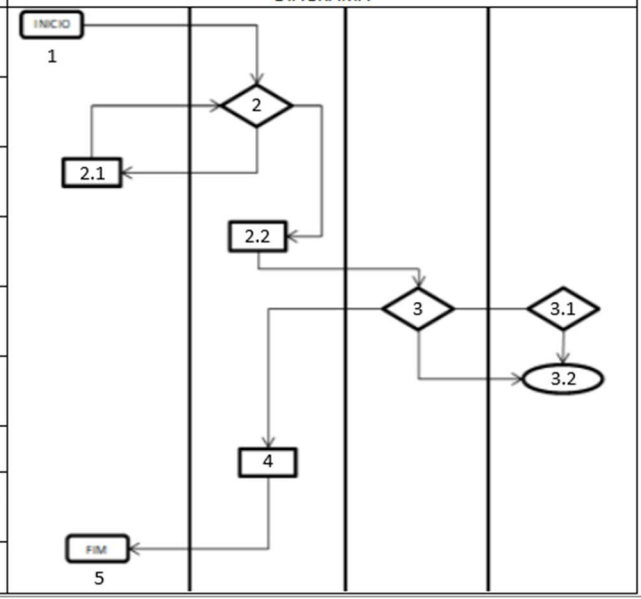
1. O solicitante realiza a abertura de um *ticket* na seção referente ao sistema final desejado e utiliza a aba de usuário beneficiado para informar seu ID de rede ou CPF (caso seja usuário externo) e o sistema de *tickets* realiza o preenchimento automático dos dados do cadastro.
2. Na abertura do *ticket*, o solicitante deve informar também qual o perfil de acesso deseja ter no sistema final, sendo este campo a variável que irá definir a permissão do usuário ao final do atendimento.
3. Um analista do time de *Access Management* avalia se a solicitação foi realizada da forma correta e certifica que os dados são satisfatórios para o prosseguimento do *ticket*. Caso não seja, o analista retorna o *ticket* para o solicitante e aguarda o retorno (este retorno é feito de forma automática pelo sistema em 3 dias úteis mesmo quando não houver resposta).
4. Se o preenchimento do *ticket* estiver correto, o analista realiza o envio da solicitação para aprovação do gestor do solicitante caso seja funcionário interno da empresa, ou seu representante caso seja usuário externo. Após a aprovação do gestor ou representante, o *ticket* transita automaticamente para o status de aguardando aprovação do responsável pelo perfil de acesso solicitado no momento de abertura do *ticket*, sendo esta aprovação realizada pelo responsável da área solicitada.
5. Caso todas as aprovações sejam realizadas, o *ticket* chega na fase final da liberação do acesso e retorna para a atuação do time *Access Management*. O

usuário então recebe um e-mail automático do sistema informando que seu acesso foi criado e a senha para o primeiro *login*.

Adicionalmente a este processo, quando um usuário externo realiza a abertura de um *ticket* pela primeira vez, é realizada também a criação de um ID genérico ao final do *ticket*, semelhante ao ID de um usuário interno, para que o cadastro em todos os sistemas que serão utilizados seja padronizado, evitando o uso de CPFs como credenciais de acesso nos sistemas internos. Após a criação, o cadastro do usuário no sistema de *tickets* também é alterado para que em futuras solicitações o CPF não seja reutilizado na abertura de novos *tickets*. A figura 2 ilustra o fluxo do sistema.

Figura 2 - Fluxograma da abertura de tickets

Nº	ETAPA
1	Usuário realiza abertura do *ticket*.
2	Time de *Access Management* valida a solicitação.
2.1	Solicitação incorreta, *ticket* aguardando retorno do solicitante.
2.2	Solicitação correta, *ticket* enviado para aprovações necessárias.
3	Aprovação do responsável do usuário. Caso não haja, é cancelado.
3.1	Acesso não aprovado em algum nível, logo é encerrado sem liberação.
3.2	Cancelado por falta de aprovação.
4	Aprovações realizadas, chamado retorna para execução do time de *Access Management*.
5	Usuário beneficiado recebe os acessos.



Fonte: Dados do projeto da empresa Duosun.

4.3. Planejamento do projeto

O projeto na organização teve início na Europa por se tratar de uma multinacional com sede na Itália. A empresa está sob o escopo de atuação tanto da LGPD quanto da GDPR. A empresa elegeu um DPO (*Data Protection Officer*) global para estes temas. Um DPO "é uma pessoa que tem a tarefa formal de garantir que a organização esteja ciente e cumpra suas responsabilidades e obrigações de proteção de dados de acordo com o GDPR e as leis do Estado-Membro." (Besemer, 2018, p.12).

Este DPO visitou cada localidade da organização que possui processos envolvendo dados de usuários. Também realizou diversas reuniões com os líderes de áreas para que pudesse ser eleita uma equipe local de analistas tanto de *business* quanto de TI que estivesse encarregada exclusivamente de acompanhar o andamento das atividades na localidade e enviar relatórios do progresso feito.

Com a ramificação da equipe completa, o departamento jurídico pôde atuar na interpretação da lei de forma clara a todos os líderes de áreas por meio de treinamentos que tinham por objetivo esclarecer todos os pontos da lei. Houve também o esclarecimento de alguns conceitos-chave, como dados e informações pessoais.

O DPO repassou as diretrizes do projeto tanto com o time global quanto com o time da América Latina, dando instruções sobre como começar o projeto de adequação e realizando o acompanhamento dos levantamentos junto a ambos os times. Conforme explicado

anteriormente, a LGPD diz o que fazer, mas não dita como estas mudanças devem ser realizadas pelas empresas.

O departamento de *compliance* foi atuante nesta fase visando identificar e mitigar possíveis riscos e áreas de vulnerabilidade da organização.

A primeira mudança surgiu do questionamento de "quais sistemas terão que mudar?". Esta pergunta não podia ser respondida prontamente, pois o time responsável pela atuação na América Latina não possuía uma lista contendo todos os sistemas e suas especificações. Então o primeiro impacto do projeto foi a criação de um portfólio de sistemas para a empresa, onde todos os sistemas estão sendo cadastrados conforme sua política de coleta de dados.

O time responsável passou então a realizar o levantamento de sistemas que tratam os dados pessoais por área, ou seja, tanto os sistemas que possuem gestão do time *Access Management* quanto os sistemas que são gerenciados pelo *business* estão no escopo de atuação do time local do projeto. Esta fase foi considerada a mais crítica, pois caso o levantamento dos sistemas fosse realizado de maneira incorreta, uma falha futura seria quase certa o que acarretaria encargos milionários para a organização.

O cadastro neste portfólio é feito em etapas, nas quais os líderes dos sistemas devem indicar se o sistema realiza algum tipo de coleta de dados do usuário, e caso a opção seja "sim", é necessário explicar detalhadamente os tipos de dados coletados, a forma de coleta dos mesmos e qual o tratamento dado a estes dados (Ficam alocados? Se sim, onde? Localmente ou em nuvem?).

Durante esta etapa, o time local sugeriu algumas soluções potenciais para a implantação da lei na empresa:

- Se o sistema é gerenciado por um fornecedor, seria necessário a criação de um termo onde o fornecedor se compromete a dividir a gestão dos usuários da empresa com o time responsável pela criação dos acessos;
- Para os sistemas que utilizam coleta de dados pessoais, a criação de um aviso solicitando o consentimento do usuário ao usar o sistema, explicando qual *cookie* está sendo utilizado e em qual nível está sendo realizada a coleta dos dados.

O projeto ainda está em fase de planejamento e esbarrou no maior desafio atualmente, o orçamento. Conforme demonstrado na seção 4.2, a cultura de gestão descentralizada da empresa faz com que o orçamento das áreas seja individual e o projeto de implantação da LGPD precisa concorrer com outros gastos do setor, fazendo com que a aquisição de nova verba se torne um processo dificultoso pois é necessário que toda a diretoria global esteja envolvida na aprovação.

O projeto também gera impactos para o futuro da empresa, pois todas as soluções que estavam em desenvolvimento passaram a contar com o time local do DPO no processo de desenvolvimento, para que todo novo sistema seja desenhado visando a legislação futura, mitigando o risco de uma eventual falha em auditorias do assunto.

A empresa possui comunicações frequentes aos usuários sobre o tema, fazendo com que a lei seja algo presente no dia a dia dos seus empregados e buscando inserir a proteção dos dados na cultura profissional.

Após diversas reuniões entre o time global e o time jurídico do Brasil, foram definidos os requisitos para a adequação de cada sistema da empresa à lei, sendo eles:

- Limitação de tempo;
- Gerenciamento de conta de usuário;
- Gerenciamento de log;
- Minimização dos dados;
- Visibilidade de dados pessoais (direitos de acesso do usuário);
- Gerenciamento de violação de dados pessoais;
- Rastreamento de coleta de dados;

- Criptografia de dados pessoais em repouso;
- Criptografia de dados pessoais em trânsito;
- Visibilidade de dados pessoais.

Então cada sistema foi avaliado individualmente para definir quais requisitos seriam contemplados para atingir os requisitos da adequação e para que os responsáveis realizassem os ajustes necessários. Para o sistema de *tickets* foram definidos os requisitos de limitação de tempo, gerenciamento de *log* e minimização dos dados para adequação, já que o sistema se encontrava em conformidade com os demais requisitos propostos no projeto. No Quadro 1 são apresentados os requisitos escolhidos e a principal ação relacionada à sua adequação.

Quadro 1 - Requisitos para adequação à LGPD

REQUISITOS	DESCRIÇÃO	AÇÃO
Limitação de tempo	Para aplicações que gerenciam dados pessoais para fins comerciais, disponibilizar procedimento manual ou automático para gerenciar os dados após o tempo de retenção.	Definição do tempo de permanência de dados pessoais na base de dados do sistema.
Gerenciamento de *log*	Para registros retidos por mais de 5 anos que contenham dados pessoais, defina e implemente um procedimento para anonimização.	Anonimização completa dos dados pessoais na base de dados após o tempo.
Minimização dos dados	Os dados pessoais devem ser adequados, relevantes e limitados ao necessário em relação aos fins para os quais são processados.	Coleta de dados relevantes para abertura de tickets.

Fonte: Projeto de adequação da empresa Duosun.

Por meio do requisito de limitação de tempo, definiu-se que o tempo máximo para a permanência dos dados pessoais de um usuário na base do sistema de *tickets* será de 5 anos, e após este período os dados deverão ser tratados pelo sistema através de uma política de anonimização dos dados pessoais. Os procedimentos para as tratativas ao final do tempo de retenção foram definidos pelo time global através de diretrizes do projeto de adequação e são:

- Eliminação dos dados pessoais – Os dados pessoais serão completamente apagados do aplicativo/sistema;
- Anonimização dos dados pessoais – Os dados pessoais não são apagados, mas convenientemente modificados, tornando possível a identificação do titular dos dados;
- Extensão do tempo de processamento permitido (por exemplo, renovação de consentimento) – A limitação de tempo é prolongada iniciando, com antecedência, uma campanha de renovação do titular dos dados, para tratamento de dados;
- Pseudonimização dos dados pessoais – Os dados pessoais não serão apagados, mas já não podem ser atribuídos a um determinado titular dos dados sem a utilização de informações adicionais.

O requisito de gerenciamento de *log* especifica que o registro do dado pessoal que fica armazenado na base do sistema de *tickets*. Definiu-se que, se um cadastro de usuário não fizer movimentação no sistema (abertura de *tickets*, alteração de dados no cadastro *etc*) em 5 anos, o sistema deve ter uma rotina que realize a anonimização dos dados do usuário, mantendo somente o ID de usuário por ser um dado da empresa e que não pode ser relacionado a uma pessoa diretamente. Caso o *log* possua mais de 5 anos e requisitos especiais sejam identificados pelo negócio (por exemplo, questões legais, regulamentares, de segurança ou outros), estes vão ser avaliados individualmente pelo responsável global de segurança da informação.

Por sua vez, o requisito de minimização dos dados especifica que os dados coletados pelo sistema devem ser adequados, relevantes e limitados ao extremo em relação aos fins para

os quais são processados. Quaisquer dados pessoais gerenciados pelo sistema de *tickets* que não forem estritamente necessários para fins de processamento serão completamente removidos e o sistema também deve ser configurado para enviar/receber apenas o conjunto mínimo de dados.

4.4. Soluções adotadas para adequação

Em reuniões ocorridas no último trimestre de 2020 entre o time de *Access Management*, *Compliance* e o time de desenvolvimento, decidiu-se pela criação de um *script* que irá percorrer toda a base do sistema diariamente para verificar cadastros que não tiveram movimentação nos últimos 5 anos, conforme definição dos requisitos de limitação do tempo e gerenciamento de *log*. Este *script* tem a finalidade de anonimizar todos os campos que possuírem dados pessoais destes usuários. Os campos que serão anonimizados são: nome; e-mail; e Telefone/ramal (em processo de descontinuação, em virtude do uso da plataforma *Microsoft Teams*).

Quando o cadastro do usuário é atualizado, quaisquer *tickets* abertos em nome destes também sofrem alteração e possuem seus dados anonimizados de forma automática. Os *tickets* passarão a contar com a seguinte informação nos campos citados acima: “Anonimizado pela LGPD”.

A base de cadastros do sistema conta atualmente com mais de 25.000 usuários cadastrados e estima-se que cerca de 28% da base atual do sistema tenha seus dados anonimizados na primeira rotina, pois referem-se a usuários que foram desligados da empresa e ainda possuem cadastro no sistema, ainda que seja um cadastro inativo e não permita movimentação dos dados. O maior desafio neste primeiro momento é a performance do sistema, visto que a base de dados do sistema é extensa e o *script* precisa ser executado diariamente para validação dos cadastros.

O time de *Access Management* em conjunto com o time jurídico definiu que, caso a usabilidade do sistema seja muito impactada durante a execução do *script*, uma alternativa seria alterar o intervalo de execução de diário para mensal, e buscar usuários cujos cadastros não tiveram movimentação em 4 anos e 11 meses.

Para entrar em conformidade com o requisito de minimização dos dados, definiu-se que campos de preenchimento obrigatório presentes hoje no cadastro, serão completamente removidos do sistema. Tal ação serve para garantir que os únicos dados coletados sejam aqueles relevantes para atendimento dos *tickets*. Os campos removidos serão: local de trabalho; departamento; e centro de custo.

Outra solução adotada em virtude da lei foi a alteração da tela inicial do sistema, que é composta de *dashboards* pré-definidos aos usuários finais, sendo um deles informativo sobre o uso do sistema. Diante disso, houve também a atualização deste *dashboard* para informações pertinentes à adequação e à lei, tendo o principal ponto, informar aos usuários que o sistema não realiza mais a coleta de dados pessoais e que *tickets* abertos com CPF como credencial de acesso serão cancelados e o documento não será retido na base de dados do sistema.

4.5. Análise da aplicação da política de privacidade de dados no sistema de *tickets*

Buscou-se verificar se os princípios de boa-fé propostos no art. 6º da LGPD estão contemplados na política de privacidade de dados da empresa e se foram implementadas ações nesse sentido no sistema de *tickets* da empresa. O Quadro 2 apresenta os resultados identificados.

Quadro 2 – Relação dos princípios de boa-fé e a política de privacidade de dados

PRINCÍPIOS	POLÍTICA DE PRIVACIDADE DOS DADOS	AÇÕES IMPLEMENTADAS NO SISTEMA DE *TICKETS*
Finalidade	Parcialmente atendidos: "Os dados pessoais devem ser relevantes para o objetivo para o qual estão sendo usados e, até o limite necessário, deve ser preciso, completo e mantido atualizado."	O sistema de tickets não realiza mais o tratamento de dados pessoais após as soluções adotadas, atendo-se somente à coleta de dados pertencentes à empresa (usuário de rede, matrícula, telefone e e-mail corporativo).
Adequação		
Necessidade		
Qualidade dos dados		
Livre acesso	"Os dados pessoais devem ser mantidos em uma forma que permita a identificação dos titulares dos dados por não mais do que o tempo razoavelmente necessário para os objetivos para os quais os dados pessoais são processados. Isso inclui o arquivamento de dados pessoais relevantes para leis específicas ou necessários para proteger a empresa em caso de processos jurídicos."	A empresa realizou a criação de um portal *online* disponível ao público onde qualquer pessoa pode preencher um formulário e todos os seus dados retidos pela empresa, serão apagados.
Transparência	"Os dados pessoais devem ser coletados para fins especificados, explícitos e legítimos e processados de maneira justa e transparente, com o conhecimento ou consentimento prévio do titular dos dados."	O sistema possui um *dashboard* informativo em sua página principal noticiando que os usuários não devem abrir *tickets* informando o CPF como chave de acesso, e caso isto ocorra, o *ticket* será cancelado e o número do documento não ficará salvo na base de dados do sistema. Adicionalmente, o empregado assina um termo de consentimento juntamente ao RH no ato de sua contratação no caso de outros sistemas.
Segurança	"Os dados pessoais devem ser processados de uma maneira que garanta a segurança adequada de tais dados, incluindo uma proteção razoável contra processos não autorizados ou ilegais e contra perda acidentais, destruição ou danos usando-se as medidas técnicas ou organizacionais razoavelmente adequadas."	Apesar do sistema de *tickets* não realizar a coleta de dados pessoais após as soluções vistas na seção 4.4, estes princípios são cobertos através da restrição do acesso a base de dados do sistema somente ao time de *Access Management,* e a restrição do acesso aos servidores de produção e *backup* ao time de infraestrutura, sendo este acesso revalidado semestralmente.
Prevenção		
Não discriminação	Não informado na política.	Não é coberto pelo sistema de *tickets*.
Responsabilização e prestação de contas	Responsabilização parcialmente atendida: "Todas as funções que processam dados pessoas são responsáveis pela conformidade com as medidas e leis de proteção de dados aplicáveis e deve ser capaz de demonstrar conformidade." Prestação de contas não informada na política de privacidade de dados.	Não é coberto pelo sistema de *tickets* explicitamente, mas o time de *Access Management* é ponto focal de todas as demandas referentes ao sistema.

Fonte: Elaborado pelos autores com base na lei nº 13.709 e a política de privacidade de dados da Duosun.

A maior parte dos princípios de boa-fé estão parcialmente atendidos na política de privacidade, mas ressalta-se que os princípios a seguir não foram totalmente atendidos: r**esponsabilização e prestação de contas**, pois a comprovação de que os sistemas estão realizando o cumprimento das normas para prestação de contas não é coberta pela política; e f**inalidade, adequação, necessidade e qualidade**, uma vez que a política de privacidade de dados não indica a obrigação de informar o usuário, sendo esta explícita no princípio de finalidade da lei.

4.6. Lições aprendidas com o processo de implantação

O gestor do time de *Access Management* ressaltou o desafio da comunicação com os usuários que não tem muito conhecimento de segurança da informação, e não estão familiarizados com o tema LGPD. O maior obstáculo identificado pelo gestor neste ponto, foi como captar a atenção do usuário, visto que é muito comum com que os colaboradores de outros setores da empresa, principalmente aqueles que estão alocados na fábrica, não realizarem a leitura de *e-mails* de comunicação do time de TI.

O gestor destacou como lição aprendida, a importância e o valor dos dados pessoais mesmo no ambiente corporativo, visto que o cadastro de visitantes na empresa e até alguns cadastros em sistemas internos usavam diversos dados pessoais para sua completude, e o usuário final, tanto interno quanto externo, mesmo que fosse da TI, teria grande dificuldade em saber onde estavam ou como eram tratados estes dados.

O analista do time de *CyberSecurity* avaliou como uma lição aprendida, a frequência com que entregamos nossos dados pessoais no dia-a-dia, por meio de cadastros presenciais ou em *websites* para pedidos de compra e etc., ressaltando que a comunicação corporativa é crucial para que os usuários, principalmente os que não têm tanto conhecimento sobre proteção de dados, compreendam a criticidade do tema e levem o conhecimento adquirido dentro da empresa para o seu dia-a-dia fazendo com que a lei seja efetiva em sua proposta, proteger os cidadãos residentes no país.

Além das lições aprendidas pelos entrevistados, deve-se destacar outras lições desse processo. Por meio do caso estudado pode-se notar como a LGPD surge com numerosas e variadas regras, destacando o quão importante é a existência de uma governança de TI bem-estruturada nas empresas afetadas pela nova lei, com políticas e diretrizes para guiar o negócio como um todo. De acordo com o COBIT 5 (ISACA, 2012), essa mudança ocorre quando os processos físicos se tornam digitais e a TI deixa de ser apenas a provedora de serviços e soluções técnicas e torna-se um parceiro de negócio da própria organização.

Tanto a LGPD quanto a GDPR possuem pontos com interpretação aberta, dificultando a identificação plena dos requisitos, e com isso, é necessária a adesão de todas as linhas de negócio na adequação, como *compliance* e o setor jurídico, antes não tão envolvidos em projetos de TI.

Outro ponto importante identificado é que, durante a observação, a governança de dados não foi tão citada quanto a governança de TI, quando deveriam estar juntas. Segundo Rêgo (2013), a governança de dados é quem atua nas normas, políticas e diretrizes da companhia, além de ser uma visão dos seus dados e define todos os processos que se alimentam destes dados.

Percebeu-se também que a presença de um portfólio de sistemas nas empresas que serão afetadas pela legislação é de extrema importância pois a empresa Duosun teve de realizar um grande esforço no princípio do projeto para realizar este levantamento, o que seria evitável caso a integração das linhas de negócio com a TI fosse maior.

Em relação a isso, pode-se citar que outra lição aprendida foi o grande impacto da adequação na cultura organizacional da empresa, pois no período anterior ao processo de

adequação, a governança de TI e área de negócio não tinham um alto nível de integração, com a TI limitando-se ao trabalho técnico quando necessário. Agora, todos os novos processos de negócio estão sendo conduzidos com apoio da governança de TI, fazendo com que se originem em conformidade com legislações vigentes, também possam ser otimizados para o meio digital.

A existência de um orçamento para o projeto de adequação é outra lição aprendida, pois não havia o direcionamento de tantos recursos financeiros para a área de TI e uma adequação tão grande como essa requer a alocação de verba para a contratação de consultorias especializadas, alocação de horas para realização de tantas mudanças e isto foi um grande desafio, visto a alocação de *budget* setorial presente na cultura da empresa.

Por fim, alguns sistemas da empresa são tratados por fornecedores externos, levantando a dúvida de como serão realizadas as tratativas para a adequação a lei por estes fornecedores, como é feito o tratamento dos dados pessoais por eles e se os contratos de serviço terão, de alguma forma, que ser revistos pela empresa Duosun.

CONSIDERAÇÕES FINAIS

A importância da proteção de dados pessoais no mundo atual é ainda mais importante com a crescente globalização da informação e o amplo acesso à internet. Todas as empresas residentes em solo brasileiro estão sob o escopo da LGPD e vão precisar se adequar à nova realidade para continuarem seu funcionamento. Esta adequação se torna ainda mais complicada em um cenário pela pandemia mundial causada pela COVID-19, e mesmo que o prazo de vigência da lei tenha sido alterado e as sanções referentes a lei só possam ser aplicadas a partir de agosto de 2021, as companhias que tratam dados pessoais devem realizar a adequação com tempo hábil para todas as alterações em seus processos.

Ante os objetivos propostos, o estudo conseguiu cumprir todos eles, ressaltando, que a integração entre a TI e as áreas de negócio está mais importante do que nunca, e todos os processos de negócios devem ter a participação da governança de TI para que a empresa evite o retrabalho para adequar processos novos à lei, evitando possíveis penalidades, uma vez que as companhias estão migrando cada vez mais para os meios digitais. Em contrapartida, é importante que a TI possua a participação de outras linhas de negócio em seus processos, pois como visto durante o estudo, o time jurídico que não possui uma integração forte com a TI, foi extremamente necessário para a interpretação da lei que possui muitos pontos vagos e não seria interpretado de maneira rápida e certeira pelo time de TI.

Por fim, as principais limitações do estudo foram não poder estar presente no dia-a-dia dos funcionários por conta da pandemia, visto que todos os integrantes do projeto de adequação da empresa estão em jornada de trabalho remoto em função da pandemia do COVID-19. A impossibilidade de realizar um acompanhamento pessoal é um obstáculo pois este ajudaria a realizar a observação das soluções e impactos de forma mais clara e mais participativa. Outro fator limitante foi o fato da lei e sua adequação serem assuntos muito recentes, com estudos acadêmicos escassos principalmente na área de TI, sendo grande parte de artigos atuais sobre o tema pertinentes à área de direito. Desta maneira espera-se que o caso estudado possa contribuir para que outras organizações também organizem os seus projetos de adequação observando a experiência da empresa.

REFERÊNCIAS

Alleasy (2020). *LGPD x GDPR*: Quais as semelhanças e diferenças. Disponível em: <https://www.alleasy.com.br/2020/03/09/lgpd-x-gdpr-semelhancas-diferencas/>. Acessado em: 13 mar. 2021.

Advocacia CHC. (2019). *Marco Civil da Internet*: O que é e o que muda para seu negócio. Disponível em: < https://chcadvocacia.adv.br/blog/marco-civil-da-internet/>. Acessado em: 10 mar. 2021.

Assi, Marcos. (2013). *Gestão de compliance e seus desafios*: como implementar controles internos, superar dificuldades e manter a eficiência dos negócios**.** São Paulo: Saint Paul Editora.

Barbieri, Carlos. (2013). *Uma visão sintética e comentada do Data Management Body of Knowledge (DMBOK).* Belo Horizonte: Fumsoft, Disponível em: <https://www.researchgate.net/publication/297699158_Uma_visao_sintetica_e_comentada_do_Data_Management_Body_of_Knowledge_DMBOK#pf7>. Acessado em: 3 jun. 2021.

Besemer, Leo. (2018). *EXIN Privacy & Data Protection Foundation*: Privacidade, Dados Pessoais e GDPR. EXIN, 2018. Livro digital.

Bezerra, Arthur Coelho. Waltz, Igor. (2014). Privacidade, neutralidade e inimputabilidade da internet noBrasil: avanços e deficiências no projeto do Marco Civil. *Revista Eptic Online*. V.16, n.2, p.161-175, Mai-ago.

Brasil. (2014). *Código Civil. Lei 12.965/14*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acessado em: 10 mar. 2021.

Brasil. (2018). *Código Civil. Lei 13.709/18.* Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acessado em: 27 fev. 2021.

Carvalho, Luis Osete Ribeiro, Duarte, Francisco Ricardo, Menezes, Afonso Henrique Novaes &. Souza, Tito Eugênio Santos. (2019). *Metodologia científica*: teoria e aplicação na educação à distância. Petrolina-PE. Livro digital. Disponível em: <https://portais.univasf.edu.br/dacc/noticias/livro-univasf/metodologia-cientifica-teoria-e-aplicacao-na-educacao-a-distancia.pdf>. Acesso em: 3 mar. 2021.

Confessore, Nicholas. (2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*, New York, abr. Disponível em: < https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>. Acessado em: 05 mar. 2021.

Correa, Rafael Murilo. (2018). *Governança de TI*: Descubra tudo o que você precisa saber para implantar a Governança de TI. Disponível em: <https://www.euax.com.br/2018/08/governanca-de-ti/#:~:text=A%20Governan%C3%A7a%20de%20TI%20%C3%A9,estrat%C3%A9gica%20e%20ativa%20no%20neg%C3%B3cio >. Acesso em: 14 mar. 2021

Davenport, Thomas H. (1988). *Ecologia da informação*: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura.

European Comission. (2016). *What personal data is considered sensitive?* Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-

organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en>. Acessado em: 13 mar. 2021.

IBM Security Identity Governance and Intelligence. (2021). *Segregação de Funções (SOD):* Um tipo específico de risco. IBM. Disponível em: < https://www.ibm.com/docs/pt-br/sig-and-i/5.2.1?topic=model-segregation-duties-sod-specific-type-risk >. Acessado em: 10 abr. 2021.

ISACA. (2012). *Modelo corporativo para governança e gestão de TI da organização***.** Disponível em: <http://www.cefet-rj.br/attachments/article/2870/Cobit_5_pt-br.pdf>. Acessado em: 09 mar. 2021.

Oliveira, Djalma de Pinho Rebouças de. (2006). *Sistemas, organização e métodos*: uma abordagem gerencial**.** 16 ed. São Paulo: Atlas.

Rêgo, Bergson Lopes. (2013). *Gestão e governança de dados*: Promovendo os dados como ativo de valor nas empresas. Rio de Janeiro: Brasport.

São Paulo, Ministério Público do Estado. (2012). *Nova lei de crimes cibernéticos entra em vigor*. São Paulo, SP. Disponível em: < http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf>. Acessado em: 3 mar. 2021.

Sêmola, Marcos. (2014). *Gestão da segurança da informação*: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier.

Soares, Fabiana De Menezes, Jardim, Tarciso Dal Maso & Hermont, Thiago Brazileiro Vilar. (2013). *Lei de acesso à informação no Brasil*: O que você precisa saber. Brasília: Universidade Federal de Minas Gerais, Senado Federal. Disponível em: < https://www12.senado.leg.br/transparencia/arquivos/sobre/cartilha-lai/>. Acessado em 10 mar. 2021.

Thompson, Marcelo. (2012). Marco civil ou demarcação de direitos? Democracia, razoabilidade e as fendas na internet do Brasil. *Revista de Direito Administrativo*, Rio de Janeiro, v. 261, p. 203-251, set./dez.

Weill, Peter & Ross, Jeanne W. (2006). *Governança de TI – Tecnologia da Informação*. São Paulo: M. Books do Brasil.

Zuboff, Shoshana. (2020). *A era do capitalismo de vigilância*: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca.