A FORMAÇÃO DE PASSIVOS CONTINGENTES PELA NÃO OBSERVÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS

Autoria

Eduardo Rodrigues Linhares - eduardo.linhares@ufc.br

Departamento de Contabilidade / UFC - Universidade Federal do Ceará

Beatriz Gomes de Morais - beatrizgdemorais@gmail.com

Resumo

RESUMO: A Lei 13.709/2018, intitulada como Lei Geral de Proteção de Dados (LGPD) tem como propósito principal a proteção das informações dos usuários brasileiros. Além disso, a Lei é voltada ao cuidado com os dados sensíveis dos usuários, contra o uso indevido. Visto isso, a legislação impõe algumas práticas para mitigar os riscos que o tratamento e a guarda dessas informações oferecem e, possíveis penalidades para estas. O objetivo deste estudo é apresentar a possível formação de passivos contingentes que podem se aparecer com a não observação da LGPD. Para tanto, foram analisados os artigos que compõem a legislação e, com isso, vinculando as possíveis formações de passivos contingentes que podem ser desde a não aplicabilidade de mecanismos de compliance até a aplicação de sanções. A metodologia utilizada, é a pesquisa qualitativa, exploratória e através de pesquisas documentais. Concluiu-se que a existência de alguns pontos que podem gerar problemas se não forem tratados e atenuados de forma preventiva. O estudo põe em evidência os principais riscos que a não adoção da LGPD pode acarretar para as companhias através de pesquisas bibliográficas, tais como: aplicações de multas e pausa nas operações empresariais.

A FORMAÇÃO DE PASSIVOS CONTINGENTES PELA NÃO OBSERVÂNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS

RESUMO: A Lei 13.709/2018, intitulada como Lei Geral de Proteção de Dados (LGPD) tem como propósito principal a proteção das informações dos usuários brasileiros. Além disso, a Lei é voltada ao cuidado com os dados sensíveis dos usuários, contra o uso indevido. Visto isso, a legislação impõe algumas práticas para mitigar os riscos que o tratamento e a guarda dessas informações oferecem e, possíveis penalidades para estas. O objetivo deste estudo é apresentar a possível formação de passivos contingentes que podem se aparecer com a não observação da LGPD. Para tanto, foram analisados os artigos que compõem a legislação e, com isso, vinculando as possíveis formações de passivos contingentes que podem ser desde a não aplicabilidade de mecanismos de *compliance* até a aplicação de sanções. A metodologia utilizada, é a pesquisa qualitativa, exploratória e através de pesquisas documentais. Concluiu-se que a existência de alguns pontos que podem gerar problemas se não forem tratados e atenuados de forma preventiva. O estudo põe em evidência os principais riscos que a não adoção da LGPD pode acarretar para as companhias através de pesquisas bibliográficas, tais como: aplicações de multas e pausa nas operações empresariais.
Palavras-chave: Lei Geral de Proteção de Dados. Passivos Contingentes. Responsabilidade.
ABSTRACT: The Law 13.709/2018, entitled Lei Geral de Proteção de Dados (General Data Protection Law) (GDPL), has the main purpose of protecting the information of Brazilian users and, with this, seeks to provide trust and value for data. In addition, the Law is concerned with the care of users' sensitive data, so that they are not misused by corporations. Furthermore, the legislation imposes some practices that companies must adopt to mitigate the risks that the treatment and storage of this information can offer and, consequently, possible penalties for these. In this context, the objective of this study is to present the main contingent liabilities that can be formed if the entity does not put into practice what the Law proposed. For this, they were compensated as mitigations and the compliance mechanisms, which were not adjusted, generate problems, such as: People who deal operationally with the data, respond civilly for the damages caused. The methodology used, not touching the problem approach, was defined as a qualitative research, since, it is intended to know more in depth the topic addressed, regarding the objectives, it is defined as exploratory and in relation to the procedures, bibliographic researches were searched. It was concluded in this work, the existence of some points that can generate problems if not treated and mitigated in a preventive way. The study highlights the main risks that non-adoption of the LGPD may pose for bibliographic research societies.
Keywords: General Data Protection Law. Contingent Liabilities. Responsibility.
Implicações Práticas: A lei Geral de Proteção de Dados (LGPD) é aplicável a todas as pessoas físicas e jurídicas que manipulam dados de outras pessoas. Nesse processo de manusear e dar destinação aos dados essas pessoas podem contrair obrigações que apareceram de forma oculta e tratam danos de imagem e/ou pecuniários sendo classificadas como passivos contingentes.

1 Introdução

A Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) foi sancionada no dia 14 de agosto de 2018 e trata da proteção dos dados pessoais dos indivíduos, tendo como principal objetivo a proteção dos direitos fundamentais dos cidadãos buscando proporcionar confiança, segurança e valor para o tratamento das informações fornecidas pelos usuários (*Lei n.º 13.709*, 2018).

Para (Mendes & Doneda, 2020), a referida Lei tem como principais influências o modelo europeu de proteção de dados, visto que a exigência de uma base legal para o tratamento de dados, nos princípios gerais, nas regras especiais para dados sensíveis, na criação

de uma autoridade para aplicação e as regras para o controlador e operados de dados. Além disso, pode-se dizer que a lei brasileira também tomou como base o direito estadunidense (*data breach*) para a criação de regras em casos de incidentes de segurança (Mendes & Doneda, 2020).

Ademais, é possível afirmar que a LGPD veio complementar o conjunto normativo de leis que tratam das informações de dados, visto que, é notório a influência da legislação brasileira, já que, em seu escopo, ao regulamentar os fundamentos da proteção de dados no País, a revisão das decisões automatizadas e a responsabilidade solidária entre as fontes, ela se baseou no Marco Civil da Internet, na Lei do Cadastro Positivo e no Código de Defesa do Consumidor, respectivamente (Mendes & Doneda, 2020).

Posto isso, a Lei Geral de Proteção de Dados é uma forma que o governo brasileiro utiliza para regulamentar o tratamento dos dados para que os mesmos não sejam utilizados de forma indevida e não explícita ao usuário final Cotterman e Kumar (1989, como citado em Pereira, Conte & Feitosa, 2015). Sendo assim, as companhias que detém essas informações precisam estar preparadas para fornecer meios que evitem a ocorrência de acidentes quanto ao mau gerenciamento de dados, buscando oferecer os melhores serviços aos usuários que confiam suas informações a elas.

Para tanto, é de suma importância à entidade que os mecanismos de *compliance* estejam ajustados para resguardá-la de futuros riscos e problemas, sendo assim, é necessário que a equipe empresarial, desde a alta gestão até o operacional, tenha a disposição as regras de conduta previstas na LGPD a fim de não prejudicar a empresa. Portanto, a pesquisa se compromete a responder a seguinte questão problema: Quais são os principais passivos contingentes que podem se formar em decorrência da inobservância da LGPD?

Para o desenvolvimento deste trabalho e atingir aos objetivos foi utilizada a metodologia exploratório, visto que procurou-se efetuar um aprofundamento nesse tema. Em relação aos procedimento a pesquisa foi documental, e utilizou-se a metodologia qualitativa para abordar o problema.

O objetivo geral do estudo é apresentar quais são os principais passivos contingentes que podem se formar com a não observação da LGPD. Para tanto, seus objetivos específicos são: identificar os principais passivos contingentes indicados no texto da própria legislação; analisar os efeitos da Lei Geral de Proteção de Dados nas empresas; definir as responsabilidades e sanções que estão previstas na Lei; e demonstrar a importância da Lei Geral de Proteção de Dados aos usuários. O presente estudo se motiva na importância que a Lei Geral de Proteção de Dados pode dar ao sistema normativo brasileiro, pois, além de dialogar com regulamentos de outros países, ela oferece mais confiança aos brasileiros quanto à forma que estão utilizando seus dados (Mendes & Doneda, 2020). Desse modo, a pesquisa justifica-se a fim de contribuir para as principais reflexões que podem ser percebidas na LGPD. Essa pesquisa se difere das demais ao analisar sob a perspectiva dos possíveis passivos contingentes que poderão ser formados pelo não cumprimento da Lei.

O trabalho é estruturado em: Introdução, Referencial Teórico, Metodologia, Desenvolvimento da Pesquisa e Considerações Finais.

2 Referencial Teórico

2.1 Passivo

De acordo com o Pronunciamento Técnico do Comitê de Pronunciamentos Contábeis (CPC) 00 (R2) (2019), Passivo é uma obrigação presente da entidade de transferir recursos econômicos como resultado de eventos passados e, para que ocorra a existência desses, é necessário que três critérios sejam cumpridos:

I. A entidade tem uma obrigação;

II. A obrigação de transferir um recurso econômico;
III. A obrigação é uma obrigação presente que existe como resultado de eventos passados.

Esse grupo de contas está disposto no Balanço Patrimonial (BP) das empresas compreendendo as exigibilidades e obrigações, sendo ainda classificada como Circulante e Não Circulante. Com isso, a Lei 6.404/76 define que as contas devem estar no BP de forma ordenada e uniforme para facilitar o entendimento dos mais diversos tipos de usuários (Lei 6.404, 1976). A Tabela 1 apresenta como o Balanço é composto de acordo com a Lei:

Tabela 1 – Balanço Patrimonial de acordo com a Lei 6.404/76

BALANÇO PATRIMONIAL

ATIVO Circulante Não Circulante	**PASSIVO** Circulante Não Circulante **PATRIMÔNIO LÍQUIDO**
Total: X	Total: X

Fonte: Elaborado pelos autores (2021).

O passivo, portanto, é uma obrigação que a empresa identifica e reconhece como algo em que algum momento no presente ou no futuro terá que transferir um recurso econômico para um determinado credor. Para esse caso a entidade tem essa obrigação de forma clara, porém, esta pode ter passivos em que ela não identifica em seus reconhecimentos e fica de forma oculta, e esse elemento é conhecido como passivo contingente (Iudícibus, Martins e Gelbcke, 2018).

2.1.1 Passivo Contingente

Como o próprio nome reporta, o termo Passivo Contingente é um passivo que ficou contingenciado, ou melhor, retido, e que não foi claramente identificado pela entidade responsável pela formação desta obrigação.

De acordo com o Pronunciamento Técnico CPC 25 (2009), Passivo Contingente é:

I. uma obrigação possível que resulta de eventos passados e cuja existência será confirmada apenas pela ocorrência ou não de um ou mais eventos futuros incertos não totalmente sob controle da entidade; ou
II. uma obrigação presente que resulta de eventos passados, mas que não é reconhecida porque:
    a. não é provável que uma saída de recursos que incorporam benefícios econômicos seja exigida para liquidar a obrigação; ou
    b. o valor da obrigação não pode ser mensurado com suficiente confiabilidade.

Sendo assim, é uma probabilidade de saída de recursos da organização, representando uma contingência para que os gestores possam estar cientes de eventuais saídas de recursos que estarão fora da rotina empresarial e em alguns casos não prevista em seus fluxos de caixa.

É importante ressaltar que passivo contingente é diferente de provisão, visto que, ela é algo que demonstra incerteza quanto aos prazos e os valores que serão necessários para a sua liquidação (Iudícibus et al., 2018). Posto isso, o CPC 25 (2009, p. 5) dita que para ela ser reconhecida é necessário que:

(a) a entidade tem uma obrigação presente (legal ou não formalizada) como resultado de evento passado;
(b) seja provável que será necessária uma saída de recursos que incorporam benefícios econômicos para liquidar a obrigação; e
(c) possa ser feita uma estimativa confiável do valor da obrigação.

2.2 Responsabilidade Civil

A Responsabilidade Civil está disposta no Código Civil Brasileiro, Lei n.º 10.406 de 10 de janeiro de 2002, no Capítulo IV, Título IX e se dispõe a regular danos que qualquer indivíduo cause a outro, sendo dever deste repará-lo, já que qualquer um possui a o dever jurídico originário de não causar danos a outrem e, se caso ocorrer, passa a ter um dever jurídico sucessivo, devendo assim, restaurar aquilo que foi comprometido (Ramos, 2012). A obrigação de haver reparação do dano parte do pressuposto que se restabeleça a ordem natural dos eventos, como se aquilo não tivesse ocorrido.

Ademais, no Código Civil, Art. 927, Parágrafo único, explicita que haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (Lei n.º 10.406, 2002) . E, além disso, se o dano causado tiver mais de uma pessoa, há a existência da responsabilidade solidária para reparar os problemas causados conforme os Arts. 932 e 942 do Código Civil Brasileiro (Lei n.º 10.406, 2002).

Em relação às formas de responsabilização civil, (Capanema, 2020) expôs que só haverá responsabilização quando o desrespeito às normas jurídicas e técnicas afetarem um dano material ou moral a um titular ou coletividade e, além disso, definiu que a LGPD possui duas situações, sendo elas: a violação de normas jurídicas, quando for relacionada ao microssistema de proteção de dados, e a violação de normas técnicas, quando for relacionada à segurança e proteção dos dados.

Sendo assim, a LGPD dispõe que:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (Lei n.º 13.709, 2018, Art. 42).

Como visto, os indivíduos e as empresas incorrem em responsabilização civil se infringirem as regras jurídicas e em especial as descritas na LGPD, com consequências para responder financeiramente pelo dano causado às pessoas ou entidades que sofreram o dano por terem os seus dados de alguma forma violados.

2.3 Lei Geral de Proteção de Dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD), Lei n.º 13.709/2018, foi sancionada em 2018, com aplicação no Brasil, para os dados pessoais de indivíduos, para o tratamento desses e quando houver ofertas de bens e serviços que necessitem deste tipo de dado (Lei n.º 13.709, 2018). É possível afirmar que a LGPD é um aprimoramento de direitos que os cidadãos brasileiros possuem, tais como aqueles definidos nos Inciso I e IV do Artigo 3.º da Constituição Federal/1988, que determina a garantia de uma sociedade livre, justa e solidária, como também, a promoção do bem de todos, sem preconceito de origem, raça, gênero, cor, idade e quaisquer outras formas de discriminação, seja ela social ou racial (Lei n.º 13.709, 2018).

Para tanto, a Constituição ainda assegura, no Art. 5.º, que: “todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade”, além de resguardar, no Inciso X, a intimidade, a vida privada, a honra e imagem de pessoas e, assim, garante o direito a indenização pelo dano material ou moral decorrente da violação destes (Lei n.º 13.709, 2018).

Dado isso, a LGPD define, em seu Inciso V do Art. 5.º, que o titular dos dados é toda e qualquer pessoa natural a quem se referem os dados e que estão sendo tratados, sendo esta operação como toda e qualquer realizada que abordem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação,

comunicação, transferência, difusão ou extração (Inciso VIII), não esquecendo, que deve haver o consentimento do detentor dos dados (Inciso XII) para que essa operação possa ser realizada (Lei n.º 13.709, 2018).

Para que ocorra o tratamento de dados, a legislação designa, nos Incisos VI e VII do Artigo 5.°, dois agentes, sendo um deles o controlador, aquele que tem a competência para tomar decisões referentes ao tratamento de dados, e o outro o operador, aquele que realiza o tratamento de dados no nome do controlador e, com isso, a Autoridade Nacional, que fiscaliza o uso de dados, poderá requisitar um relatório de impacto à proteção de dados (Inciso XVII) para analisar se não há o tratamento regular desses, sendo considerada irregularidade quando não houver observância na legislação e o não fornecimento de segurança adequada (Lei n.º 13.709, 2018) .

Sendo assim, caso ocorra incidentes com a segurança, os agentes de tratamento, definidos no Inciso IX do Art. 5.º da LGPD como operador e controlador de dados, podem responder diretamente, de forma subjetiva e solidária, os danos causados (Lei n.º 13.709, 2018).

Além disso, a autoridade nacional poderá aplicar algumas possíveis sanções, tanto aos agentes de tratamento quanto a empresa, que deverão ser ponderadas considerando as peculiaridades de cada caso, devidamente julgadas em processos administrativos, com a condição do exercício da ampla defesa do sancionado considerando os parâmetros e critérios de acordo com o Parágrafo 1.º do Art. 52 da LGPD (Lei n.º 13.709, 2018).

Ante o exposto, a LGPD veio para proteger as pessoas físicas e jurídicas contra o uso indiscriminado e desautorizado dos seus dados, gerando penalidades para os manipuladores dos dados alheios, caso os mesmos distorçam o uso dos dados que lhes foram confiados, para obter vantagens econômicas ou até mesmo por distribuição involuntária. Para tanto, como previsto no Art. 15 da Lei, o término do tratamento dos dados se dará à medida que a finalidade for sendo alcançada ou pela revogação do titular e ainda por determinação da Autoridade Nacional (ANP) (Lei n.º 13.709, 2018). É importante acrescentar que se houver quebra de sigilo dessas informações particulares, os agentes de tratamento ficarão sujeitos a sanções administrativas, como previstas no Art. 52 da LGPD, que, dependendo da gravidade, as infrações podem ser: advertências, multa de até 2% sobre o faturamento da pessoa jurídica bloqueio e eliminação dos dados pessoais a que se refere a infração, suspensão parcial ou total das atividades relacionadas a tratamento de dados e do banco de dados a que se refere a infração (Lei n.º 13.709, 2018).

3 Metodologia

O presente trabalho possui abordagem qualitativa, visto que se preocupa em fazer análises mais específicas em relação ao tema estudado que não pretendem quantificar ou mensurar os objetos estudados (Richardson et al., 1999).

Quanto aos objetivos, a pesquisa pode ser classificada como exploratória, que segundo Gil (2010), tem como finalidade proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses. Uma característica interessante da pesquisa exploratória consiste no aprofundamento de conceitos preliminares sobre determinada temática não contemplada de modo satisfatório anteriormente (Raupp & Beuren, 2006; Souza, 2020).

Quanto aos procedimentos é classificado como documental, que, de acordo com Fonseca (2002), recorre a fontes mais diversificadas e dispersas, sem tratamento analítico.

O estudo foi realizado a partir de uma análise da Lei n.º 13.709/2018, listando os possíveis passivos contingentes que poderão ser formados se a entidade não executar seus procedimentos conforme a Lei. O trabalho focalizou precisamente nos seguintes eventos, ou situações, ou ambientes em que podem aparecer passivos contingentes: sistema de gestão de dados eficiente e seguro, estrutura e gestão de dados, mapeamento do conjunto de dados, classificação dos dados, consentimento do titular dos dados, término do tratamento de dados,

agentes de tratamento, contratação de terceiros para tratamento dos dados, sistema de gerenciamento de dados, segurança e sigilo dos dados, risco pessoal dos agentes de tratamento, e boas práticas de gestão de dados (IOB, 2020, p. iob).

Essas situações mencionadas no parágrafo anterior foram extraídas de reflexões que a própria LGPD proporcionava ao longo do seu texto e permitiu a identificação de possíveis fragilidades que os sistemas computacionais empresariais poderiam ter na execução das suas atividades de tratamento de dados, bem como fragilidades do tratamento propriamente dito executado pelos agentes de tratamento de dados.

Com isso, a pesquisa não se torna empírica devido ao fato de haver uma abordagem das reflexões da LGPD sobre a perspectiva apenas teórica dos passivos contingentes, não sendo objeto de estudo do presente trabalho casos práticos ou análise de dados.

4 Desenvolvimento da Pesquisa

Em primeira análise, conforme Art. 1.º da LGPD percebe-se que o principal efeito que a Lei poderá trazer para as entidades é tornar as relações, tanto internas quanto externas, mais confiáveis, visto que, com a regulamentação do tratamento de dados, estes passam a ser, se cumpridos os requisitos legais, mais seguros e personalizados (Lei n.º 13.709, 2018). Dessa forma, é importante salientar que as companhias precisam estar cientes para que essa elevação do nível de segurança ocorra, é necessário que a mitigação de riscos tais como problemas de privacidade e segurança, má administração e mau uso dos dados, redundância de dados, informações desatualizadas (Terra, 2018), seja a tarefa mais importante a ser adotada, demandando, assim, tempo, recursos e procedimentos contínuos de avaliações internas, visto que a aplica-se e de acordo com o caput do Art. 3.º da LGPD, a qualquer forma de tratamento de dados e executado por qualquer pessoa física ou jurídica de direito público ou privado (Lei n.º 13.709, 2018).

Cabe ressaltar que o respeito à privacidade, como previsto no Inciso I do Art. 2.° da LGPD, é um dos fundamentos que pretendem garantir a disciplina da proteção de dados e que as empresas que prestam atividades de tratamento devem obedecer (Lei n.º 13.709, 2018). Diante disso, é importante avaliar que isso é amparado no Art. 21 do Código Civil Brasileiro que explicita "[...] a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (Lei n.º 10.406, 2002).

Em suma, a LGPD prevê a privacidade de dados desde a sua concepção, isto é, todas as empresas devem incorporar a privacidade, passando pela modelagem e tratamento, até o encerramento, de qualquer projeto que essa execute (Lei n.º 13.709, 2018). Com isso, demonstra que um dos objetivos da Lei é a proteção da privacidade do indivíduo com intuito de manter a intimidade, honra e imagem dos usuários, ratificando o que já vinha na redação da Constituição Federal.

4.1 Formação de Passivos Contingentes

Os passivos contingentes, conforme já mencionado no tópico Passivo Contingente deste trabalho, tem uma característica de formação oculta, ou seja, ele atende a todas as características de um passivo, porém não fica explícito como passivos tradicionais em que normalmente um documento, ou um reconhecimento mais cristalino, dão a certeza da assunção de certo compromisso como sendo uma obrigação da entidade.

Seguindo esse raciocínio, a não observância da legislação pode acarretar problemas na rotina empresarial e caso do seu não cumprimento, conforme o Art. 52 da LGPD, elas devem estar preparadas para possíveis passivos contingentes que poderão ser formados mais especificamente em relação a regulamentação do tratamento de dados no Brasil (Lei n.º 13.709, 2018). Com isso, pode-se dizer que a adequação de processos tais como de governança de

dados e *compliance,* se tornará algo fundamental e de necessária implantação tendo como consequência, a mudança da cultura operacional. Além disso, terá que haver a implementação de programas que passam segurança aos usuários que estão confiando seus dados a entidade e, para tal, é necessário que haja investimento em ferramentas de segurança de dados, *upgrade* em procedimentos e fluxos internos e externos de circulação da informação, e aplicação mais incisiva de mecanismos de controle (Pinheiro, 2020).

Inicialmente serão tratados alguns pontos relevantes, pontos esses já citados no tópico da Metodologia, serão extraídos da LGPD onde podem ser formados esse tipo de obrigação, objetivando trazer reflexões dessa legislação sob a perspectiva dos passivos contingentes, sem pretensão de exaurir esse assunto, ficando assim como uma sugestão para futuros trabalhos que irão tratar desse tema, os assuntos não abordados neste texto.

Para tanto, é importante entender o que venha a ser um Sistema de Informação Empresarial (SI) que pode ser definido como o mecanismo que processa, armazena e compartilha as informações de forma estruturada e que são necessárias às atividades da organização, sendo elas informações operacionais, fiscais, gerenciais ou estratégicas (Gil et al., 2010).

Nesse sentido deve-se afirmar que um sistema de gestão de dados eficiente e segura deve observar pelo menos os itens tratados no Art. 6.º da LGPD, isso é uma medida essencial a ser tomada para evitar consequências inesperadas para a entidade, visto que, a adoção deste fornece à empresa tanto o tratamento quanto a segurança adequada dos dados aos quais lhe são confiados (Lei n.º 13.709, 2018). Como visto, o Art. 2.º da LGPD cita os principais fundamentos da proteção de dados para que este atinja exatamente a função a que se destina e que foi objetivada pelos seus proprietários (Lei n.º 13.709, 2018). Considerando os dois elementos apresentados neste Parágrafo, uma gestão de dados eficiente e segura quando observada aplicada em seus processos de tratamento de dados mitiga a formação de passivos contingentes.

Do ponto de vista da estruturação e gestão de dados são fatores de suma importância para qualquer empresa pois servem, principalmente, para mapear possíveis riscos e, para tanto, a entidade deve estar atenta aos requisitos básicos para manter o sistema de segurança tais como: a verificação de duas etapas, definição de permissões no sistema com nível de privilégio de acesso de cada usuário, local de armazenamento dos dados e informações dos usuários local ou remoto (*cloud*) (Pinheiro, 2020), dentre outros.

Em conjunto a atividade de estruturação e gestão de dados, a empresa deve de forma complementar adicionar esforços para que o mapeamento do conjunto de dados seja o mais completo possível. Para tanto, considera-se como o mapeamento de dados a atividade de tentativa de apresentação dos dados em um formato que favoreça a forma que o significado do dado se torne explícito (Cruz, 2015), e que se torna efetiva a partir da própria prática operacional no manuseio das informações e na identificação do nível de sensibilidade (I. M. R. Santos, 2019), bem como da privacidade destes, pois os dados devem estar estruturados de forma a atender requisitos de segurança conforme legisla o Art. 49 da LGPD (Lei n.º 13.709, 2018). É relevante considerar que a organização segregue e classifique por grau de risco e de exposição destes identificando-os, ou seja, determinando quais os eventos que podem trazer repercussão negativo nos negócios da empresa (Konzen, 2013), e quanto mais sensível for as informações, menos exposta deverá ser, sendo, portanto, fatores inversamente proporcionais e devendo ponderar pincipalmente o que conceitua o Inciso II do Art. 5.º da LGPD sobre dados pessoais sensíveis (Lei n.º 13.709, 2018).

Também, outra forma de contribuir para aumento da segurança é a de determinar os usuários em perfis individuais ou em grupos nos quais serão definidos qual é o privilégio de acesso a determinados dados visto que o usuário final é o elo mais fraco do processo de segurança da informação e onde as interações provocam maiores riscos para todo o sistema de

informação (Pereira et al., 2015). Cotterman e Kumar (1989, como citado por Pereira et al., 2015) citam ainda que dentro de uma empresa, o usuário final pode atuar no desenvolvimento, na operação e no controle de sistemas de informação (SI).

Com efeito, caso não haja a atividade de mapeamento, e o conhecimento do grau de risco dos dados não ficarem explicitamente identificados, e também os perfis de usuários não forem configurados, esses dados poderão ser utilizados por qualquer usuário que tenha acessos irrestritos ao sistema de gestão da empresa. Caso haja o vazamento, a extensão da sanção será ponderada pelos critérios estabelecidos no Parágrafo 1.º do Art. 52, tais como: gravidade e a natureza das infrações e dos direitos pessoais afetados, a boa-fé do infrator, vantagem auferida ou pretendida pelo infrator, o grau do dano, proporcionalidade entre a gravidade da falta e a intensidade da sanção, entre outros (Lei n.º 13.709, 2018). Com isso, os danos podem afetar significativamente a operação da empresa e podem ser tanto pecuniários quanto de imagem da organização e, de acordo com Parágrafo 2.° do Art. 52, não descarta ou elimina outras sanções administrativas, civis e penais (Lei n.º 13.709, 2018) . Adicionado a isso a inclusão de parâmetros para identificar intrusos, softwares antivírus, criptografia de dados e certificado digital são algumas métricas rigorosas que ajudam a melhorar a qualidade e a confiabilidade do sistema de gestão de dados (Laudon & Laudon, 2014).

Em relação a Classificação dos Dados, o Art. 5.º da LGPD segrega em dado pessoal, dado pessoal sensível e dado anonimizado, especificamente o Inciso I defino com sendo dado pessoal a informação relacionada a pessoa natural identificada ou identificável, portanto, qualquer dado que consiga ser relacionado a uma pessoa natural é possível identificá-la com clareza (Lei n.º 13.709, 2018) . Nesse sentido, o Inciso II do Art. 5.º da LGPD aprofunda um pouco mais o conceito de dado e explicita o que é um dado pessoal sensível como sendo o "[...] 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." (Lei n.º 13.709, 2018) .

No que diz respeito ao dado sensível o cuidado deve ser redobrado, pois deve ser classificado e reconhecido como tal para que na Gestão dos Dados efetuados através dos sistemas de informação, os manipuladores os reconheçam como dados que requerem maiores cuidados nesse manejo (Machado & Bianchini, 2016).

Continuando, no Inciso III do Art. 5.º da LGPD, especifica o que é um dado anonimizado como sendo um "[...] dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (Lei n.º 13.709, 2018). Como visto, esse dado se refere a uma pessoa natural sem, no entanto, ser possível relacioná-lo a um indivíduo real.

Conforme comentado anteriormente quando se tratou da gestão de dados, a classificação entre dados pessoais, dados sensíveis e dados anonimizados é de muita importância para organização para não deixar vulnerável informações que possam trazer algum dano para a organização que o manipula.

Nesse contexto, o cuidado que deve existir para prevenir a não formação de passivos contingentes, nas situações em que não ocorre a classificação desses dados como conceitua os Incisos I, II e III do Art. 5.º (Lei n.º 13.709, 2018) é no seu acesso pelos diversos usuários da organização que manejam essas informações, devendo haver segregação destes em grupos de usuários com privilégio de alcance aos dados e, principalmente, atentando para que nem todos os usuários possam ter acesso livre às informações, portanto, todos os usuários deveriam ser agrupados considerando prioritariamente o grau de risco de exposição dos dados, conforme já exposto nesse texto (D. L. dos Santos, 2014).

Além disso, um Sistema de Auditoria, que definido por Castro e Lima (1999) foi criado para "[...] assegurar a adequação, privacidade dos dados e informações oriundas dos sistemas

eletrônicos de processamento de dados, observando as diretrizes estabelecidas e a legislação específica [...]", deve também fazer o registro de acesso aos dados identificando quem, quando e com que frequência determinado usuário fez consulta a esse dado ou conjunto de dados para determinar se o acesso está condizente ao objetivo de trabalho do operador.

A extensão do grau do dano pelo prejuízo causado ao proprietário dos dados, bem como a gravidade e a natureza da disponibilização desses dados a pessoas desautorizadas a ter acesso às informações, dentre outros, podem ser alguma das ocorrências em que passivo contingente pode ser formado, de acordo com os Incisos I e VI, do Parágrafo 1.º, do Art. 52 (Lei n.º 13.709, 2018) .

Em adição, é imprescindível o consentimento do titular dos dados, que, de acordo com o Parágrafo 4° do Art. 8° da LGPD, o proprietário das informações deverá permitir o seu uso, bem como deverá saber a que se destina essa cessão de dados (Lei n.º 13.709, 2018). Essa permissão deverá ocorrer de forma contínua (Inciso I do Art. 7.º) e a utilização deve ocorrer apenas mediante autorização, com exceção apenas em casos em que há obrigações legais ou regulatórias, pois, essa concessão acontece de forma implícita, como estabelece os Incisos de II a IV , do Art. 7.º (Lei n.º 13.709, 2018) .

É importante abordar que quando há manipulação das informações, a cessão para uso e tratamento destes deve ser segura, confiável e atenda estritamente e unicamente a finalidade para o qual foram cedidas como preceitua o Inciso XII do Art. 5.º (Lei n.º 13.709, 2018). Complementando esse raciocínio, segundo o Caput do Art. 8.º da LGPD, apenas o titular dos dados pode conceder o acesso aos seus dados e, de acordo com Parágrafo 5.º do Artigo 8.º da LGPD, também é do titular dos dados, o poder de revogar a qualquer tempo essa concessão de acesso aos seus dados, e este deve demonstrar esse desejo através de manifestação clara e inequívoca ao agente de tratamento de dados que o titular dos dados pretende encerrar o seu direito de uso dos dados anteriormente cedidos (Lei n.º 13.709, 2018).

Para tanto, as organizações que têm a posse dos dados devem ter ciência que o processamento deverá ser baseado conforme o consentimento do proprietário dos dados com fins específicos ou no que é exigido por Lei, conforme estabelecem o Inciso XII, do Art. 5.º e o Art. 7.º (Lei n.º 13.709, 2018). Com isso, é fundamental que as sociedades estejam atentas as autorizações e principalmente a possíveis revogações dessas autorizações para uso de dados, pois nesse ponto em que a cessão de dados é encerrada por vontade do proprietário, é que a empresa pode continuar com o processamento e gerar possíveis passivos contingentes previstos no Parágrafo 1.º do Art. 52 da LGPD, mais especificamente no Inciso III, que pode ser interpretado como a possibilidade obtenção de alguma vantagem econômica para quem os tratou (Lei n.º 13.709, 2018).

Ademais, é necessário que as empresas tenham para além do que determina a LGPD, em sua cultura operacional, que a segurança da informação, guiada pelos princípios fundamentais da confidencialidade, integridade e disponibilidade (Pereira et al., 2015) sejam matérias essenciais e, por conseguinte, a importância do investimento em segurança técnica, físicas e operacionais, ratificando que os dados estejam livres de possíveis problemas tais como vazamentos e fraudes, conforme recomenda o Parágrafo 7.º, do Art. 52 (Lei n.º 13.709, 2018) .

Vinculado a isso, pode-se afirmar que quando ocorrer o término do tratamento de dados de que trata os Arts. 15 e 16 (Lei n.º 13.709, 2018) é de suma importância que haja a eliminação correta destes, visto que, caso ocorra algum vazamento dessas informações, poderá ser aplicável, aos agentes de tratamento, a obrigação de reparar danos, independentemente da culpa como estabelece o Art. 927 do CCB (Lei n.º 10.406, 2002). Para tanto, o Artigo 15 da LGPD, cita algumas hipóteses de quando ocorre a finalização: a finalidade for atingida; houver o fim do período de tratamento; houver revogação expressa do proprietário; ou quando a Autoridade Nacional determinar (Lei n.º 13.709, 2018) .

De forma geral, como abordado no Artigo 16 da LGPD, ao fim da análise dos dados, o

controlador deve certificar-se que os dados serão eliminados da base em que estão armazenados, excetuando-se nas seguintes condições: cumprimento de obrigações legais ou regulatórias; quando solicitado por órgãos de pesquisa com anonimização dos dados sempre que possível; para transferência a terceiros; e quando utilizado exclusivamente pelo controlador, de forma anonimizada e sem disponibilizá-lo a terceiros (Lei n.º 13.709, 2018). Deve-se ressaltar ainda que os Incisos I a IV, do Art. 16 da LGPD cita que em casos específicos de obrigações legais ou regulatórias, dentre outras, em que os dados devem ser mantidos até o prazo prescricional que a legislação exige (Lei n.º 13.709, 2018).

Dado isso, como a eliminação dos dados é obrigatória, em exceção às situações em que a guarda é exigida, se os dados forem mantidos na estrutura de bancos de dados da empresa, e ocorra algum incidente de segurança conforme Pereira, Conte e Feitosa (2015, p. 62) tais como "tentativas não autorizadas de acesso a sistemas ou dados, bem como modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema", a empresa deverá adotar prontamente medidas que corrijam a falha, bem como a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, de acordo respectivamente com os Incisos X e VIII, do Parágrafo 1.º, do Art. 52, sendo esses parâmetros utilizado para fazer a dosimetria da sanção administrativa e, portanto, o tamanho da obrigação contingente (Lei n.º 13.709, 2018). Como forma de mitigar esses problemas, após término do tratamento de dados e pesando que uma boa política de gestão da informação executada por bons gestores deve levar em conta a segurança da informação (Nassif & Resende, 2016), é recomendável que estes dados sejam retirados das operações da entidade sendo segregados dos demais dados com possibilidade de acesso restrito feito somente por pessoas específicas autorizadas ainda a manipulá-los, sendo essa mais uma medida que minimizaria a formação de passivos contingentes.

É importante salientar que para que a qualidade do tratamento dos dados seja efetiva, a entidade deve segregar os agentes de tratamentos com privilégio para acessá-los e manipulá-los. Estes agentes são definidos nos Incisos VI e VII, do artigo 5.º da LGPD, como controlador e operador, que, em resumo, são as pessoas para as quais os dados são disponibilizados com intuito de tratamento a fim de atender uma demanda específica de informação e, por isso, são os responsáveis por executar,

> [...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Lei n.º 13.709, 2018, Art. 5.º, Inciso X).

Diante dessa condição, o controlador deve estar sempre com autorização referente à cessão dos dados para tratamento em vigor e, de acordo com o que o proprietário dos dados destinou essa cessão pois essa é uma das atribuições de controle dentro de um sistema (Pereira et al., 2015). Portanto, cabe ao controlador provar que esse tratamento foi concedido e que a finalidade foi cumprida. Em relação ao operador é a pessoa que efetua o tratamento dos dados cedidos pelo proprietário em nome do controlador, em consonância com o Inciso VII do Art. 5.º, porém a este não exime a responsabilização civil pelo uso indevido ou não autorizado dos dados disponibilizados (Lei n.º 13.709, 2018).

Em resumo, a principal diferença entre eles reside no poder em que um detém sobre a informação (controlador) e que o outro não detém (operador) e, nesse sentido, há uma necessidade de ambos entenderem de suas responsabilidades sobre o processo de tratamento desses dados. Dessa forma, essa responsabilização, prevista no Art. 42 da LGPD, tem o fim voltado para que ninguém seja prejudicado e, aqueles que causaram os danos, sejam cobrados para que a ordem social seja mantida (Lei n.º 13.709, 2018). Nesse sentido, ao nível da sensibilidade dos dados, a necessidade de compreensão por parte dos tratadores de dados

principalmente no que se refere aos riscos assumidos, ponderando que quem define o nível de sensibilidade são exatamente essas pessoas (Bennett & Raab, 2018, citado por I. M. R. Santos, 2019) e as imposições legais se fazem importantes atividades de reeducação para toda a cadeia interna que manuseia esses dados apresentando os perigos da não conformidade com a legislação, indicando as principais sanções administrativas da operação incorreta citadas no Art. 52 da LGPD e ponderadas pelo Parágrafo 1.º do mesmo artigo, sendo essa novamente outra medida que busca mitigar ou mesmo evitar o aparecimento de passivos contingentes (Lei n.º 13.709, 2018).

É necessário, também, que a empresa esteja ciente se caso houver contratação de terceiros para o tratamento dos dados, por imposição do Art. 47 da LGPD ficam estes obrigados a garantir segurança da informação, bem como recomenda-se averiguar se cumprem as boas práticas e de governança de dados citadas nos Art. 50 e 51 da LGPD, e ainda certificando-se que estes atinjam os cinco domínios da governança de dados sendo eles: princípios de dados; qualidade dos dados; metadados; acesso de dados e ciclo de vida dos dados (Khatri & Brown, 2010), e dentro desses domínios verificar se existem certificação e capacidade técnica para realizar tal tarefa, e também exigir que faça uma declaração constando a finalidade específica do trabalho e um termo constando todas as responsabilidades e reparação de danos, se houver, pois, assim, resguarda a empresa de futuros prejuízos (Lei n.º 13.709, 2018) .

Em relação ao sistema de gerenciamento de dados, espera-se que este seja estruturado como recomenda o Art. 49 para atender os requisitos básicos de segurança, aos padrões de boas práticas de governança e aos princípios gerais previstos nas normas regulamentares (Lei n.º 13.709, 2018) . Além disso, é necessário que haja perfis e níveis de privilégio no acesso, para que nem todos os usuários tenham acesso, eficiência no processamento e segurança na operação, como o armazenamento criptografado, já relatados neste trabalho, entre outros (D. L. dos Santos, 2014). Estes foram alguns exemplos que se pode citar para evitar acessos indesejados aconteçam ao sistema, além de garantir que o tratamento de dados seja possível de ser configurado e totalmente confiável. Ainda, a Autoridade Nacional, de acordo com o Parágrafo 1.º, do Art. 46 da LGPD poderá determinar quais são os padrões técnicos mínimos desejáveis para atender toda a segurança e sigilo dos dados (Lei n.º 13.709, 2018).

Com efeito sobre a mesma vertente, mas sendo em relação a segurança e sigilo dos dados, o Caput do artigo 46 da LGPD, afirma que é de responsabilidade dos agentes de tratamento a adoção de medidas de segurança que sejam capazes de impedir "[...] qualquer forma de tratamento inadequado ou ilícito" (Lei n.º 13.709, 2018). Esse assunto vai além da segurança que um sistema de gerenciamento de dados deve oferecer aos usuários, sendo essa uma medida técnica já exigida que esse sistema possua, e que diz respeito também ao comportamento do tratador de dados quanto ao nível de sensibilidade do conjunto de informações manipuladas e os riscos dessa atividade (Pereira et al., 2015).

Por parte do sistema, conforme já relatado neste trabalho espera-se que este garanta que os acessos tanto ao sistema propriamente dito, quanto aos dados para que sejam possíveis de serem configurados e totalmente confiáveis (D. L. dos Santos, 2014). Por parte dos agentes de tratamento de dados espera-se um comportamento prudente e zeloso no mesmo sentido de garantir o sigilo e a segurança da informação, dos dados manipulados, e conscientes de que o não atendimento poderá causar inclusive danos pecuniários pessoais (Pimenta et al., 2016). E nesse sentido, o controlador deve informar a autoridade nacional qualquer "[...] ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares [...]", com o intuito principalmente reverter ou mitigar danos causados pelo ocorrido (Lei n.º 13.709, 2018, Art. 48).

Ante o exposto, na hipótese de ocorrer posturas relapsas e pouco cuidadosas com os dados operados e o seu compartilhamento, podem iniciar o aparecimento de um passivo contingente, pois os agentes de tratamento de dados têm a obrigação de garantir a segurança e

o sigilo da informação. Nesse sentido, o comportamento informacional do usuários, que trata das necessidade de informação dos usuários e os meios que estes buscam para obter, influencia diretamente na segurança da informação (Ohtoshi, 2013), portanto, um problema muito mais de reeducação, consciência dos danos que pode sofrer e, principalmente de comportamento proativo.

Além de todos os riscos mencionados neste trabalho, existe o risco pessoal dos agentes de tratamento que, por manterem contato direito com a manipulação, poderão, de acordo com o Art. 42 da LGPD, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, e ser obrigado a repará-lo (Lei n.º 13.709, 2018). Entretanto, o artigo 43 da mesma norma aborda que se houver comprovação que o tratamento dos dados que lhes foi atribuído não foi realizado, ou mesmo fazendo o tratamento de dados, não violaram a legislação, ou o dano foi causado pelo próprio proprietário dos dados ou por terceiros, não há aplicações de medidas punitivas (Lei n.º 13.709, 2018). Com o intuito de se resguardar de possíveis processos, o Art. 37 da LGPD recomenda que os agentes devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse (Lei n.º 13.709, 2018).

Nessa linha, pode-se afirmar que, na situação do controlador, haverá uma responsabilidade maior, pois ele é quem será acionado primeiramente e caso seja demandado deverá responder a autoridade nacional elaborando ainda um relatório, conforme o Art. 38, descrevendo o "[...] impacto à proteção de dados pessoais, inclusive de dados sensíveis [...]" (Lei n.º 13.709, 2018), além de outras solicitações estabelecidas nos Artigos 38 e 40 da LGPD, e ainda compulsoriamente, em caso de ocorrência de incidente de segurança com possibilidade de acarretar risco ou dano relevante aos titulares, segundo o Caput do Art. 48, o controlador deve "[...] comunicar à autoridade nacional e ao titular [...]" (Lei n.º 13.709, 2018) quando deverá informar pelo mesmo o que cita os Incisos I a VI, do Art. 48 (Lei n.º 13.709, 2018) .

Ao operador, de acordo com Inciso I, do Parágrafo 1.º, do Art. 42, além de seguir estritamente as determinações do controlador para o tratamento de dados, tem a obrigação de verificar o que as normas sobre a matéria de proteção de dados explicitam (Lei n.º 13.709, 2018). Portanto, o ônus da prova recai primeiramente sobre os agentes de tratamento de dados, e esses devem estar munidos de documentação necessária a fim de salvaguardar-se para que respondam a possíveis processos.

Em síntese, por manterem o contato direto com os dados e os manipularem, o controlador e o operador devem se resguardar na medida do possível, cumprindo estritamente o que está na lei, e tendo plena consciência que pelos seus atos podem responder pessoalmente processos que resultaram em sanções pecuniárias. Com isso, muitas das ações que o controlador pode implementar dentro da empresa devem estar com a finalidade de sanar os problemas com a privacidade dos dados e o processo de tratamento destes (Pimenta et al., 2016) seguindo o que está na LGPD. Por isso torna-se uma atividade obrigatória, a de confrontar o que está na legislação e a realidade do processo de tratamento de dados, para os controladores, principalmente aqueles que representam as empresas que tratam os dados, identificar as falhas, entender que a proteção e a privacidade das informações é um princípio constitucional que devem ser os guias básicos para evitar a formação de passivos contingentes.

No tocante ao tópico das Boas Práticas e de Governança de Dados,

> [...] ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular [...] (Lei n.º 13.709, 2018, Art. 50, §1.º).

Essas regras além de estabelecer padrões de conduta também estabelecem padrões técnicos que passam a ser um compromisso do controlador com os dados que estão sob sua responsabilidade e que poderão ser publicadas periodicamente, em concordância com o

Parágrafo 3.º, do Art. 50 da LGPD, como uma forma de criar um círculo virtuoso para as demais organizações, além é claro de dar visibilidade a entidade pioneira na prática dessas regras (Lei n.º 13.709, 2018) .

Os padrões em relação às boas práticas e de governança antes de tudo precisam cumprir os Cinco Domínios da Governança de Dados (Khatri & Brown, 2010) e poderão virar regras

> [..] que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (Lei n.º 13.709, 2018, Art. 50).

Diante do exposto, essas regras passam a ser um pacto social na qual compromete as decisões da alta administração (Terra, 2018) e se mostram uma valiosa forma de mitigar os riscos no que diz respeito ao aparecimento de passivos contingentes no processo de tratamento de dados. Por outro lado, segundo o Inciso IV, do Art. 52, se o compromisso não for cumprido de forma plena pode acarretar danos à imagem da empresa com a publicização da infração, além da ponderação da penalidade por conta de "adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados" e também da falta da "adoção de política de boas práticas e governança", conforme explicitam respectivamente os Incisos VIII e IX, do §1.º ,do Art. 52, que foram criadas como um compromisso da entidade perante à sociedade e à autoridade nacional e poderão agravar as sanções administrativas as quais estão sujeitas (Lei n.º 13.709, 2018) .

Portanto, a falha na implementação das regras de boas práticas e de governança pode representar uma regressão aos esforços da empresa em cuidar da privacidade dos dados, perda de recursos de tempo e financeiros, além da possível redução na confiança depositada pelos proprietários dos dados na empresa que efetua o tratamento.

5 Considerações Finais

Tendo como principal base a Lei Geral de Proteção de Dados (LGPD), o presente estudo observou alguns passivos contingentes que podem ser formados pela inobservância adequada da legislação. Com isso, pode-se afirmar que caso as entidades não atendam os principais requisitos propostos na LGPD, os custos, como vistos no Art. 52 da Lei, podem ser, além de financeiros, os de causar danos, principalmente, na reputação, dado que, a entidade será vista como não confiável e poderá perder seu valor explícito e implícito de mercado. Além disso, haverá dispêndio para sanar todos os prejuízos causados, bem como a exposição de fiscalizações por parte dos reguladores, que no caso é a Autoridade Nacional de Proteção de Dados (ANPD).

Os pontos de controle mais relevantes da não-observância da lei foram: gestão de dados eficiente e segura, estruturação e gestão dos dados, mapeamento do conjunto de dados, dado pessoal e anonimizado, consentimento do titular dos dados, término do tratamento dos dados, os agentes de tratamento, sistema de gerenciamento de dados, segurança e sigilo dos dados, risco pessoal dos agentes de tratamento e as boas práticas de governança corporativa. Cada um destes foi demonstrado de forma explicativa, desenvolvendo reflexões sobre um possível aparecimento de passivo contingente.

Sendo assim, como foi analisado, os principais pontos em que poderá haver a formação de passivos contingente é caso a empresa: adote licenças de sistemas não confiáveis ou que não ofereçam suporte necessário para o resguardo das informações, não ter ou não executar as práticas de governança de dados, não adquirir mecanismos de segurança e sigilo da informação, agentes de tratamento não conscientes dos riscos envolvidos e não treinados o suficiente ou

que não realizem o trabalho de forma competente e, por fim, ignorar o término consentimento do titular dos dados e para quais finalidades os dados foram cedidos.

Portanto, pode-se considerar que as companhias podem precisar rever sua cultura organizacional para tratar as informações a elas confiadas de forma responsável e, consequentemente, estarem alinhadas quanto a todas as imposições propostas pela legislação a fim de evitar futuros desembolsos em litígios formados exatamente por passivos contingentes.

A conscientização dos agentes de tratamento também é outro ponto a ser destacado. Apesar dos dados em boa parte serem automatizados, o responsável pela utilização das informações são os seres humanos, passíveis de falhas que podem causar grandes vazamentos. Nessa perspectiva, é importante que haja reeducação dos funcionários atuantes no setor de tratamento de dados apresentando os possíveis perigos e as formas mais apropriadas de mitigá-los.

Nesse sentido, o estudo contribui com a análise da Lei Geral de Proteção de Dados, bem como o preenchimento de estudos relacionados a passivos contingentes que podem ser formados a partir de alguma legislação. Além disso, deve-se ressaltar que a disciplina de proteção de dados pessoais diz respeito a uma matéria em constante evolução e que o ordenamento jurídico brasileiro deve ficar atento para os desenvolvimentos tecnológicos que cotidianamente alteram a vida dos cidadãos (Mendes & Doneda, 2018).

Por fim, como limitações da pesquisa, pode ser trazido o fato da lei ser recente e por isso não há tantos materiais, se comparado a outras leis mais conhecidas como a Lei que dispõe sobre as Sociedade por Ações (*Lei n.º 6.404*, 1976). Para futuros trabalhos, sugere-se: [a] o aprofundamento da legislação, buscando jurisprudências em tribunais superiores; [b] a utilização de mecanismos para averiguar se as empresas estão em conformidade com a LGPD, como aplicação de questionários e; [c] estudos de casos práticos como processos judiciais, fontes comuns de passivos contingentes.

REFERÊNCIAS

Alcântara, V. D. C., Pereira, J. R., & Silva, É. A. F. (2015). Gestão Social e Governança Pública: Aproximações e (de)limitações teórico-conceituais. *Revista de Ciências da Administração*, *1*(3), 11. https://doi.org/10.5007/2175-8077.2015v17nespp11

Lei n.º 6.404, de 15 de dezembro de 1976, Presidência da República, Diário Oficial da União (1976), Dispõe sobre as Sociedades por Ações. http://www.planalto.gov.br/ccivil_03/LEIS/L6404compilada.htm

Lei n.º 10.406, de 10 de fevereiro de 2002, Presidência da República, Diário Oficial da União (2002), Institui o Código Civil. https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm

Lei n.º 13.709, de 14 de agosto de 2018, Presidência da República, Diário Oficial da União (2018), Dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD). http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm

Pronunciamento Técnico CPC 25, de 26 de junho de 2009, Comitê de Pronunciamentos Contábeis (2009) (testimony of Conselho Federal de Contabilidade Brasil), Dispõe sobre Provisões, Passivos Contingentes e Ativos Contingente. http://static.cpc.aatb.com.br/Documentos/304_CPC_25_rev%2014.pdf

Pronunciamento Técnico CPC 00 (R2), de 01 de novembro de 2019, Comitê de Pronunciamentos Contábeis (2019) (testimony of Conselho Federal de Contabilidade Brasil), Dispõe sobre a estrutura conceitual para relatório financeiro. http://static.cpc.aatb.com.br/Documentos/573_CPC00(R2).pdf

Capanema, W. A. ([s.d.]). A responsabilidade civil na Lei Geral de Proteção de Dados. *Cadernos Jurídicos: Direito Digital e proteção de dados pessoais*, *21*(53), 163–170.

Recuperado 17 de junho de 2021, de https://core.ac.uk/reader/322682320

Castro, R. G., & Lima, D. V. (1999). *Auditoria para concursos* (1º ed). Vestcon.

Cortez, I. S., & Kubota, L. C. (2013). Contramedidas em segurança da informação e vulnerabilidade cibernética: Evidência empírica de empresas brasileiras. *Revista de Administração (São Paulo)*, *48*(4), 757–769. https://doi.org/10.5700/rausp1119

Cruz, J. A. G. da. (2015). *Mapeamento de bancos de dados para domínios semânticos* [Dissertação (Mestrado em Ciência da Computação), Universidade Federal de Goiás]. http://repositorio.bc.ufg.br/tede/handle/tede/4639

Fonseca, J. S. da F. (2002). *Metodologia da pesquisa científica* (1º ed). UECE.

Fontes, E. L. G., Balloni, A. J., & Laudon, K. C. (2007). A segurança de sistemas da informação: Aspectos sociotécnicos. In A. J. Balloni (Org.), *Por que GESITI: segurança, inovação e sociedade*. Komedi.

Gil, A. C. (2010). *Como elaborar projetos de pesquisa*. Atlas.

Gil, A. de L., Biancolino, C. A., & Borges, T. N. (2010). *Sistemas de Informações Contábeis: Uma abordagem gerencial*. Saraiva.

IOB. (2020, novembro 13). LGPD - Escritório de Contabilidade. *IOB On Line*. https://www.iobonline.com.br/pages/coreonline/coreonlineDocuments.jsf?guid=IAE8138295595342EE05363B5DE0A18CA&nota=1&tipodoc=3&esfera=FE&ls=2&index=1#highlight-1

Iudícibus, S. de, Martins, E., & Gelbcke, E. R. (2018). *Manual de contabilidade societária* (3º ed). Atlas.

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the Association for Computing Machinery (ACM)*, *53*(1), 148–152. https://doi.org/10.1145/1629175.1629210

Konzen, M. P. (2013). *GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO BASEADA NA NORMA NBR ISO/IEC 27005 USANDO PADRÕES DE SEGURANÇA*. http://repositorio.ufsm.br/handle/1/8276

Laudon, K. C., & Laudon, J. P. (2014). *Sistemas de informação gerenciais* (11º ed). Pearson Educacion Brasil Ltda.

Machado, S. B. C., & Bianchini, D. (2016). Efetividade em Gerencia de projetos e Segurança da Informação: Uma proposta para Cidades Inteligentes. *Brazilian Technology Symposium*, *1*, 5.

Melo, L. P. de. (2008). *Proposta de metodologia de gestão de risco em ambientes corporativos na área de TI* [Dissertação (Mestrado em Engenharia Elétrica), Universidade de Brasília]. https://repositorio.unb.br/bitstream/10482/1628/1/2008_LaertePeottaDeMelo.pdf

Mendes, L. S., & Doneda, D. (2020). Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista Direito do Consumidor*, *120*, 469–483.

Nassif, M. E., & Resende, W. da C. (2016). Gestão da informação e do conhecimento e suas relações com segurança da informação, tecnologias da informação e compartilhamento. *Ciência da Informação*, *45*(3), Article 3. http://revista.ibict.br/ciinf/article/view/4052

Ohtoshi, P. H. (2013). *O comportamento informacional: Estudo com especialistas em segurança da informação e criptografia integrantes da RENASIC/COMSIC* [Dissertação (Faculdade de Ciência da Informação), Universidade de Brasília]. https://repositorio.unb.br/handle/10482/14394

Pereira, K., Conte, T., & Feitosa, E. (2015). IHC e Segurança: Avaliando do Risco de Usuários.

In *IHC 2015—Livro dos Tutoriais* (p. 59; 85). https://www.researchgate.net/profile/Eduardo-Feitosa/publication/284183707_IHC_e_Seguranca_Avaliando_do_Risco_de_Usuarios/links/564f125f08ae4988a7a7f74d/IHC-e-Seguranca-Avaliando-do-Risco-de-Usuarios.pdf

Pimenta, A. M. S., Quaresma, R. F. C., Pimenta, A. M. S., & Quaresma, R. F. C. (2016). A segurança dos sistemas de informação e o comportamento dos usuários. *JISTEM - Journal of Information Systems and Technology Management*, *13*(3), 533–552. https://doi.org/10.4301/s1807-17752016000300010

Pinheiro, P. P. (2020). *Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD* (1º ed). Saraiva Educação SA.

Ramos, A. L. S. C. (2012). *Direito Empresarial Esquematizado* . (4º ed). Grupo Gen-Método.

Raupp, F. M., & Beuren, I. M. (2006). Metodologia da pesquisa aplicável às ciências. In I. M. Beuren (Org.), *Como elaborar trabalhos monográficos em contabilidade: Teoria e prática. São Paulo: Atlas* (3º ed, p. 76–97). Atlas.

Richardson, R. J., Peres, J. A. S., Wanderley, J. C. V., Correia, L. M., & Peres, M. H. M. (1999). *Pesquisa social: Métodos e técnicas* (3º ed). Atlas.

Santos, D. L. dos. (2014). *Controle de acesso em sistemas gerenciadores de banco de dados* [Especialização (Configuração e Gerenciamento de Servidores e Equipamentos de Rede), Universidade Tecnológica Federal do Paraná.]. http://repositorio.utfpr.edu.br:8080/jspui/handle/1/17300

Santos, I. M. R. (2019). *O legítimo interesse do controlador ou de terceiro no tratamento de dados pessoais* [Monografia (Faculdade de Direito), Universidade de Brasília]. https://bdm.unb.br/handle/10483/23535

Sayão, L. F., & Sales, L. F. (2015). *Guia de gestão de dados de pesquisa para bibliotecários e pesquisadores.* Instituto de Engenharia Nuclear. http://carpedien.ien.gov.br:8080/handle/ien/1624

Souza, L. C. (2020). Estrutura lógica de organização da pesquisa científica: Texto básico para auxiliar pesquisadores (1º ed). Editora UEMG.

Terra, P. de M. (2018). *A influência da governança de dados na gestão estratégica* [Monografia (graduação em Sistemas da Informação), Universidade Federal Fluminese]. https://app.uff.br/riuff/handle/1/7580