UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
FACULDADE DE ADMINISTRAÇÃO E CIÊNCIAS CONTÁBEIS
CURSO DE CIÊNCIAS CONTÁBEIS

ÉRICA DOS SANTOS DE FREITAS

ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E SUA APLICAÇÃO NAS EMPRESAS DE CONTABILIDADE

Belford Roxo
2022

ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E SUA APLICAÇÃO NAS EMPRESAS DE CONTABILIDADE

Trabalho de conclusão de Curso apresentado ao curso de CiênciasContábeis, Faculdade de Administração e Ciências Contábeis da Universidade Federaldo Rio de Janeiro, para obtenção do títulode bacharel em Contabilidade.

Orientador: Prof. Edson da Rocha

Belford Roxo

2022

ÉRICA DOS SANTOS DE FREITAS

ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E SUA APLICAÇÃO NAS EMPRESAS DE CONTABILIDADE

Trabalho de conclusão de Curso apresentado ao curso de Ciências Contábeis, Faculdade de Administração e Ciências Contábeis da Universidade Federal do Rio deJaneiro, para obtenção do título de bacharel em Contabilidade.

Belford Roxo, 16 de dezembro de 2022.

Orientador – Prof. Esp. Edson da Rocha

Universidade Federal do Rio de Janeiro - UFRJ - (Consórcio Cederj)

Profª. Drª. Marília Cecília Carvalho Chaves

Universidade Federal do Rio de Janeiro - UFRJ

Profª. Drª. Márcia Maria Machado Pereira
Universidade Federal do Rio de Janeiro - UFRJ

Ficha Catalográfica

CIP - Catalogação na Publicação

d722a

dos Santos de Freitas, Érica
ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E SUA APLICAÇÃO NAS EMPRESAS DE CONTABILIDADE / Érica dos Santos de Freitas. -- Rio de Janeiro, 2022.
26 f.

Orientador: Edson da Rocha.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Administração e Ciências Contábeis, Bacharel em Ciências Contábeis, 2022.

1. Dados. 2. Lei Geral de Proteção de Dados. 3. Empresas de Contabilidade. I. da Rocha, Edson, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

RESUMO

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018) dispõe sobre o tratamento de dados pessoais, inclusive por meios digitais, por pessoa natural ou jurídica. A implantação da lei propõe maior comprometimento com a segurança e transparência em relação ao tratamento dos dados, propiciando a pessoa natural maior proteção ao seu direito de liberdade e de privacidade e o livre desenvolvimento de sua personalidade. O objetivo deste estudo é analisar a aplicabilidade da Lei Geral de Proteção de Dados nas empresas de contabilidade. . A proteção de dados pessoais é de suma importância dada a vulnerabilidade dos titulares na maioria dos casos e a forma como os dados pessoais são divulgados e tratados. Ante o exposto, pretende-se responder ao seguinte questionamento: como se aplicar, de forma eficaz, a aplicação da Lei Geral de Proteção de Dados às Empresas de Contabilidade? Conclui-se que os escritórios contábeis estão preparados para aplicação da Lei Geral de Proteção de Dados, uma vez que consideram indispensável o consentimento do titular para o tratamento dos dados, atendem aos princípios previstos na lei e adotam as medidas de segurança necessárias. Esta pesquisa contribui para enfatizar a importância da lei para sociedade, trazendo para as empresas mais clareza a respeito da regulação sobre coleta, tratamento, armazenamento e compartilhamento dos dados, e garantindo aos cidadãos mais privacidade e proteção dos seus dados.

Palavras-chave: Dados, Lei Geral de Proteção de Dados, Empresas de Contabilidade.

ABSTRACT

The General Law for the Protection of Personal Data (Law No. 13,709, of August 14, 2018) provides for the processing of personal data, including by digital means, by natural or legal persons. The implementation of the law proposes a greater commitment to security and transparency in relation to the processing of data, providing individuals with greater protection of their right to freedom and privacy and the free development of their personality. The objective of this study is to analyze the applicability of the General Data Protection Law in accounting companies. The protection of personal data is of paramount importance given the vulnerability of holders in most cases and the way in which personal data is disclosed and treated. In view of the above, it is intended to answer the following question: how to effectively apply the application of the General Data Protection Law to Accounting Firms? It is concluded that the accounting offices are prepared for the application of the General Data Protection Law, since they consider essential the consent of the holder for the processing of data, comply with the principles set forth in the law and adopt the necessary security measures. This research contributes to emphasize the importance of the law for society, bringing more clarity to companies regarding the regulation on data collection, treatment, storage and sharing, and guaranteeing citizens more privacy and protection of their data.

Keywords: Data, General Data Protection Law, Accounting Companies.

SUMÁRIO

1 INTRODUÇÃO

O mundo da tecnologia cria novas formas de comunicação e facilita as interações, por isso é preciso ter cuidado com os dados que são compartilhados, pois quase todo clique é rastreado, tornando-o inseguro. Entende-se por dados pessoais toda e qualquer informação que permita a identificação de uma pessoa singular, seja pelo nome próprio, apelido, morada, rendimentos, localização, e-mail, hábitos de navegação ou consumo.

Os dados pessoais são utilizados em diversos contextos, pelo que, como os dados pessoais são muitas vezes utilizados sem o consentimento do titular, não é raro que a segurança desses dados seja negligenciada e a vida privada do titularnão seja protegida. No entanto, o direito à privacidade é a necessidade de permitir espaço para o desenvolvimento particular dos indivíduos e de sua individualidade sem a intervenção de terceiros, com ou sem poder público.

Quando se trata de proteção de dados, pode-se pensar que apenas empresas de tecnologia devem se adequar à nova lei, mas a LGPD atinge todas as empresas, públicas ou privadas, e todos os ramos de atividade, que demandam dados de seus clientes, cliente interno ou externo. A proteção de dados pessoais é de suma importância dada a vulnerabilidade dos titulares na maioria dos casos e a forma como os dados pessoais são divulgados e tratados. Ante o exposto, pretende-se responder ao seguinte questionamento: como se aplicar, de forma eficaz, a aplicação da Lei Geral de Proteção de Dados às Empresas de Contabilidade?

Para tal, este estudo, é fruto de uma revisão bibliográfica, com abordagem qualitativa e enfoque descritivo, quanto à finalidade. Mediante a todo embasamento teórico consolidado os resultados apurados permitiram alcançar uma compreensão mais detalhada sobre a literatura que aborda a temática, se estabelecendo um bom embasamento teórico que contribui significativamente para a consistência da investigação proposta.

2 DESENVOLVIMENTO

2.1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

No Brasil, a Constituição Federal de 1988 apresenta, em seu inciso X, do art. 5º, como direito fundamental e inviolável, a privacidade, a vida privada e a imagem das pessoas, não só este, mas também a inviolabilidade do sigilo da correspondência, podendo haver indenização por danos materiais ou morais decorrentes de sua violação (BRASIL, 1988).

De acordo com a Lei nº 10.406, de 10 de janeiro de 2002, que institui o Código Civil, em seu “Art. 1º. “toda pessoa é capaz de direitos e deveres na ordem civil.”. Isso significa que todo ser humano é capaz de direitos ou obrigações por meio de um conjunto de leis e princípios que regem o comportamento e os interesses particulares da sociedade.

De acordo com art. 1º da LGPD, Lei n° 13.709, de 14 de agosto de 2018, a mesma aplica-se a qualquer tratamento de dados de qualquer forma por pessoa física ou jurídica de direito público ou privado:

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

A Lei Geral de Proteção de Dados Pessoais foi sancionada no dia 14 de agosto de 2018 e deveria entrar em vigor após 24 meses de sua publicação, ou seja, em agosto de 2020, mas devido à pandemia causada pelo novo coronavírus (COVID-19), entrou em vigor somente em maio de 2021, conforme previsto namedida provisória 959, de 2020, válida em todo o território do país e sobrepondo-sea qualquer lei estadual ou municipal (KRÜGER, 2022).

Entende-se que o hiato foi necessário para que as organizações cumprissem as novas obrigações relativas ao uso, armazenamento e proteção de dados pessoais e tempo suficiente para a constituição de uma autoridade fiscalizadoralegal (Autoridade Nacional de Proteção de Dados - ANPD) e foi prorrogado em razãoda a difícil situação em que todas as organizações se encontram naquele momento de crise, não só no Brasil, mas em todo o mundo.

A lei é baseada no GPDR (Regulamento Europeu de Proteção de Dados) e

especifica como as empresas devem usar os dados pessoais quando se trata de uma pessoa física identificada ou identificável. A LGPD surgiu para preservar os direitos constitucionais de todos os cidadãos à liberdade e à privacidade,protegendo-os de qualquer dano (DA CRUZ; PASSAROTO & JUNIOR, 2021).

Segundo Câmara (2020):

> Essa Lei define que deverão estar em conformidade tanto a portaria de um prédio, que registra os dados dos visitantes em um livro, quanto um laboratório de análises clínicas que registra os dados pessoais de seus funcionários na área de RH e disponibiliza osresultados das análises clínicas dos clientes na Web. Esta é a primeira Lei que punirá por inércia: além de as instituições serem obrigadas a se adequar à Lei, deverão demonstrar (evidenciar) a sua conformidade, tanto para o titular quanto para a autoridade nacional, para evitarem as penalizações (CÂMARA, 2020, p.10)

Até que a lei entrasse em vigor, as empresas deveriam seguir as diretrizes contidas em leis esparsas, como a Lei de Sigilo Bancário, o Marco Civil da Internet e a Lei de Proteção ao Consumidor. Assim, o surgimento da lei exigiu a observação de como os dados são processados, não apenas porque a privacidade deve ser respeitada (PEITER et al., 2019). A proteção de dados é uma evolução dos requisitos humanos, o maior diferencial é a visão moderna de como tratar os dados, sempre observando a finalidade do tratamento, e deixando o cidadão possuir, ter a propriedade dos dados, porque ele é o único titular.

De acordo com Pimentel (2022), os fundamentos da proteção de dados disciplinados pela LGPD são:

> O respeito a privacidade, autodeterminação informativa, liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico, tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (PIMENTEL, 2022, p.12).

A Lei Geral de Proteção de Dados Pessoais visa proteger os direitos fundamentais de liberdade e privacidade e a livre formação da personalidade de cada pessoa. A lei regulamenta o tratamento de dados por pessoas físicas ou

jurídicas de direito público ou privado e abrange diversas operações realizadas de forma manual ou digital.

A lei se aplica para pessoa física ou jurídica que gerem uma base para fins económicos; dados tratados em território nacional, independentemente do método utilizado; dados utilizados para o fornecimento de bens ou serviços. A lei não se aplica a dados originados fora do Brasil e não sujeitos a transferências internacionais, para fins jornalísticos e artísticos; segurança pública; defesa nacional; segurança nacional; investigação e repressão de infrações penais; e pessoas físicas (RIBEIRO et al., 2022).

A LGPD nos traz, em seu art. 6°, os princípios que devem ser seguidos ao realizar tratamentos de dados pessoais:

> 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.

Uma vez que o tratamento de dados envolve uma invasão da vida pessoal do titular dos dados, os princípios estabelecidos por lei devem ser observados e o titular

dos dados tem total liberdade para aceitar ou rejeitar tal tratamento e saber quais os dados que serão tratados e para que finalidades.

Segundo Santos (2021) comissão europeia define dados pessoais como:

> Dados pessoais são informação relativa a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa. Dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, mas que possam ser utilizados para reidentificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do RGPD. Dados pessoais que tenham sido tornados anónimos de modo a que a pessoa não seja ou deixe de ser identificável deixam de ser considerados dados pessoais. Para que os dados sejam verdadeiramente anonimizados, a anonimização tem de ser irreversível (SANTOS, 2021, p.8).

Exemplos de dados pessoais incluem nome, endereço residencial ou de e-mail, número de identificação, dados de localização, endereço IP, seu número de telefone e até dados de um hospital ou médico que possam identificar uma pessoa (RIGO, 2021). Dados pessoais são o acúmulo de fatos e eventos que moldam a personalidade de cada indivíduo, e os dados pessoais podem contar com precisão a história de vida de cada cidadão.

De acordo com a LGPD, os dados são divididos em três tipos, dados pessoais, dados pessoais sensíveis e dados anônimos. Toda e qualquer informação que possa estar associada a uma pessoa identificada ou identificável é considerada dados pessoais. Dados pessoais sensíveis são quaisquer dados que possam levar a algum tipo de discriminação, como religião, vida sexual, dados genéticos. Dados anônimos são dados que não estão mais diretamente relacionados a uma pessoa, ou seja, quando o conjunto de dados passa a ser dados estatísticos (DE CARVALHO e FREITAG, 2021).

Detentor ou titular é entendido como o indivíduo que possui os dados pessoais a serem processados e que deve autorizar ou não o processamento dos dados. O agente de tratamento é o controlador e o operador. O controlador é responsável pelas decisões relacionadas ao processamento de dados pessoais e por quaisquer eventos que possam ocorrer. O operador é a pessoa que trata os dados e deve obedecer a todos os comandos do responsável pelo tratamentorelativamente ao tratamento dos dados. O responsável pela comunicação entre o titular, o controlador e a autoridade nacional de proteção de dados são chamados de

responsáveis (SCHERER FILHO, 2020).

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável pela implementação e administração das normas da LGPD, garantindo o cumprimento da lei, realizando auditorias e impondo as sanções cabíveis em caso de infração à lei.

2.1 Tratamento de dados

Tratamento de acordo a LGPD é:

> 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 (BRASIL, 2018).

A LGPD se aplica a todo e qualquer processamento de dados realizado por pessoas físicas ou jurídicas e para fins comerciais, desde que o processamento ocorra total ou parcialmente no território nacional. Esta lei não se aplica ao tratamento de dados para fins não econômicos, ou para fins jornalísticos e artísticos,no âmbito da segurança pública, defesa nacional e nacional, e dados originados no exterior e não compartilhados com agentes.

A Lei Geral de Proteção de Dados traz outros conceitos interessantes para que haja ou não o tratamento de dados:

> **Consentimento:** permissão dada pelo titular para que determinado(s) dado(s) pessoal(is) seja(m) tratado(s). Deve ser pedido de forma explícita, clara e transparente pelo operador ou controlador, e se referir a uso específico e limitado.
> **Bloqueio:** suspensão do tratamento de dados, que não isenta o operador e o controlador de precisarem proteger os dados pessoais e o banco de dados em que eles se encontram (BRASIL, 2018).

2.1.2 Eliminação: exclusão de dados pessoais.

O consentimento para o processamento de dados é uma parte importante do respeito ao direito à liberdade de escolha e deve ser livre, informado, claro, específico, determinado e expresso. O consentimento é a principal ferramenta para otratamento de dados e deve respeitar a forma prescrita por lei, seja por escrito oupor qualquer meio que indique a vontade do titular dos dados (MOREIRA, 2022). O titular pode retirar tal consentimento a qualquer momento.

O consentimento nem sempre é obrigatório e não é necessário para instituições de pesquisa onde o tratamento se destina a cumprir a lei e a política pública, mas devem usar dados anônimos sempre que possível, ao fazer cumprir contratos ou exercer direitos regularmente, o que é um caso de litígio e um casopara proteger a saúde e proteger a vida (COUTO et al., 2022).

Em casos excecionais em que não seja necessário o consentimento do titular dos dados, o responsável pelo tratamento deve obter novamente o consentimento do titular dos dados se o tratamento for necessário para outros fins, mesmo que o responsável pelo tratamento já possua os dados.

2.2 DA SEGURANÇA DOS DADOS PESSOAIS

A segurança pode ser entendida como uma série de medidas destinadas a proteger pessoas ou coisas de riscos, perigos ou perdas. Em muitos casos, a segurança da informação nas empresas garante a continuidade dos negócios, aumenta a estabilidade e mantém pessoas e bens protegidos de ameaças e perigos (KRÜGER et al., 2022). As perdas não são apenas monetárias, pois também existem custos que podem ser difíceis de calcular, como perda de reputação ou publicidade negativa.

Os dados pessoais e confidenciais são exponencialmente valiosos e, se esses dados forem roubados ou perdidos, pode ser muito caro para uma empresa recuperá-los ou compensar o impacto dos danos causados. Além das multas em dinheiro, você corre o risco de perder a confiança de seus clientes, investidores e parceiros.

As pessoas não sabem o quanto seus dados pessoais são valiosos para o

mercado, nem como são coletados, armazenados e compartilhados, portanto, uma simples falha de segurança pode deixá-los expostos (DA CRUZ; PASSAROTO e JUNIOR, 2021).

De acordo com Câmara (2020):

> Diariamente, algoritmos são alimentados por informações pessoais que indicam como pensamos e quais os nossos desejos, criando perfis de consumo dos usuários, para fins de publicidade direcionada e venda desses dados pessoais para outras empresas. Nesse sentido, a proteção da privacidade passa pela proliferação dessas práticas comerciais de “big data”, “targeting” e “profiling” dos usuários, deixando as pessoas presas dentro de uma realidade on-line customizada (“tailored reality”).

A maioria das pessoas, ao fazer compras online, já se deparou com a necessidade de preencher formulários cadastrais com diversos dados pessoais, o que teoricamente é inútil. Hoje em dia, para programas de educação fiscal, informaro CPF no momento da compra é fundamental, mas nem todos os dados exigidos são necessários.

O que as pessoas não sabem é que esses dados estão sendo registrados, seja para criar perfis de usuários, para entregar conteúdo publicitário direcionado ou para vendê-los para outras empresas. A vida em uma sociedade hiperconectada é determinada por algoritmos automatizados, e parte do processamento desses algoritmos é feito por inteligência artificial (PIMENTEL, 2022). No entanto, de acordo com a LGPD, é possível solicitar a exclusão desses dados após o término da relação comercial entre as partes.

O artigo 18 da LGPD dispõe sobre o direito ao apagamento dos dados, que estabelece que o titular pode, a qualquer momento, solicitar ao controlador que:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II- acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo coma regulamentação da autoridade nacional, observados os segredos comercial e industrial;

> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas noart.16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do §5º do art.8ºdesta Lei.

As organizações que processam dados pessoais também devem estar sempre em conformidade com a LGPD, pois devem seguir as regras e implementar os procedimentos necessários para manter os dados seguros e evitar penalidades previsíveis.

2.2.1 Gestão em casos de vazamentos de Dados

Segundo o dicionário: "Um incidente é um evento ou circunstância inesperada que altera a ordem normal das coisas". Quando se trata de incidentes relacionados a dados, o impacto é variado e as leis atuais de proteção de dados garantem consequências e penalidades. Uma empresa mantém um banco de dados contendo uma série de informações pessoais de clientes ou funcionários, que devem ser mantidas em segurança (RIBEIRO et al., 2022). Para tanto, é necessário tomar medidas para evitar vazamentos ou incidentes que possam comprometer a proteção de dados e a imagem da empresa.

O custo de prevenir uma ameaça deve ser menor do que o custo de recuperá-la quando ela atingir você. É mais viável que as empresas tomem medidas preventivas e façam análises de risco, ao invés de assumirem multas de até 2% de seu faturamento, que podem chegar a até 50 milhões por infração dependendo do faturamento da empresa (SANTOS, 2021).

Nos termos do artigo 48 da Lei 13.709/18 (Lei Geral de Proteção de Dados), o controlador é obrigado a informar as autoridades nacionais e o titular de qualquer incidente de segurança que possa representar um risco para o titular, o que deve ser feito em um prazo razoável, mencione pelo menos:

> I - a descrição da natureza dos dados pessoais afetados;
> II- as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV – os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata;
> VI – as medidas que foram ou que serão adotadas para rever ter ou mitigar os efeitos do prejuízo.

Os principais tópicos no tratamento adequado de um incidente de segurança são a preparação prévia de um plano de resposta a incidentes, a comunicação adequada com as autoridades nacionais e os titulares e a adoção de medidas para mitigar ou compensar o risco ou dano causado.

Quanto ao plano de resposta a incidentes, este deve incluir todos os colaboradores da empresa, mesmo os de baixo escalão, pois devem ser obrigados a reportar eventuais violações operacionais relacionadas à proteção de dados, que podem resultar em penalidades caso não sejam notificados, sendo necessário criar um fluxo de comunicação que facilita a chegada de informações de violação de dados para a ação (RIGO, 2021). Os prestadores de serviços que processam dados também devem ser incluídos no plano.

Qualquer incidente e violação de dados deve ser comunicado à autoridade nacional de proteção de dados e ao titular. Os controladores devem analisar, junto com as autoridades nacionais, quais medidas são necessárias para eliminar os riscos apresentados pelos eventos (DE CARVALHO e FREITAS, 2021). Quanto à comunicação com os titulares, ela deve ser o mais transparente possível e feita de forma estratégica.

Relatório de impacto à proteção de dados pessoais de acordo com o art. 5º da LGPD:

> XVII- relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salva guardas e mecanismos de mitigação de risco.

Sempre que um determinado tratamento de dados possa criar um risco de dano para o titular dos dados, o responsável pelo tratamento deve manter umrelatório de impacto na proteção de dados pessoais de forma a compreender os perigos envolvidos em cada evento. Este relatório é um documento que contém uma

descrição dos processos de tratamento de dados pessoais que podem criar riscos, bem como as medidas e mecanismos de mitigação de riscos. Com ela, justifica-se o devido cuidado em evitar tais riscos no tratamento de dados.

De acordo com o art.38 da Lei Geral de Proteção de Dados Pessoais:

> Art.38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredoscomercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Um oficial de proteção de dados pode ser alguém de TI, jurídico, não importa. É importante que quem assiste o responsável forme assessoria técnica multidisciplinar, pois só assim a legislação poderá ser organizada de forma mais eficaz.

2.3 ADAPTAÇÃO E EMPREGO DA LGPD NAS EMPRESAS DE CONTABILIDADE

Todas as empresas que coletam, armazenam e processam dados pessoais de pessoas físicas devem cumprir as disposições da Lei Geral de Proteção de Dados, incluindo escritórios de contabilidade. Essas empresas devem empregar mecanismos internos e sistemas de controle para garantir o cumprimento da lei, afim de proteger os dados pessoais de possíveis riscos de incidentes (SCHERER FILHO, 2020).

As empresas devem cumprir todos os princípios da LGPD antes de processar quaisquer dados pessoais, e para isso é necessário demonstrar que possuem o consentimento dos titulares e que dispõem de infraestrutura para garantir a segurança de todas as informações. Portanto, a certificação ISO 27001 pode ser confiável (MOREIRA, 2022).

De acordo com Hasse (2021):

> A ISO 27001 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, privada ou pública, pequenaou grande. Ela é escrita pelos melhores especialistas mundiais no campo de segurança da informação e provê metodologia para aimplementação da gestão da segurança da informação em uma organização. Ela também possibilita que organizações obtenham certificação, o que significa que um organismo certificador independente confirmou que uma organização implementou a segurança da informação em conformidade comaISO27001.

Implementar a LGPD em um escritório de contabilidade, assim como em qualquer outro tipo de organização, não é uma tarefa fácil, mas é uma lei que deve ser rigorosamente cumprida para garantir a proteção dos dados pessoais de seu trabalho e evitar penalidades. Para isso, é necessário realizar análises de risco e tomar medidas preventivas para adequar a execução das atividades organizacionais às normas.

Segundo Hasse (2021), uma equipe de TI bem treinada pode contribuir muito para a segurança dos dados de uma empresa, e riscos significativos podem ser evitados com o estabelecimento de políticas internas sobre o uso de recursos digitais. Além de tomar todas as providências possíveis, é importante elaborar relatórios de riscos, destacando os pontos fracos, os riscos enfrentados por cada departamento da empresa, bem como os incidentes ocorridos e como foram solucionados, para que a criação de políticas internas seja direcionada e tem uma maior eficácia de impacto.

2.3.1 Dados tratados em Empresas de Contabilidade

O surgimento da LGPD, juntamente com as obrigações práticas e novas práticas que impõe aos empregadores (agora controladores) e, em última análise, as consequências administrativas do descumprimento, forçou a necessidade de reexaminar a natureza das informações pessoais e a maneira como elas são devem ser tratados nas empresas (MOREIRA, 2020). A nova legislação estabelece regras claras sobre como as organizações devem coletar, armazenar e compartilhar dados pessoais dos usuários, seja por meio digital ou físico. Assim como qualquer organização, os escritórios devem cumprir os requisitos legais.

Os profissionais já cumprem o Código de Ética do Contador, que trata do sigilo de dados e informações sigilosas e, a partir de sua vigência, também devem cumprir os princípios da Lei Geral de Proteção de Dados sob pena de penalidades.

Os escritórios de contabilidade não apenas processam dados de seus clientes, mas também de seus funcionários, dados de funcionários de seus clientes, como: nome, endereço residencial, e-mail, RG, CPF (COLARES, 2021). Todos esses dados são protegidos por lei e devem ser solicitados, além de informar claramente ao titular como serão tratados, para que finalidade ou se serão compartilhados.

O e-Social é um dos sistemas gerenciados pelo departamento de contabilidade que associa diversos dados de funcionários, seus familiares e até ex- funcionários da empresa, por isso é muito importante informar aos funcionários que seus dados serão coletados e repassados para o governo por meio do e-Social (COUTO et al., 2021). Embora coletar e enviar essas informações seja uma exigência legal, a transparência na relação entre uma organização e seus colaboradores é extremamente necessária.

Os departamentos de recursos humanos em escritórios e outras empresas solicitam e processam rotineiramente grandes quantidades de dados pessoais, como números de telefone, endereços residenciais e de e-mail, vários documentos pessoais e, às vezes, até registros médicos, orientação sexual, políticas e crenças religiosas. O Ministério exige dados desde o momento da pré-seleção do posto de trabalho, da celebração deste contrato de trabalho, durante a execução do contrato e até à sua cessação.

2.3.2 Impactos positivos e negativos da Lei nas empresas de contabilidade

A LGPD terá impactos positivos e negativos nos escritórios de contabilidade, já que esses escritórios lidam com grandes volumes de dados pessoais importantes. No entanto, as regras podem ser seguidas se houver preocupações com a privacidade, com as medidas e procedimentos de segurança adequados para proteger os dados (JÚNIOR e DE CARVALHO, 2022). O e-Social é um dos sistemas administrados por contadores que conecta uma série de dados de funcionários de

empresas e até mesmo de seus familiares e ex-funcionários que merecem privacidade e cuidado.

O mais importante para o escritório é a gestão dos documentos do cliente, pois cabe a ele provar perante as autoridades que está agindo dentro do marco legal. O que é certo é que se houver qualquer tipo de violação de dados, e os clientes ficarem sabendo, serão os primeiros a condenar a empresa por tal descuido e perder a credibilidade da empresa por não investir em segurança para proteger seus dados (SILVA e GILES, 2022). E mesmo que tais incidentes levem a problemas mais graves, depende de culpa e multas da empresa.

Um dos efeitos positivos dessa lei para os escritórios de contabilidade é que eles poderão se tornar mais comprometidos em manter os dados dos clientes seguros e poderão contar com a ajuda de bons profissionais de privacidade de dados nessas áreas. Eles também devem investir mais em segurança para evitar hackers e vazamento de informações importantes.

Como efeito negativo para todos e quaisquer agentes de tratamento de dados, podem ser invocadas as sanções previstas no artigo 52.º da Lei Geral de Proteção de Dados:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III -multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> VII - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelocontrolador;
> VIII - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses,prorrogável por igual período;
> IX - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Conforme mencionado acima, podem ser aplicadas sanções e multas muito severas que tenham um impacto significativo no Escritório. Além da perda de valor, o

maior impacto pode ser a falta de credibilidade da empresa, mais difícil de recuperar do que qualquer dinheiro (SCHERER FILHO, 2020). Um dos grandes investimentos feitos em uma organização contábil é a criação de responsáveis pela segurança das informações armazenadas e geradas, seja um comitê de segurança ou um órgão de processamento de dados pessoais.

2.3.3 Como as empresas de contabilidade podem se adaptar à LGPD

As empresas de contabilidade devem tomar várias medidas para cumprir a Lei Geral de Proteção de Dados. As empresas são capazes de documentar quais dados serão processados, como serão armazenados, qual software será usado, comoserão processados, com quem serão compartilhados, por quanto tempo serão armazenados e a finalidade do uso de cada dado (RIGO, 2021).

Para acomodar a LGPD, há também a necessidade de “ordenar a casa”, que envolve mapear dados, classificá-los, organizá-los de acordo com a base legal que autoriza seu processamento e, então, torná-los mais seguros. Várias mudanças devem ser feitas para garantir o cumprimento da lei e proteger as atividades (HASSE,2022). Alguns escritórios empregam provedores de software para armazenar dados na nuvem, por isso é importante entender quais são as responsabilidades desses provedores com relação aos dados, quais são suas políticas e principalmente se estão de acordo com os princípios da LGPD.

De acordo com o site Thomson Reuters (2020), as medidas que os escritórios de contabilidade devem adotar para se adaptar a LGPD, são:

> **1. Consentimento no recolhimento e uso de dados**
> A única pessoa que pode autorizar os escritórios de contabilidade a usá-los é o titular dos dados. Esse consentimento explícito deve ser reforçado especialmente em sistemas digitais.
> **2. Diferenciação entre controlador e operador**
> A Lei também exige que as empresas definam quem irá fazer uso dos dados. Isso é determinado em dois níveis de trabalho: de controlador e de operador. A responsabilidade de cada um é diferente: o controlador direcionará o que será feito com os dados. Já o operador é quem lida com eles, na prática.
> **3. Comitês de segurança da informação**
> Os escritórios de contabilidade devem criar um Comitê de Segurança da Informação para avaliação das medidas de proteção de dados próprios e dos clientes. Neste comitê haverá um profissional exclusivo, o Data Protection Officer, responsável pelo cumprimento da nova lei.
> **4. Medidas de redução de exposição**

> O escritório contábil deve utilizar técnicas de segurança administrativas e de operações diversas, implementadas de forma ampla, para que todos os colaboradores possam praticar. Isso também é parte do trabalho do comitê de segurança da informação.
> **5. Responsabilidade das terceirizadas**
> Os escritórios de contabilidade que tiverem subcontratadas devem exigir que elas também se adaptem às medidas de proteção de dados, porque estarão também sujeitas às sanções em casos de vazamentos. Assim, é fundamental ter clareza quanto aos procedimentos de segurança.

Para Couto et al (2022), a computação em nuvem é um dos recursos que mais traz utilidade aos profissionais de escritório, facilitando as interações com os clientes e a conclusão das atividades. Além disso, mantém os dados seguros e aumenta a produtividade da equipe.

Toda empresa que se dedica à coleta, armazenamento e tratamento dedados deve ter uma política interna de proteção desses dados, na qual o responsável deve ser selecionado de acordo com as regras de proteção desses dados. É importante determinar o método de obtenção do consentimento do clientee como agir em caso de violação de segurança ou violação de dados, bem como a resolução dessas situações.

CONDIDERAÇÕES FINAIS

A LGPD torna-se necessária e relevante para padronizar a forma como os dados são tratados e para garantir a segurança e transparência dos dados coletados. Esse tratamento faz parte do dia a dia dos profissionais da contabilidade e, como tal, esses profissionais serão diretamente afetados pela nova legislação. Pode-se observar que a legislação trará transparência entre os contadores e seus clientes.

A transparência é um princípio previsto na legislação, pois trará novas possibilidades, pois os titulares dos dados precisarão receber informações sobre como seus dados são processados, bem como o direito de excluir completamente o direito de encerrar o relacionamento em caso de desconforto. Vale ressaltar que a transparência é um dos principais benefícios da legislação, pois fortalece a relação de confiança entre clientes e contadores.

Há vários pontos que precisam ser melhorados, como investimento em tecnologia, para se obter um sistema que atenda as exigências da legislação. Esse é um problema que foi mostrado na pesquisa e é totalmente consistente, pois a partir do momento que um escritório tem um sistema confiável e compatível, provavelmente não terá problema com vazamento de dados pelo sistema.

A partir disso, conclui-se que a área contábil precisa entender e estudar essa nova legislação, pois os profissionais precisam dominar o assunto para transmitir informações e auxiliar seus clientes nesse processo de mudança, pois atuarão como comunicadores da legislação. Fica evidente com a pesquisa que a LGDP afeta todas as áreas de atuação dos profissionais da área contábil,ou seja, todos os procedimentos contábeis, desde atividades simples como recebimento de documentos até atividades complexas como consultoria, por exemplo. disse que a nova lei vai tornar o trabalho do contador mais sólido, de forma transparente e completa, seguindo as diretrizes da legislação, ou seja, a legislação vai aprimorar as práticas já implementadas pela profissão contábil.

Também foi sugerido que, no que se refere às boas práticas de gestão contábil, ajustes são urgentes, como identificar os responsáveis pelo

processamento de dados e especificar controladores e operadores em seus escritórios. Além disso, é necessário fazer as alterações necessárias no contrato de prestação de serviços para deixar claro para seus clientes como os dados serão tratados pelo seu escritório.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 10 out. de 2022.

BRASIL. **Lei nº 13.709, de 14 de Agosto de 2018**. Brasília, DF: Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm >. Acesso em: 10 out. de 2022.

BRASIL. [Constituição (2002)]. **Lei nº 10.406, de 10 de Janeiro de 2002**. Brasília, DF: Presidência da República, [2018]. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm >. Acesso em: 10 out. de 2022.

KRÜGER, Cristiane et al. Como Adequar os Escritórios de Contabilidade à Lei Geral de Proteção de Dados? Desenvolvimento de um Roteiro para Implantação e Avaliação. **Revista FSA**, v. 19, n. 9, 2022. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&profile=eh>. Acesso em: 10 out. de 2022.

DA CRUZ, Uniran Lemos; PASSAROTO, Matheus; JUNIOR, Nauro Thomaz. O impacto da lei geral de proteção de dados pessoais (lgpd) nos escritórios de contabilidade. **ConTexto**, v. 21, n. 49, p. 30-39, 2021. Disponível em: <https://www.seer.ufrgs.br/ConTexto/article/view/112561>. Acesso em: 10 out. de 2022.

CÂMARA, Flávia da Silva. **Lei Geral de Proteção de Dados Pessoais (LGPD)-aplicada às empresas de Contabilidade**. 2020. Trabalho de Conclusão de Curso. Universidade Federal do Rio Grande do Norte. 2020. Disponível em: <https://repositorio.ufrn.br/handle/123456789/41227>. Acesso em: 10 out. de 2022.

PEITER, Ester Escalante et al. **Lei Geral de Proteção de Dados: Roteiro para Implantação e Adequação em Escritórios de Contabilidade**. 2019. Disponível em: <https://congressousp.fipecafi.org/anais/22UspInternational/ArtigosDownload/3631.pdf>. Acesso em: 10 out. de 2022.

PIMENTEL, Almiro Felipe Santana. **Lei geral de proteção de dados: uma análise da percepção dos profissionais dos escritórios de contabilidade na cidade de Sapeaçu-BA.** 2022. Disponível em:

<http://131.0.244.66:8082/jspui/handle/123456789/2593>. Acesso em: 10 out. de 2022.

RIBEIRO, Jésun Gomes et al. Lei geral de proteção de dados: aplicação da lei geral de proteção de dados na contabilidade. **LIBERTAS: Revista de Ciênciais Sociais Aplicadas**, v. 12, n. 1, 2022. Disponível em: <https://www.periodicos.famig.edu.br/index.php/libertas/article/view/205>. Acesso em: 10 out. de 2022.

SANTOS, Cicera da Conceição Oliveira. **Os desafios na implantação da lei geral de proteção de dados nos escritórios de contabilidade de Cuiabá-MT.** 2021. https://www.google.com/url?sa=t&rct=j&q=&esr>. Acesso em: 10 out. de 2022.

RIGO, Caroline Pessini. **LGPD-Lei Geral de Proteção de Dados (Lei nº 13.709/18): análise das dificuldades encontradas na adequação do Departamento Pessoal dos escritórios de contabilidade perante a sua implantação.** 2021. Disponível em: <https://repositorio.ucs.br/xmlui/handle/11338/10662>. Acesso em: 10 out. de 2022.

DE CARVALHO, Hannibal Escobar RH; FREITAG, Alberto Eduardo Besser. Adequação das Organizações à LGPD: Aspectos a serem considerados para evitar a Vulnerabilidade Humana na exposição indevida de Dados Pessoais. In: **XI SICONF-Simpósio de Contabilidade e Finanças de Dourados**. 2021. Disponível em: <https://www.researchgate.net/profile/Alberto-Freitag/publication/357517884_>. Acesso em: 10 out. de 2022.

SCHERER FILHO, João Luiz. **Tratamento de dados em sistemas de informações contábeis a partir da lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais): um estudo multicaso.** 2020. Disponível em: <https://repositorio.ucs.br/xmlui/handle/11338/6598>. Acesso em: 10 out. de 2022.

MOREIRA, Augusto. **Automação dos processos contábeis.** 2022. Disponível em: <http://repositorio.ufu.br/bitstream/123456789/34347/1/Automa%C3%A7%C3%A3oDosProcessos.pdf>. Acesso em: 10 out. de 2022.

HASSE, Fernanda Gabrieli. **A Lei Geral de Proteção de Dados Pessoais (LGPD) Aplicada à Utilização do Arranjo Financeiro PIX.** 2021. Disponível em: <http://repositorio.upf.br/handle/riupf/2197>. Acesso em: 10 out. de 2022.

MOREIRA, Natanael de Jesus. **Lei geral de proteção de dados pessoais: a adaptação das empresas prestadoras de serviços contábeis da região sul catarinense.** 2020. Disponível em: <http://repositorio.unesc.net/handle/1/8936>. Acesso em: 10 out. de 2022.

COLARES, Ana Carolina Vasconcelos. **Contabilidade contemporânea aplicada**. AYA Editora, 2021.

COUTO, Karlla Soares et al. A Adequação de uma Associação Comercial à LGPD: Um Estudo de Caso. **Journal of Technology & Information (JTnI)**, v. 2, n. 3, 2022.

Disponível em: <http://www.jtni.com.br/index.php/JTnI/article/view/48>. Acesso em: 10 out. de 2022.

JÚNIOR, Reis; DE CARVALHO, Sebastião. **Tecnologia e a Lei geral de proteção de dados: estudo da implementação de um sistema ERP em uma clínica de saúde, visando o cumprimento da LGPD.** 2022. Disponível em: <http://repositorio.undb.edu.br/handle/areas/777>. Acesso em: 10 out. de 2022.

SILVA, Indira; JALES, José. **O impacto da nova LGPD (lei geral de proteção de dados) no âmbito empresarial.** 2022. Disponível em: <https://repositorio.animaeducacao.com.br/handle/ANIMA/25237>. Acesso em: 10 out. de 2022.