

CENTRO UNIVERSITARIO - UNINOVAFAPÍ
BACHARELADO EM DIREITO

HIWYS EULALIA RODRIGUES REIS

DESAFIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

TERESINA

2020

HIWYS EULALIA RODRIGUES REIS

DESAFIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Artigo de Conclusão de Curso
apresentado a banca examinadora do
Centro Universitário UNINOVAFAPI
como requisito parcial para obtenção do
grau de Bacharel em Direito.

Orientadora: Prof^a Dra. Cléa Mara
Coutinho Bento.

TERESINA

2020

FICHA CATALOGRÁFICA

R375d Reis, Hiwys Eulalia Rodrigues.

Desafios da lei geral de proteção de dados. Hiwys Eulalia Rodrigues Reis. – Teresina: Uninovafapi, 2020.

Orientador (a): Prof. Dr. Cléa Mara Coutinho Bento.
Centro Universitário UNINOVAFAPI, 2020.

21. p.; il. 23cm.

Monografia (Graduação em Direito) – Centro

Catálogo na publicação

Antonio Luis Fonseca Silva– CRB/1035

Francisco Renato Sampaio da Silva – CRB/1028

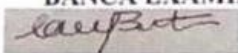
HIWYS EULALIA RODRIGUES REIS

DESAFIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

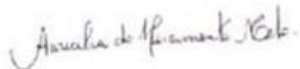
Artigo de Conclusão de Curso
apresentado à Banca Examinadora do
Centro Universitário UNINOVAFAPI,
como requisito parcial para obtenção do
grau de Bacharel em Direito

Data de Aprovação: 09 / 12 / 2020

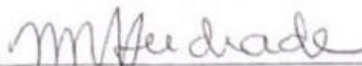
BANCA EXAMINADORA



Prof.ª Dra. Cléa Mara Coutinho Bento,
Centro Universitário - UNINOVAFAPI
(Orientador)



Prof.ª Dra. Auricelia do Nascimento Melo,
Centro Universitário - UNINOVAFAPI
(1º Examinador)



Prof.ª Dra. Marília Martins Soares Andrade
Centro Universitário - UNINOVAFAPI
(2º Examinador)

AGRADECIMENTOS

Agradeço, primeiramente à Deus, porque até aqui tua mão me guiou, me sustentou e mesmo em meio as lutas e desafios não permitiu que me faltasse força e coragem para alcançar esta vitória tão desejada.

A minha família, em especial meus pais, pois foram meus alicerces e meus irmãos, por toda paciência e compressão. Me sinto uma pessoa profundamente abençoada e honrada pela graça de ter uma família com quem posso sempre contar, minha gratidão será eterna.

Ao meu namorado, por todo apoio, incentivo e compreensão.

A todos os meus professores do curso de Bacharel em Direito da Universidade UNINOVAFAPI pela excelência da qualidade técnica de cada um.

A minha professora orientadora, Dra. Cléa Mara, por todo apoio, paciência e ensinamentos ao longo da elaboração do meu artigo. Obrigada, Professora!

Aos meus amigos, Isadora, Leticia, Mariana e Valter, com quem convivi intensamente durante os últimos anos, pelo companheirismo e pela troca de experiências que me permitiram crescer não só como pessoa, mas também como formando.

Por fim, quero agradecer a todos aqueles que de alguma forma, direta ou indiretamente, colaboraram para que esse sonho se tornasse realidade.

RESUMO

A era das redes sociais e inteligência artificial e os crescentes casos de violação de privacidade, bem como a exponenciação de vítimas, deixaram evidente que o conjunto normativo nacional até então vigente não era suficiente para a proteção da privacidade dos dados pessoais. Foi nesse contexto que surgiu a LGPD, buscando garantir o domínio e a regular a coleta desses dados pelas empresas e pelo governo. A pesquisa objetivou a verificação a LGPD e os benefícios, em potencial, para a sociedade em geral, no que se referem a proteção de dados pessoais. A LGPD faz diferenciação entre o dado pessoal e o dado pessoal sensível, apontando que esses que necessitam de maior proteção, haja vista serem determinantes para a identificação do indivíduo e possuem uma maior possibilidade de ofensa aos direitos fundamentais. Do estudo, constatou-se que LGPD se mostrou inovadora no que se refere ao sistema protetivo da privacidade de dados pessoais, destacando-se a criação da autoridade nacional de dados pessoais (ANPD), um protocolo de boas práticas como medida de prevenção e o sistema repressivo, baseado na responsabilidade administrativa. Destacou-se a efetividade do sistema de repressão administrativa independente da responsabilização judicial no âmbito cível e penal. A LGPD representa um significativo avanço normativo na proteção da privacidade dos dados pessoais forçando grandes mudanças comportamentais nas empresas, na forma de lidar com os dados *online* e *offline* de seus usuários e consumidores. Concluiu-se que os mecanismos institucionais, preventivos e repressivos de proteção de dados pessoais utilizados permitem afirmar que a lei tem potencial para ser efetiva.

Palavras-chave: Lei Geral de proteção de dados. Sistemas protetivos e repressivos. Efetividade.

ABSTRACT

The era of social networks and artificial intelligence added to the growing cases of breach of privacy, as well as the escalation of number of victims, made it evident that the current national set of rules was not sufficient to protect the privacy of personal data. It was in this context that the General Law of Data Protection (in Portuguese, LGPD) emerged, seeking to guarantee dominance and regulate the data collection by both companies and the government. The research aimed to verify the LGPD and the potential benefits for society in general, regarding the protection of personal data. The LGPD differentiates what is considered personal data and sensitive personal data, pointing out that the latter needs greater protection, since they are determinants for the identification of the individual and have a greater possibility of offending fundamental rights. From the study, it was found that LGPD proved to be innovative in what concerns the personal data privacy protection system, highlighting the creation of the national personal data authority (in Portuguese, ANPD), a protocol of good practices as a preventive measure and the repressive system, based on administrative responsibility. The effectiveness of the system of administrative repression regardless judicial liability in the civil and criminal spheres was highlighted. The LGPD represents a significant normative advance in protecting the privacy of personal data by forcing major behavioral changes in companies, in the way of dealing with the online and offline data of their users and consumers. It was concluded that the institutional, preventive, and repressive mechanisms for the protection of personal data used allow us to say that the law has the potential to be effective.

Keywords: General Law of data protection. Protective and repressive systems. Effectiveness.

1 INTRODUÇÃO

Na era das redes sociais e inteligência artificial, a privacidade de dados pessoais ganha a tônica de desafio, sobretudo quanto à efetiva proteção jurídica. Isso porque os casos de violação de privacidade são cada vez mais comuns e atingem números gigantescos de vítimas.

Os crescentes casos de violação de privacidade e exponenciação de vítimas deixaram evidente que o conjunto normativo nacional até então vigente, como o Código de Defesa do Consumidor, o Marco Civil da Internet (Lei 12.965/2014), a Lei de Acesso à Informação (Lei 12.527/2011), a Lei do Cadastro Positivo (Lei 12.414/2011), dentre outras normativas, mostraram-se insuficientes para a efetiva proteção da privacidade dos dados pessoais.

Assim, os escândalos recorrentes levaram o Brasil a buscar apoio de outras nações na intenção de construção de uma política de proteção de dados pessoais mais eficiente.

É nesse contexto que surge a Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD) para garantir o domínio sobre dados pessoais e regular a coleta de dados de organizações, empresas e pelo governo. O motivo que inspirou o surgimento da regulamentação de proteção dos dados pessoais está diretamente relacionado ao próprio desenvolvimento do modelo de negócio da economia, que passou a ter uma dependência muito maior dos fluxos de dados, especialmente, os relacionados a pessoas, viabilizados pelos avanços tecnológicos e a globalização.

Diante dessas considerações, o objeto do presente estudo é analisar a LGPD e como as empresas estão se portando diante da nova lei, que entrou em vigor em agosto de 2020. O trabalho visa responder o seguinte questionamento: Os mecanismos de proteção de dados pessoais criados pela LGPD estão hábeis para alcançar os objetivos propostos?

Desta feita, o objetivo geral da pesquisa é verificar a efetividade da LGPD dentro das empresas que utilizam dados pessoais de clientes, tanto no meio virtual quanto físico, como também demonstrar seus benefícios para a sociedade em geral. E os objetivos específicos são: descrever as medidas preventivas de proteção de dados, que constituem boas práticas de governança; discutir a LGPD com as mudanças das tecnologias da informação; caracterizar as medidas repressivas, oriundas da responsabilização civil e administrativa decorrente da violação da LGPD.

Esta pesquisa tem como justificativa o conhecimento e a contribuição de informações que devem ser amplamente divulgadas, expondo como as empresas devem se portar, assim como as pessoas podem exigir a proteção de seus dados pessoais. Ressalta-se que é de relevante

importância tanto para as empresas como para o cidadão em si, o conhecimento e o uso da proteção de dados pessoais.

O artigo utilizará como metodologia a pesquisa bibliográfica narrativa e documental, que será apresentada e organizada em 3 tópicos que abordarão: (1) Considerações Gerais da LGPD e a efetividade de seus mecanismos institucionais; (2) A efetividade da segurança e as medidas preventivas de proteção de dados, que constituem boas práticas de governança e compliance na tecnologia da informação; (3) Medidas repressivas, oriundas da responsabilização civil e administrativa decorrente da violação da LGPD. Ao final, os principais resultados do problema investigado serão apontados nas considerações finais.

2 ASPECTOS GERAIS DA LEI DE PROTEÇÃO DE DADOS (LGPD)

A LGPD surge como novo paradigma da segurança de dados frente a necessidade de resgate do compromisso das instituições com as pessoas, no tocante à proteção e a garantia dos direitos humanos fundamentais de liberdade e de privacidade, previstos na Constituição de 1988, no artigo 5º, inciso X, resultado de um movimento espontâneo da sociedade e autoridades brasileiras.

O art. 2º da LGPD apresenta um rol de fundamentos, incluindo:

I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2020).

Essas diretivas consistem numa base geral para a interpretação de todos os dispositivos da lei e resguarda relação com os direitos fundamentais da Constituição Federal.

A nova lei impõe uma profunda transformação no sistema de proteção de dados brasileiro, forçando grandes mudanças na maneira como as empresas lidam com os dados *online* e *offline* de seus usuários. É uma lei que estabelece regras detalhadas para coletas, uso, tratamento e armazenamento de dados pessoais. Essa medida afetará todos os setores da economia, inclusive a relação entre clientes e fornecedores de produtos e serviços, empregado e empregador, relações comerciais internacionais e nacionais, além de outras relações nas quais dados pessoais sejam coletados, tanto no ambiente digital quanto fora dele.

As novas regras jurídicas estabelecidas pela LGPD serão aplicadas, na forma do art. 3º, inc. I, II, III. Litteris:

A qualquer operação de tratamento realizada por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional (BRASIL, 2020).

É considerado dado pessoal “*a informação relacionada a pessoa natural identificada ou identificável*” (art. 5º, inc. I). A lei faz diferenciação entre o dado pessoal e o dado pessoal sensível e de acordo com a LGPD, o dado pessoal sensível, é 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. O titular do dado pessoal, segundo o art. 5º, inc. V, é “*qualquer pessoa natural a quem se referem os dados pessoais que são objeto de tratamento*” (BRASIL, 2018).

Os dados sensíveis são aqueles que necessitam de maior proteção, haja vista estes serem determinantes para a identificação do indivíduo e possuírem uma maior possibilidade de ofensa aos direitos fundamentais.

O tratamento de dado pessoal é classificado de acordo com o art. 4º que:

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).

Considerando-se estratégico em seu compromisso de oferecer atividades de qualidade às organizações que precisam cada dia mais da tecnologia da informação, é fundamental assegurar a proteção ajustada deste ativo. O meio mais adequado é a implantação de um conjunto de normas e diretrizes que estabeleçam a aplicação dos sistemas das organizações.

De acordo com o art. 6º da LGPD as atividades de tratamento de dados pessoais devem observar boa-fé nos princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e contribuição (BRASIL, 2018).

Com efeito, todas as organizações brasileiras, seja de qual porte for (pequeno, médio e grande), deverão fazer investimento em segurança tecnológica e executar técnicas de *compliance* existentes para impedir, detectar e corrigir violações de dados pessoais, principalmente porque a lei presume que a preferência de política de boas práticas será considerada como método favorável das penas.

Um dos principais debates a respeito da LGPD é sobre seus mecanismos de proteção de dados pessoais e se eles terão a efetividade necessária para garantir o cumprimento dos seus objetivos. O objetivo da LGPD é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2.1 A efetividade e os mecanismos institucionais da LGPD

A LGPD possui dois mecanismos formais de proteção de dados pessoais. O primeiro mecanismo é a instituição de agentes de proteção de dados pessoais, nas figuras do controlador, que é a quem compete as decisões relativas ao tratamento; e do operador, que é quem realiza o tratamento, em nome do controlador, além da figura do encarregado pelo tratamento de dados pessoais, que com autonomia e estabilidade, é o responsável por atender as demandas dos titulares. O segundo mecanismo é a criação de uma Autoridade Nacional de Proteção de Dados (ANPD), que é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo território nacional, por meio do exercício de competências normativas, deliberativas, fiscalizadoras e sancionatórias.

2.2 Quem são os agentes e o encarregado pelo tratamento de dados pessoais

A LGPD define dois tipos de agentes de tratamento de dados pessoais: o controlador e o operador. Além disso, a lei define uma terceira pessoa, que fará o papel de encarregado pelo tratamento de dados pessoais:

Art. 5º Para os fins desta Lei, considera-se:

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;

IX - agentes de tratamento: o controlador e o operador (BRASIL, 2018)

O controlador e o operador são obrigados a manter o registro das operações de tratamento de dados que realizarem, especialmente quando envolver o legítimo interesse. A lei estabelece

a hierarquia funcional entre o operador e o controlador, onde o operador deve realizar o tratamento de dados segundo instruções fornecidas pelo controlador, que verificará a observância das instruções e suas próprias normas sobre o tratamento de dados.

O controlador tem competência para elaborar o relatório de impacto à proteção de dados pessoais, inclusive dados pessoais sensíveis, referente a suas operações de tratamento de dados, que poderão ser exigidos pela autoridade nacional, desde que seja observado os segredos comercial e industrial. A LGPD antevê requisitos mínimos para a elaboração do relatório, como: a metodologia utilizada para coleta; a descrição dos tipos de dados coletados; a metodologia utilizada para garantir a segurança das informações; e a análise do controlador com relação aos mecanismos de mitigação de risco adotados.

Ao comentar a lei, Pinheiro (2019) afirma que o controlador é o possuidor do consentimento do titular e, por essa razão, é o responsável pelo ciclo de vida dos dados pessoais. Da mesma forma, é ele o responsável não só pelo registro das operações de tratamento de dados pessoais, mas também pela revisão e atualização dos procedimentos adotados para que, então, a proteção dos dados pessoais seja efetiva.

As autoridades nacionais poderão utilizar de normas complementares, ou seja, a GDPR pode ser utilizada como complementação à visão de necessidade de atualização e revisão dos dados pessoais.

A LGPD também prevê a figura do encarregado pelo tratamento de dados pessoais. O encarregado é indicado pelo controlador e tem como principais atividades: aceitar reclamações e comunicações dos titulares; prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais, além de executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares (BRASIL, 2018).

Em suma, a figura do encarregado assegura que as informações fiquem centralizadas, certificando o controlador de que a aplicação das normas receberá a efetiva validação.

Os agentes e o encarregado pelo tratamento de dados pessoais são as figuras essenciais para o controle interno das empresas, pois têm a função de zelar pela proteção de dados pessoais durante o exercício da atividade empresarial, assegurando aos usuários de que seus dados estarão resguardados.

A efetividade dos agentes e do encarregado não dependerá só do desempenho no ambiente interno da empresa, mas também da consonância com uma autoridade nacional, que terá o papel de zelar pela proteção de dados pessoais no ambiente externo das organizações a que pertencem.

2.3 A Autoridade Nacional de Proteção de Dados Pessoais

Para fiscalizar e regulamentar a LGPD, criou-se a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), o órgão integrante da administração pública federal que integra a estrutura da Presidência da República, que foi alterada pela Medida Provisória nº 869, de 2018, com autonomia técnica e decisória assegurada por lei.

A ANPD é composta por pelo Conselho Diretor (órgão máximo de direção), Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e possui unidades administrativas e especializadas na aplicação nos dispositivos da Lei 13.709/2018.

Segundo o Art. 55-D, §§1º, 2º e 3º, o órgão máximo da ANPD é composto por cinco diretores nomeados pelo Presidente da República, escolhidos dentre brasileiros de reputação ilibada, com nível superior de educação e que tenha um elevado conceito no campo em que atuarão, para cumprimento de um mandato de quatro anos (BRASIL, 2018).

Os membros do Conselho Diretor da ANPD só perderão o cargo em razão de renúncia, condenação judicial transitada em julgado ou demissão decorrente de processo administrativo disciplinar, da qual a competência de instauração é do Ministro de Estado Chefe da Casa Civil e de julgamento é do Presidente da República, que poderá inclusive afastar preventivamente o conselheiro durante o processo caso seja recomendado pela comissão especial. Os membros do Conselho Diretor, após o exercício do cargo, submetem-se a disciplina de conflito de interesse, disposto no art. 6º da Lei nº 12.813, de 16 de maio de 2013.

A ANPD tem como competência principal “zelar pela proteção dos dados pessoais”, e para isso, suas competências mais relevantes dentre as XXIV são:

Art. 55-J. Compete à ANPD:

- I - Zelar pela proteção dos dados pessoais, nos termos da legislação;
- II - Zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
- III - Elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;

- IV - Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- V - Apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
- VI - Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
- VII - Promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade (BRASIL,2018).

A criação de uma autoridade nacional provém da convergência do legislador brasileiro ao modelo teórico da regulação de risco. A “regulação do risco”, que foi inicialmente construída para lidar com problemas de ameaças à saúde com relação a novos medicamentos, alimentos industrializados e poluição ambiental (HUBER, 1983), coloca o risco como elemento central – a incerteza quantificável ou a probabilidade de que um ato malefício ocorra - visando proteger direitos e liberdades coletivas.

Segundo Zanatta (2017, p.181), o modelo de regulação de risco na LGPD privilegia a reunião de informações sobre os riscos regulados, a criação de padrões de conduta e, principalmente, a aplicação e o monitoramento das mudanças de comportamento social. A LGPD deposita a aplicação do seu modelo regulatório na capacidade institucional de uma agência reguladora, para que possa alcançar a efetividade desejada.

A criação de uma autoridade com características de uma agência reguladora para interpretar a LGPD é de suma importância, conforme a visão de **Lemos (2018)**, que ressalta que "Assim como o petróleo, dados quando vazam também provocam danos ambientais significativos. Por isso a importância da proteção de dados".

Ao comparar a capacidade institucional de cortes e agências na interpretação de conflitos regulatórios, as agências reguladoras possuem um nível superior de competências técnicas e, portanto, estão melhor posicionadas para decidir qual é o melhor sentido do texto normativo. Além do que, a proximidade das agências com a atividade regulada permite melhor compreensão sobre quais fatos representam ameaças verídicas ao cumprimento da lei.

A advogada Pinheiro (2019), ao analisar o artigo 40 da LGPD, afirma que o poder de fiscalização da ANPD é expressivo, pois o emprego de padrões de ação por esses órgãos simplifica a execução das normas. Por consequência, como a regulação dos dados pessoais será efetuada por uma agência nacional, a aplicação das sanções deve seguir os mesmos nortes e princípios do direito administrativo.

Contudo, a efetividade do modelo de regulação de risco pode ser ameaçada no Brasil pela judicialização de medidas regulatórias e administrativas, com a imposição de barreiras procedimentais estratégicas por interesses econômicos específicos. Existe ainda uma grande possibilidade de isolamento do cidadão comum do debate a respeito da proteção de dados pessoais, de uma forma que as negociações coletivas sejam protagonizadas apenas por grandes empresas de tecnologia e entidades civis altamente especializadas, como a autoridade reguladora.

Por consequência, a efetividade dos mecanismos institucionais de proteção de dados pessoais está diretamente ligada à capacidade dos agentes e dos encarregados, no ambiente interno da organização que pertence, e da ANPD, no ambiente externo, de fazer com que a atividade empresarial se conforme com a LGPD, por meio da implementação de mecanismos preventivos de proteção de dados pessoais, como a adoção de medidas de segurança e a formulação de regras de boas práticas e governança.

3 A EFETIVIDADE DA SEGURANÇA E AS MEDIDAS PREVENTIVAS DE PROTEÇÃO DE DADOS, QUE CONSTITUEM BOAS PRÁTICAS DE GOVERNANÇA E COMPLIANCE NA TECNOLOGIA DA INFORMAÇÃO.

A LGPD adotou dois mecanismos preventivos de proteção de dados pessoais. O primeiro mecanismo é a adoção de medidas de segurança, técnicas e administrativas aptas a proteger e evitar situações acidentais ou ilícitas de qualquer natureza, como destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. O segundo mecanismo é a formulação de regras de boas práticas e de governança corporativa que estabeleçam a organização, os procedimentos - incluindo reclamações e petições de titulares - algumas normas de segurança, obrigações específicas para os diversos envolvidos no tratamento, os padrões técnicos, os mecanismos internos de supervisão, a mitigação de riscos e as obrigações no tratamento de dados pessoais (BRASIL, 2018)

Segundo Pinheiro (2019), a LGPD almeja estimular que seus dispositivos sejam aplicados em caráter preventivo, ou melhor, exige uma adequação dos processos de governança corporativa, com a instalação de um programa mais consistente de *compliance* digital. Tal programa passa a exigir algumas mudanças, como investimentos, atualizações de ferramentas de segurança, melhorias nos fluxos internos e externos de dados pessoais, revisões documentais e, acima de tudo, a evolução cultural, considerada a principal dessas mudanças.

3.1 A aplicação de medidas de segurança.

A segurança baseada em risco, sugere estabelecer prioridades e tomar decisões, avaliando a sensibilidade dos dados, a vulnerabilidade do sistema e a probabilidade de ameaças. É uma abordagem holística, construindo uma compreensão do risco em todas as decisões relacionadas à segurança. Essa abordagem de segurança baseada em risco deve ser usada para identificar objetivamente quais os controles de segurança que serão aplicados, determinando onde e quando devem ser aplicados.

A LGPD determina que seus agentes devem adotar medidas de segurança de caráter técnico e administrativo, aptas a resguardar os dados pessoais de acesso restrito ou de situações acidentais ou ainda de situações ilícitas de destruição, perda ou qualquer forma de tratamento inadequado ou ilícito, como demonstra o art. 46:

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018).

A lei determina que os agentes de tratamento devem adotar medidas de segurança e que à ANPD devem utilizar-se de regulamentação específica a respeito dos padrões de segurança a qual se refere. Em se tratando de padrões de segurança da informação, é indispensável observar as normas editadas pela Organização Internacional de Padronização (International Standardization Organization - ISO). Normas as quais são recomendadas pela Agência Brasileira de Normas Técnicas (ABNT).

Além do mais, a LGPD determina que o controlador, em casos eventuais de incidentes de segurança que possam acarretar risco ou dano relevante para os titulares dos dados pessoais, comunique as informações da ocorrência à autoridade nacional e ao titular em prazo razoável. Posteriormente, a autoridade nacional deverá averiguar a gravidade do incidente e, caso seja necessário, o controlador tem por determinação adotar medidas de providências, dentre elas a

ampla divulgação do fato e medidas para reverter ou mitigar os efeitos do incidente. O profissional terá ainda que avaliar se foram tomadas as medidas técnicas adequadas.

Ao contrário da Regulamento Geral sobre Proteção de Dados (GDPR), um rigoroso conjunto de regras sobre privacidade válido para a União Europeia, que em seu artigo 33 determina que a notificação do ocorrido deve ser em até 72 horas após ter conhecimento do ocorrido, o legislador brasileiro preferiu que a comunicação seja feita em prazo razoável.

Perante o exposto, as medidas de segurança de natureza técnica e administrativa para proteção de dados pessoais só serão efetivas se estiverem em consonância com a formulação de regras de boas práticas e de governança.

3.2 As medidas preventivas de proteção de dados que formulam as boas práticas de governança e *compliance* na tecnologia da informação.

No âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, os controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos (incluindo reclamações), 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.

A lei não especifica quais são as medidas preventivas. No entanto, destaca-se que podem existir padrões técnicos mínimos estabelecidos pela autoridade nacional. A ANPD considera os princípios previstos na lei e “a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis”.

O legislador deixou de forma facultativa aos controladores e operadores de tratamentos de dados pessoais a formulação de regras de boas práticas e de governança. Como determinado em seu art. 50:

Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança 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 (BRASIL, 2018).

A LGPD, ao estabelecer regras de boas práticas, utiliza-se de alguns parâmetros para consideração do controlador e do operador, como a natureza, o escopo, a finalidade e a probabilidade e gravidade dos riscos e benefícios decorrentes do tratamento de dados do titular.

O legislador indica a implementação de um programa de governança em privacidade, com base nos princípios da segurança e da prevenção. Deve-se levar também em consideração a estrutura, escala e volume das operações, bem como a sensibilidade dos dados e a probabilidade e gravidade dos danos para os titulares dos dados. Ademais, necessita-se cumprir com os requisitos mínimos exigidos em seu art. 50, § 2º, I:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas (BRASIL, 2018).

A LGPD, determina ainda que seja demonstrada a efetividade do programa de governança em privacidade quando apropriado, especialmente a pedido da ANPD ou outra entidade que, de qualquer forma, promova o seu cumprimento.

Segundo Pinheiro (2018), é essencial a introdução de medidas e regras de boas práticas e de governança para que todos os requisitos necessários à proteção dos dados pessoais sejam efetivados. A autora observa que a lei prevê e exige que existam encarregados da proteção dos dados pessoais nas organizações, e que o controlador e o operador devem pensar em regras e meios técnicos para proteger os dados pessoais e comprovar sua efetividade nas empresas.

Nesse contexto, as empresas devem adaptar suas políticas de segurança da informação, bem como seus regulamentos internos de segurança informacionais e seus termos de uso da segurança da informação.

As medidas de proteção à privacidade devem ser incorporadas às soluções tecnológicas oferecidas pelas empresas desde a etapa inicial de seu planejamento. Isso se dá porque a LGPD impõe a adequação da atividade empresarial ao conceito de privacidade. Dessa forma, a legislação deixa claro que as empresas são responsáveis, por capacitar permanentemente todos os seus colaboradores que participam do desenvolvimento de tecnologias nas políticas de segurança da informação.

As empresas certamente estão com sofrendo dificuldades de adaptação à LGPD, em razão do elevado número de alterações que passaram a enfrentar em seu novo cotidiano da atividade empresarial. Todavia, existem diversos escritórios de advocacia que estão à disposição para auxiliar na aplicação da nova lei, de modo que as boas práticas e a governança sejam efetivadas.

Verifica-se que, a efetividade dos mecanismos preventivos de proteção de dados pessoais, seja pela formulação de regras de boas práticas e de governança, seja pela adoção de medidas de segurança, só terá aplicação concreta se for interpretada em conjunto com as regras de responsabilização administrativa e civil através de mecanismos repressivos de proteção de dados pessoais.

4 MEDIDAS REPRESSIVAS, ORIUNDAS DA RESPONSABILIZAÇÃO CIVIL E ADMINISTRATIVA DECORRENTE DA VIOLAÇÃO DA LGPD.

A LGPD possui dois mecanismos repressivos de proteção de dados pessoais. O primeiro mecanismo é a responsabilização administrativa por meio de sanções aplicáveis pela autoridade nacional (ANPD), que terá competências normativas, deliberativas, fiscalizadoras e sancionatórias, como advertência, multa, publicação da infração, bloqueio e eliminação de dados pessoais. O segundo mecanismo é a responsabilização civil e o ressarcimento de danos por meio do acionamento dos mecanismos tradicionais de jurisdição do Poder Judiciário.

4.1 A responsabilidade administrativa por meio de sanções.

A LGPD prevê a responsabilização administrativa dos agentes de tratamento de dados em razão das infrações cometidas em prejuízo das disposições normativas que institui, por meio da aplicação das sanções e penalidades pela ANPD deverão levar em consideração os parâmetros fixados em lei e vão de advertência até multas com limite de R\$ 50.000.000,00 (cinquenta milhões de reais). Nota-se que as Empresas deverão tratar com seriedade a

conformidade com a LGPD, sempre atentando aos seus princípios norteadores, perante o risco de sofrerem graves punições. Por fim, é necessário ressaltar que para um funcionamento eficiente e coeso da ANPD, é indispensável a composição da equipe de maneira multidisciplinar, com conhecimento técnico, jurídico e social da proteção de dados pessoais (BRASIL, 2018).

Na aplicação da multa, ANPD deverá considerar o faturamento total da empresa ou do grupo de empresas, desde que não disponha do valor do faturamento no ramo da atividade empresarial na qual tenha ocorrido a infração, ou ainda quando o valor for apresentado de forma equivocada. Determina ainda a emissão de regulamento próprio sobre as metodologias de cálculo do valor-base das sanções de multa previstas na LGPD após a realização de consulta pública. No caso do cálculo do valor de multas diárias, deverá ainda observar parâmetros como a gravidade da falta e a extensão do dano ou prejuízo causado a ser fundamentada pela autoridade nacional (BRASIL, 2018).

Para implicar em maior efetividade da norma, as penalidades por multa levam em consideração valores elevados, que influenciam na ação do controlador ou operador, pois mesmo que estejam aplicando todos os controles determinados por lei, ainda assim poderá haver a infração e o incidente de vazamento de dados pessoais.

Para o cálculo do valor-base na aplicação das sanções de multa, deve-se considerar o caso específico e o princípio constitucional da proporcionalidade. Ademais, deve haver um controle nas aplicações das punições, visando que elas possuam um caráter geral no setor da economia e possam atingir tanto pequenas empresas quanto empresas que assumem maiores riscos, segundo Pinheiro (2018).

Portanto, a efetividade da responsabilidade administrativa por meio de sanções para proteção de dados pessoais deve pautar-se na não exclusão da responsabilização civil e no ressarcimento de danos pelo Poder Judiciário.

4.2 A responsabilidade civil e do Ressarcimento de Danos da LGPD

A responsabilidade civil está regulamentada na Seção III do Capítulo VI da LGPD, intitulada “Da Responsabilidade e do Ressarcimento de Danos”. Essa regulamentação prevê a possibilidade genérica de ajuizamento de ação perante o Poder Judiciário para defesa dos interesses e dos direitos dos titulares de dados, que poderá ser exercida em juízo, individual ou

coletivamente na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva (BRASIL,2018).

A responsabilidade aparece no exercício da atividade de proteção de dados que viole a “legislação de proteção de dados”. Em decorrência dessa expressão, o legislador reconhece que a proteção de dados é um microssistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural. A ocorrência de eventuais falhas relacionadas ao tratamento de dados pessoais pode gerar danos que, por sua vez, geram o dever de reparação civil.

No Código Civil, a previsão da responsabilização civil de pessoas físicas e jurídicas por eventuais atos ilícitos consta nos arts. 186, 187 e 927:

Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.

Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Art. 927: Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, é obrigado a repará-lo.

Parágrafo único. 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 (BRASIL, 2020, p.1).

A lei impõe ao controlador e ao operador, especificamente, a obrigação de reparação de danos decorrentes da violação à legislação de proteção de dados pessoais, em seu artigo 42 em conjunto com o art. 44, parágrafo único, que assim dispõe:

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.

Art. 44, parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano (BRASIL, 2018).

O art. 46, por sua vez, estabelece que os agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas, visando a proteção de dados pessoais. Tais normas podem ser editadas, inclusive, pela ANPD.

Dessa forma, é possível identificar duas situações de responsabilidade civil na LGPD, seriam elas: a violação de normas jurídicas, do microssistema de proteção de dados e a violação de normas técnicas, voltadas à segurança e proteção de dados pessoais. E, evidentemente, só

caracterizará a responsabilidade civil, se a violação de norma jurídica ou técnica ocasionar dano material ou moral a um titular ou a uma coletividade.

Com o propósito de assegurar a efetiva indenização aos titulares de dados, a legislação prevê a responsabilização solidária do operador e controlador ou de controladores que estiverem envolvidos no tratamento gerador do dano. Tais hipóteses de solidariedade estarão afastadas caso presentes as hipóteses de exclusão de responsabilidade, previstas no art. 43, como demonstrado abaixo:

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

- I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
- II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
- III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (BRASIL, 2018).

Além do mais, a LGPD prevê a possibilidade de o magistrado promover a inversão do ônus da prova a favor do titular dos dados quando houver verossimilhança das alegações, hipossuficiência para fins de produção da prova ou for excessivamente onerosa a sua produção. Ainda, a lei permite expressamente o ajuizamento de ação de reparação de danos coletivos.

Verifica-se também o fato de a responsabilidade civil da LGPD ser da modalidade objetiva, onde não há discussão sobre a culpa do agente.

De acordo com Sá Junior (2019, p. 29), a responsabilização civil das empresas, nesse caso, se dá com fundamento no Código de Defesa do Consumidor (CDC). A relação consumerista pode ser evidenciada na medida em que o titular dos dados é considerado consumidor direto ou indireto e a empresa é considerada fornecedora de produtos ou serviços.

Nenhum tipo de segurança será absolutamente capaz de cobrir todos os riscos das atividades. Todavia, com base nos preceitos do CDC, o Poder Judiciário considerará a teoria do risco da atividade para concluir pela responsabilidade objetiva do fornecedor.

A irregularidade do tratamento de dados será constatada pelo magistrado quando deixar de observar a legislação ou não fornecer a segurança esperada pelo titular do dado. Serão consideradas algumas circunstâncias, como os resultados e riscos razoavelmente esperados, o modo pelo qual é realizado e as técnicas de tratamento de dados pessoais disponíveis à época da realização. Dessa forma, o Poder Judiciário será acionado para efetivar as reparações civis previstas na LGPD e para eventuais casos de judicialização de medidas administrativas da ANPD (BRASIL, 2020).

5 CONSIDERAÇÕES FINAIS

Ao desenvolver a pesquisa foi possível observar que os mecanismos institucionais, preventivos e repressivos de proteção de dados pessoais utilizados permitem afirmar que a lei tem potencial para ser efetiva. Para tanto, cada mecanismo utilizado deverá cumprir o seu papel.

A LGPD faz diferenciação entre o dado pessoal e o dado pessoal sensível e, de acordo com a lei, os dados sensíveis são aqueles que necessitam de maior proteção, haja vista serem determinantes para a identificação do indivíduo e possuírem uma maior possibilidade de ofensa aos direitos fundamentais.

Outro ponto de destaque é a ANPD que agirá no âmbito externo da organização, juntamente com os agentes e os encarregados pelos dados pessoais no âmbito interno da organização a que pertence, assegurando que os mecanismos preventivos - as medidas de segurança e as regras de boas práticas - sejam regulamentados, compreendidos e devidamente aplicados.

Serão instalados processos administrativos pela ANPD na hipótese de descumprimento da lei por parte das empresas e/ou de seus colaboradores, que apurará os riscos, danos e a conduta dos envolvidos no incidente. Caso seja detectado que houve infração à LGPD, deverá aplicar-se uma das sanções administrativas, independentemente da responsabilização civil e até penal, pelo âmbito do Poder Judiciário.

Portanto, é indiscutível que as organizações devem buscar sua conformidade da melhor forma possível e o quanto antes, visto que seu nível de adequação à LGPD pode pautar o sucesso na proteção de dados, evitando sanções administrativas.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO/IEC 27000: norma internacional de segurança da informação é revisada. 2018. Disponível em: Acesso em: 21 setembro. 2020.

AVAST. Os últimos 10 maiores vazamentos de dados. 2019. Disponível em: Acesso em: 21 set. 2020.

BORINI, Guilherme. LGPD: especialistas cobram criação de agência reguladora. São Paulo, 2018. Disponível em: <https://computerworld.com.br/negocios/lgpd-especialistas-cobram-criacao-de-agencia-reguladora/>. Acessado em: 12 out. 2020.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: Acesso em: 18 set. 2020.

BRASIL. Lei nº 10.406, de 10 de Janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: Acesso em: 18 set. 2020.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados, Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020.

CASTRO, Rodrigo. Eficácia, eficiência e efetividade na Administração Pública. ENANPAD. Salvador, 2006. Disponível em:
<http://www.anpad.org.br/diversos/download/10/enanpad2006-apsa-1840.pdf>. Acesso em: 18 set. 2020.

<https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf>. Acesso em: 22 out. 2020.

HUBER, P. The Old-New Division in Risk Regulation. Virginia Law Review , 69 (6), 1025-1107, 1983.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: Comentários à Lei 123.709/20019(LGPD). São Paulo: Saraiva Educação, 2018.

SÁ JUNIOR, Sergio Ricardo C. A regulação jurídica da proteção de dados pessoais no brasil. 2019. Monografia de especialização – Pontífica Universidade Católica do Rio de Janeiro, Rio de Janeiro. p. 29.

TUPINAMBÁ, Regina. Lei Geral de Proteção de Dados: Brasscom divulga FAQ sobre a LGPD – PLC 53/2018. São Paulo, 2018. Disponível em: <https://cryptoid.com.br/banco-de-noticias/35672-lei-geral-de-protecao-de-dados-brasscom/>. Acesso em: 12 out. 2020.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? I Encontro da Rede de Pesquisa em Governança da Internet. Rio de Janeiro, 2017.

DECLARAÇÃO

Declaramos para os devidos fins, que o projeto de pesquisa intitulado: "**Desafios da Lei Geral de Proteção de Dados**", da discente **Hiwys Eulalia Rodrigues Reis**, orientada pela **Profa. Cléa Mara Coutinho Bento**, foi cadastrado na Coordenação de Pesquisa, Extensão e Pós-Graduação, **sob o processo nº 153/2020**.

Teresina, 30 de novembro de 2020



Profa. Dra. Adélia Dalva da Silva Oliveira
Coordenadora de Pesquisa, Extensão e Pós-Graduação do Centro
Universitário UNINOVAFAPI

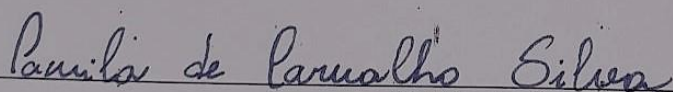


ANEXO: DECLARAÇÃO DE CORREÇÃO GRAMATICAL

DECLARAÇÃO DE CORREÇÃO ORTOGRÁFICA

Declaro para os devidos fins que eu, CAMILA DE CARVALHO SILVA, de CPF 061.365.493-52, realizei a correção gramatical do Artigo de Conclusão de Curso intitulada: DESAFIOS DA LEI GERAL DE PROTEÇÃO DE DADOS, realizado pela acadêmica HIWYS EULÁLIA RODRIGUES REIS, tendo como orientadora a Profa. Dra. Cléa Mara Coutinho Bento. O trabalho será apresentado ao Centro Universitário UNINOVAFAPI, para a conclusão do curso de Bacharelado em Direito.

Teresina, 05 de dezembro de 2020 .



Camila de Carvalho Silva

Graduada em Letras

CPF: 061.365.493-52