HELOIZA MACÊDO RODRIGUES

(IN)EFETIVIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL: Responsabilidade Civil

CURSO DE DIREITO – UniEVANGÉLICA

2022

HELOIZA MACÊDO RODRIGUES

(IN)EFETIVIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL: Responsabilidade Civil

Monografia apresentada ao Núcleo de Trabalho de Curso da UniEVANGÉLICA, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação da Profª. M.e Karla de Souza Oliveira

ANÁPOLIS - 2022

HELOIZA MACÊDO RODRIGUES

(IN)EFETIVIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL: Responsabilidade Civil

Anápolis, ____ de _____ de 2022.

Banca Examinadora

_____

_____

AGRADECIMENTOS

Primeiramente, agradeço aos meus pais todo o apoio, amor e todo o esforço para que esse momento se tornasse possível, principalmente naqueles momentos onde mais precisei de sustento emocional. Obrigada por acreditarem que estou trilhando o caminho certo e me amparar nessa caminhada. A minha orientadora, Prof. Karla de Souza Oliveira, que me guiou nesta pesquisa, além de toda a compreensão e assistência. A Raissa Camargo, uma amiga que me auxiliou diversas vezes em momentos difíceis durante esses últimos anos de curso e durante o processo de desenvolvimento da monografia. Por fim, a Deus que me sustentou até aqui, mesmo quando eu cogitei desistir, em meio a tanta desesperança, Sua mão sempre me amparou e me fez seguir em frente.

RESUMO

A presente monografia tem como objetivo principal analisar a natureza jurídica e a aplicação da responsabilidade civil no âmbito da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção dados. Nesse sentido, inicialmente procura-se esclarecer quais são os princípios norteadores da lei e quais os diferentes tipos de dados, posteriormente objetiva explorar, através de análise doutrinária, o entendimento sobre qual teria sido o fundamento utilizado na responsabilidade civil na LGPD, bem como uma intersecção entre a Lei de Acesso a Informação e a LGPD. A metodologia empregada à pesquisa é preponderantemente bibliográfica, a partir de pesquisa doutrinária e com o aprofundamento das legislações anteriores e da legislação vigente sobre LGPD relevantes ao tema. Para tanto, utiliza-se a pesquisa documental e bibliográfica, tendo como fontes livros, publicações de revistas, artigos e legislação, principalmente, a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018 e a Lei nº 12.527, de 18 de novembro de 2011. Autores como Pinheiro (2018); Maciel (2019); Bioni (2021), Lima (2022), serviram também amparar a análise. A partir da análise, observou-se que a Lei Geral de Proteção de Dados Pessoais adotou a responsabilidade civil objetiva para responsabilizar o Poder Público, baseando-se do Direito Administrativo e a subjetiva, aos agentes de tratamento, a luz do Código de Defesa do Consumidor, no caso de vazamento de dados, o que condicionou a obrigação de reparar o dano ao exercício de atividade de tratamento de dados pessoais e à violação da lei protetiva em questão. Destarte, por ser considerada uma lei norteada por princípios e elencar uma série de disposições sobre prevenção e segurança dos dados pessoais aos agentes de tratamento, além de estabelecer que a responsabilização dos agentes ocorrerá em expressa violação à lei protetiva, a responsabilidade subjetiva mostra-se como regra geral a ser aplicada.

Palavras-chave: Lei Geral de Proteção de Dados; Lei de Acesso a Informação; Responsabilidade civil; Direito Digital.

SUMÁRIO

INTRODUÇÃO 01

CAPÍTULO I – DOS DADOS PESSOAIS

1.1 Conceito e características dos dados pessoais 03

1.2 Do consentimento 07

1.3 Finalidade e necessidade 09

CAPÍTULO II – LAI X LGPD

2.1 Lei de acesso a informação 13

2.2 Privacidade x transparência.....16

2.3 Conflito ou harmonização legal?.....20

CAPÍTULO III – DA RESPONSABILIDADE CIVIL E FISCALIZAÇÃO

3.1 Da responsabilidade civil do poder público.....22

3.2 Da responsabilidade civil dos agentes de tratamento 25

3.3 Da Agência nacional de proteção de dados.....29

CONCLUSÃO 34

REFERÊNCIAS BIBLIOGRÁFICAS 37

INTRODUÇÃO

O presente trabalho traz consigo o condão de tratar de um tema que historicamente foi responsável pelo aumento exponencial de novas tecnologias alavancando importantíssimos avanços tecnológicos para o mundo. Entretanto, ao passo que referidos avanços possam ser benéficos e de grande valia, há também, assim como em qualquer outra vertente, os malefícios que o seu mau uso pode acarretar.

Devido ao diversos meios e práticas que fazem o uso de dados pessoais, tem sido cada vez mais recorrentes ações de cunho invasivo e discriminatório, o que fortemente concorreu para o fortalecimento do debate quanto à necessidade de regulamentação em todos os âmbitos que envolvem práticas que utilizam e precisam de dados pessoais.

Com toda uma nova regulamentação, faz-se também necessário entender os conceitos a ela atrelados, os bens jurídicos dos quais a lei exerce uma tutela, quem são os responsáveis e com competência para regulamentar, fiscalizar e aplicar sanções caso constatado o seu descumprimento. Verifica-se a necessidade de um estudo que traga clareza quantos aos objetivos e finalidades tendo em vista que se trata de um novo cenário ao qual o mundo, o Brasil e a legislação brasileira estão tendo de se adequar.

Ainda, verifica-se a necessidade de compreender como a lei geral de proteção de dados terá harmonia com a lei de acesso a informação, esta que visa garantir transparência de informações aos cidadãos ao passo que a outra tem o objetivo de resguardar a intimidade e inviolabilidade de fatos e garantias pessoais,

que não devem de forma alguma servir de meio para o seu prejuízo. Sendo assim, é de grande importância o estudo e análise dessas vertentes e como essa legislação tem surtido e possa surtir os melhores efeitos de forma equilibrada para atingir suas finalidades e objetivos.

Desta, a pesquisa científica que segue, por meio de um procedimento bibliográfico, utilizando-se de um método de abordagem empírica e analítica, foi estruturada em três capítulos, sendo abordada no primeiro capítulo o conceito de dados pessoais, no segundo a intersecção entre a LAI e a LGPD e por fim no terceiro as disposições da responsabilidade civil, tanto pelo poder público, quanto pelos agentes de tratamento e explicitar a respeito da ANPD.

CAPÍTULO I – DOS DADOS PESSOAIS

O presente trabalho proposto pretende analisar e conceituar questões relacionadas ao tratamento de dados pessoais na Lei 13.704 de 14 de agosto de 2018. Em seguida, tratar da visão de consentimento segundo a referida lei. Por fim, discorrer sobre a finalidade e a necessidade da proteção de dados no país.

1.1 Conceito e características dos dados pessoais

A definição de dados pessoais é a delimitação essencial para a proteção das informações do indivíduo, exatamente por demarcar o domínio deste direito. Pode o referido direito ser mais restrito, onde limita a interpretação dos operadores do direito, ou mais amplo, possibilitando a análise sob novas perspectivas. Tal análise pode ser feita já que a lei se refere a “pessoa natural identificada” e a “identificável”, onde podem ser traçados e identificados perfis baseando-se apenas num padrão de ações do indivíduo.

Conforme apresentado por Bernardo Menicucci Grossi para a Comissão Especial de Proteção de Dados da OAB de Minas Gerais: “Considera-se dado pessoal aquele que se encontra atrelado à projeção, à extensão ou à dimensão de uma determinada pessoa, tanto na sua esfera individual, quanto em sua esfera relacional”. (GROSSI, 2020*, online*).

O intuito basilar da Lei 13.709/2018 é a regulamentação do tratamento de dados pessoais pelos captadores de informações sobre os indivíduos, digitalmente ou não. A captação desses dados deve seguir um protocolo linear para a legalização

da sua utilização, aplicando-se essas etapas a pessoais naturais, jurídicas, públicas ou privadas, com enfoque nos meios digitais.

Como elencado no artigo 5º da referida lei, conceitua-se os dados pessoais como toda e qualquer informação que possa levar a identificação da pessoa natural. Ou seja, dados como nome completo, e-mail, telefone, Carteira de Identidade (RG), Cadastro de Pessoa Física (CPF) e endereço, conta bancária, tal como dados indiretos, como endereços de IP, geolocalização de dispositivos móveis e demais identificadores eletrônicos (BRASIL, 2018*, online*).

O inciso II do supracitado artigo, define como dados sensíveis os dados passíveis do uso incorreto para fins discriminatórios e prejudiciais ao cidadão; como acesso a informações sobre a 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; tais informações requerem uma proteção maior, já que tratam de questões extremamente privadas e necessitam do consentimento específico do titular (BRASIL, 2018*, online*).

De acordo com Patrícia Pinheiro, os dados sensíveis merecem tratamento especial, porque em algumas situações a sua utilização mostra-se indispensável, porém o cuidado, o respeito e a segurança com tais informações devem ser assegurados, haja vista que – seja por sua natureza, ou por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa (PINHEIRO, 2018).

Seguindo na análise do artigo 5º, o inciso III trata de dados anonimizados. Tal categoria é assim nomeada quando um dado pessoal deixa de ser diretamente relacionado a uma pessoa que não permite ser identificada, considerando a utilização de meios para seu tratamento. Um exemplo é em relação às pesquisas de recenseamento, onde os dados pessoais do entrevistado são colacionados aos dos demais e se tornam estatísticas; esses dados estão fora da proteção da LGPD (BRASIL, 2018*, online*).

Há de se atentar quando se fala em dados anonimizados, pois conforme a lei, tal categoria não é considerada como tratamento de dados pessoais. A lei é clara quando estabelece no art.12 em seu caput: “os dados anonimizados não serão considerados dados pessoais para os fins desta Lei.”, mas há exceções que são resguardadas quando o processo de anonimização for ou puder ser revertido. (BRASIL, 2018*, online*).

Há também uma subcategoria, que são os dados “pseudo-anonimizados”, nos quais são tratados de forma semelhante ao da anonimização, porém neste caso algumas informações adicionais são mantidas particularmente pelo controlador em um local seguro. O “pseudo-anonimato” é encorajado pelo próprio regulamento como forma de reduzir os riscos, sendo assim, torna-se compreendido pela Lei Geral de Proteção de Dados.

Sendo assim, a “pseudo-anonimização” trata a privacidade do titular como prioridade. Lidando com as consequências de possíveis intercorrências, um bom exemplo é o vazamento de dados pessoais, que seriam afetados apenas os não-identificáveis, evitando problemas ao titular.

Ao determinar como deve ser feito o tratamento de dados pessoais, a LGPD destaca o princípio da boa-fé, onde também faz-se necessário atentar-se a questão do consentimento solicitado de forma clara e explícita, e que seja sempre com uma finalidade determinada, tendo limites, que haja prestação de contas, que seja garantida a segurança e transparência, assim como a livre consulta dos titulares, caso haja pedido, tudo isso torna-se ainda mais importante quando tratamos dados sensíveis (BRASIL, 2018, *online*).

Nos casos de exceções em que o tratamento pode ser feito sem pedir o consentimento do titular, a tratativa dos dados é semelhante ao que é feito nos casos comuns: há de se obedecer a regulamentação, executar políticas públicas, realizar pesquisas.

A LGPD deixa explícito em sua redação a proibição ao controlador de vender ou compartilhar os dados com o intuito de gerar lucro, sendo passível de

punição. Claro que com exceção de quando há necessidade de compartilhar tais dados para prestação de serviços relacionados a saúde, onde tal exceção abre margem para uma portabilidade de dados médicos, como por exemplo de um hospital para outro (BRASIL, 2018, online).

O tratamento de dados pessoais por órgãos de pesquisa que investigam questões relativas à saúde pública deve acontecer única e estritamente dentro do órgão e para fins de produção científica com todos os cuidados de praxe. Nesses casos é preferível dar predileção para a anonimização (ou pseudo-anonimização) dos dados, haja vista que a intimidade e privacidade dos titulares deverão ser protegidas (PINHEIRO, 2018, *online*).

Os dados relacionados aos menores de dezoito anos estão classificados em uma categoria específica, visto que requerem um maior cuidado. É necessário garantir que o consentimento realmente foi fornecido por um dos pais ou responsáveis legais.

Pondera a doutrina que nos casos excepcionais, o controlador poderá usar de tais dados para contatar o responsável legal pela criança ou quando eles forem necessários para proteger o titular menor de idade, em qualquer um desses casos não é permitido o compartilhamento dos dados obtidos.

Dita a LGPD que as informações sobre o tema devem ser fornecidas com uma linguagem adequada a idade dos usuários do produto/serviço em questão. Dispõe também que o fornecimento de tais informações devem ser de forma clara, simples e acessível podendo utilizar de áudio, vídeo e imagens para complementar as informações e facilitar o entendimento (BRASIL, 2018, *online*).

E após o fim do tratamento, os dados pessoais devem ser eliminados, porém tal ação não é exigida quando o controlador necessita da permanência das informações para cumprimento de suas obrigações legais, e também se aplica essa exceção no que tange aos órgãos de pesquisa (BRASIL, 2018, *online*).

1.2 Do consentimento

Tendo como premissa que se não houver permissão, não há o que se falar em tratamento de dados particulares, então tem-se o consentimento como parte de maior valia tratando-se do assunto em questão, e tal concessão nada mais é do que a permissão dada pelo titular para que determinados dados pessoais sejam tratados.

A solicitação deve ser feita de forma explícita, clara e transparente pelo operador ou controlador, podendo ser por escrito ou por outro meio que demonstre a manifestação de vontade do titular, sem vício de consentimento e referir-se a finalidades determinadas. É necessário destacar que tal concessão pode ser revogada a qualquer momento mediante manifestação expressa do titular, de forma gratuita e facilitada (BRASIL, 2018*, online*).

Como explanado por Patricia Peck Pinheiro, em sua obra que trata de comentários a respeito da Lei Geral de Proteção de Dados: “a linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas” (2018, *online*).

Os artigos 8º e 9º da Lei 13.709/2018 trazem no discorrer de seus parágrafos a hipótese do consentimento que pode ser considerado nulo nos casos em que houver conteúdo enganoso, abusivo ou se as informações forem fornecidas sem a devida transparência, assim como quando houver mudança na finalidade do tratamento no qual fora pactuado anteriormente, que deve ser informada pelo controlador, caso não concorde com as alterações pode ser revogado pelo titular o consentimento, sem necessidade de justificar o porquê não mais autoriza o uso de seus dados.

Nesta mesma lógica, Bruno Bioni diz:

> Nesse sentido, o princípio da limitação da coleta, seguido pelo princípio da especificação dos propósitos, estabelece a técnica normativa pela qual o titular dos dados deve ser informado sobre as

> finalidades do seu processamento para, então, autorizá-lo, consolidando-se, por fim, a sua participação ao longo de todo o fluxo informacional (2019, *online*).

Ao controlador são atribuídas algumas responsabilidades. Uma delas relativa à sua identificação e seus meios de contato para possíveis buscas de informações por parte do titular, bem como também lhe é incumbido o ônus da prova nos casos em que necessitar de comprovação que houve o consentimento e que tal permissão foi concedida em conformidade com o disposto em lei.

Os artigos supracitados também tratam da forma como deve ser feita a solicitação do titular. Primeiramente, as cláusulas referentes ao uso de dados devem vir apartadas das outras, ou seja, não podem ser inseridas no entremeio do termo de uso, perdendo-se no corpo do documento, bem como devem ter finalidade específica, sendo bem explanada a forma e duração do tratamento que será feito, logicamente sendo ponderados todos os pormenores relativos aos segredos comerciais e industriais. Outros quesitos importantes a serem ressaltados é a devida responsabilização dos agentes que tratarão dos dados e a nítida menção de quais são os direitos abrangidos no artigo 18 da Lei aqui discutida.

Tal medida é adotada para que o titular saiba com exatidão o que será feito com seus dados, e para isso é necessário que seja utilizada linguagem clara e acessível para uma fácil compreensão de qualquer pessoa, independentemente de seu conhecimento técnico a respeito do tema.

Neste sentido, Rafael Fernandes Maciel menciona em sua obra que caixas de seleção, que ao abrir da página de aceite já estão previamente sinalizadas não validam o consentimento, pois são consideradas ilegítimas, devendo o controlador do tramite de dados utilizar de meios eficientes para que seja provada a obtenção do consentimento (MACIEL, 2018).

Por outro lado, há hipóteses em que não é obrigatório a solicitação do consentimento, onde a LGPD procura um meio termo entre os interesses do titular de manter controle sobre a utilização de seus dados e as necessidades dos

controladores para exercerem suas atividades, que em alguns casos é imprescindível para o cumprimento de suas obrigações.

Uma dessas hipóteses é quando se trata dos órgãos da administração pública, quando o tratamento é necessário para o efetivo cumprimento de leis e de políticas públicas, bem como os órgãos de pesquisa, mas estes são aconselhados a priorizarem o uso dos dados anonimizados sempre que puderem.

Outras situações de exceção em que o tratamento de dados pessoais pode ocorrer com a falta do consentimento expresso são dadas por Patricia Peck Pinheiro, em sua obra:

> Quando é necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; para a proteção da vida do titular ou de terceiro; quando necessário para atender aos interesses legítimos do controlador ou de terceiro; para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (2018, *online*).

Observa-se então que, ao contrário do que é pré-concebido por muitos, são várias as possibilidades de uso dos dados pessoais sem o consentimento do titular, principalmente no tocante a contratos e ao dever de assegurar os direitos tanto do titular, quanto de terceiros.

1.3 Finalidade e necessidade

A sistemática da organização da LGPD por si só já especifica com clareza a razão pela qual se faz uso de um dado. Mas os princípios da finalidade e da necessidade trazem ainda mais definições concretas para esse tema, que engloba o legitimo interesse do controlador, a minimização de dados e a pertinência, entre outros tantos tópicos alusivos ao assunto em questão.

O primeiro inciso do artigo sexto trata da finalidade e discorre a respeito de que se deve informar o titular e realizar o tratamento para propósitos legítimos,

específicos, explícitos e onde não haja a possibilidade de um tratamento de dados que não esteja em harmonia com essas finalidades (BRASIL, 2018*, online*).

De acordo com Bruno Bioni, “a definição de uma finalidade é o que permitirá analisar regressivamente se o cidadão foi adequadamente informado para iniciar um processo de tomada de uma decisão livre”, para que não reste dúvidas acerca do fim ao qual os dados serão utilizados (2019, *online*).

A delimitação, ou a falta dela, causa um problema na aplicação da Lei 13.709, pois não se sabe até que ponto pode-se flexibilizar a fundamentação que é tratada no artigo 10. Se for tratada com muita maleabilidade, corre o risco de ficar genérico em demasia, o que consequentemente abre um vácuo no conhecimento do que será tratado; em contrapartida, se usar de grande rigidez, pode sobrecarregar o cidadão levando-o a chamada fadiga do consentimento e a inovação seria prejudicada, pois restringiria a capacidade de uso dos dados pelos controladores.

Neste sentido, Bruno Bioni diz que “toda e qualquer atividade precisaria de um espaço não previamente definido para criação, de modo que exigir um escopo inventivo pré-definido na economia dos dados seria inviabilizá-lo”. Tal delimitação faria com que as possibilidades de se criar algo inédito fossem quase nulas, assim como geraria um incômodo desmedido para os usuários que teriam que deliberar acerca de toda e qualquer coisa, por mais simples que seja (2019, *online*).

Para que não haja tal limitação, foram arroladas possibilidades nos casos em que não se adequem ao artigo inframencionado, não necessitando de uma prévia autorização do titular, valendo ressaltar que como citado no dispositivo, tais situações concretas não se esgotam apenas nas elencadas no bojo do artigo, o que possibilita a avaliação subjetiva do controlador.

Na LGPD há alguns fundamentos para o tratamento com finalidades legítimas, os quais estão previstos no seu artigo 10. São eles:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades

> legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei (BRASIL, 2018, *online*).

Na atual conjuntura da sociedade, um dos bens mais valiosos é a informação, que está presente não só nos fatos noticiosos, mas na construção da opinião pública e na análise crítica, bem como na validação de dados, como exemplo das *fake news* tão disseminadas nas redes sociais. Por isso, a necessidade de se ter uma lei que proteja os dados e informações torna-se imprescindível.

Seguindo por esse caminho, onde após a expansão da tecnologia pelo mundo, houve a consequente disseminação do uso de dados para fins comerciais, por isso deve-se ter um mecanismo para regular esse filtro. Opinam sobre o tema:

> Surge a partir da necessidade de regular o crescente desenvolvimento no campo da tecnologia da informação, de forma a assegurar, em alguma medida, a autodeterminação informativa do indivíduo, voltada para o próprio desenvolvimento de sua personalidade, que é impactada pelo tratamento de seus dados pessoais, tanto no âmbito da administração pública quando do setor privado (FRAZÃO; TEPEDINO; OLIVA, 2020).

Nessa perspectiva, o princípio da necessidade traz consigo a tarefa de criar esse crivo para que não seja usado de forma errônea esta ferramenta para serviços, compras ou quaisquer transações *online* onde necessite o fornecimento de informações pessoais. Bem colocado por Rafael Fernandes, o tripé para a utilização correta dos dados é a finalidade, adequação e a necessidade. O princípio da necessidade carrega o posto de impeditivo crucial para a desmedida utilização dos dados, que devem ser “pertinentes, proporcionais e não excessivos” (MACIEL, 2019).

Após a confirmação do legítimo interesse do controlador, avalia-se a real necessidade de usar todos os dados solicitados para atingir o fim desejado. Para isso, aplica-se o princípio da necessidade que é guiado pela minimização, tendo como objetivo o uso do mínimo de dados possível.

Neste sentido, Bruno Bioni faz um importante questionamento sobre a reflexão, onde “se seria possível atingir o mesmo resultado por meio de uma quantidade menor de dados, sendo, em última análise, menos intrusivo e impactando menos o indivíduo”. Por exemplo, nas pesquisas de recenseamento baseadas em estudos de natureza demográfica, epidemiológica ou de planejamento em saúde pública, faz-se necessário conhecer o objeto de pesquisa, que neste caso são as pessoas a serem entrevistadas, para isso usa-se de dados obtidos em levantamentos periódicos ou ocasionais (2019, *online*).

A indústria do *marketing* e da publicidade tem como padrão o agrupamento do maior número de informações possíveis sobre os consumidores, para criar um perfil mais completo da personalidade e preferências dos usuários. E é neste contexto que deve ser aplicado o princípio da minimização, para que a coleta dos dados não seja intrusiva e excessiva. Conforme dita o artigo 6º, inciso III da legislação nos seguintes termos: “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” (BRASIL,2018, *online*).

Em suma, o princípio da necessidade funciona como uma diretriz da legislação, estipulando dentro do contexto da Lei Geral de Proteção de Dados, de forma restritiva e garantindo que somente dados pessoais pertinentes para o atendimento da finalidade pretendida sejam coletados para o uso no tratamento de dados, sendo dispensada a coleta excessiva, bem como o princípio da finalidade tem como propósito proteger as informações pessoais do titular, fazendo com que os dados coletados em situações específicas não sejam utilizados indevidamente ou para fins não esclarecidos. Esses dois princípios sintetizam todos os outros que compõem a LGPD.

CAPÍTULO II – LAI X LGPD

Este capítulo trata acerca da Lei de Acesso a Informação e a relação com a Lei Geral de Proteção de Dados no ordenamento jurídico brasileiro. Aborda as disposições legais acerca das referidas leis, bem como, apresenta o viés da privacidade em oposição à transparência governamental. Por fim, demonstra o limiar entre as considerações finais de tribunais superiores e um conflito.

2.1 Lei de acesso a informação

Com o objetivo de garantir o direito constitucional dos cidadãos ao livre acesso às informações públicas, a Lei de Acesso a Informação foi sancionada em 18 de novembro de 2011, sendo ela aplicável para os três poderes da União, dos Estados, do Distrito Federal e dos Municípios.

Seu propósito é trazer mais transparência sobre o Governo e de facilitar para o cidadão o acesso às informações de caráter público, instituindo obrigações, prazos e procedimentos para a divulgação de dados. Nesse sentido como previsto pela Carta Magna no art. 5º, inc. XXXIII: “Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado” (BRASIL, 1988, *online*).

Para que os cidadãos possam desempenhar seus direitos e deveres como personagens ativos da sociedade é necessário que recebam orientações

sobre como podem ser fiscais das ações do Estado. Com base no artigo supracitado, nota-se que no Brasil a democracia é participativa, isto é, a população atua ativamente nas decisões de interesse coletivo e para a consolidação da democracia o acesso às informações públicas é fundamental, pois viabiliza aos cidadãos a participação efetiva nas decisões que afetam toda a sociedade.

A Lei de acesso a informação, publicada dia 18 de novembro de 2011, (Lei nº 12.527/2011) determina a obrigatoriedade da prestação de contas de todos os órgãos e entidades da Administração Direta e Indireta – seja empresa pública, sociedade de economia mista ou entes controlados pela União – bem como, de entidades privadas sem fins lucrativos que recebem recursos públicos (BRASIL, 2011, *online*).

Os princípios norteadores que ditam a disponibilização de informações é a publicidade e a transparência das informações, sendo o sigilo uma exceção do preceito geral. Isto posto, compreende-se que toda e qualquer informação que está sob o domínio do Estado é sempre pública, tendo seu acesso restrito apenas em casos especiais e por período definido. Patrícia Peck, conceitua em sua obra “Direito Digital” a importância de se manter a sociedade informada: “O acesso à informação constitui o maior valor de uma sociedade democrática, e a massificação da Internet como serviço de informação e informatização possibilita um aumento de competitividade global de comunidades antes marginalizadas” (2007, p. 41).

De acordo com a referida lei, assim como preceitua a LGPD, os dados pessoais são as informações que tem relação com a pessoa natural identificável. A forma de tratamento desses dados deve ser feita seguindo uma linha ética de respeito a intimidade, à vida privada, a honra, a imagem do indivíduo, a liberdade e as garantias constitucionais.

É importante salientar que, as informações pessoais não são públicas e terão seu acesso restringido – independente da classificação de sigilo – por um prazo máximo de 100 (cem) anos. Podem ser acessadas a qualquer tempo pelo cidadão mediante comprovação de identidade e, apenas em casos excepcionais previstos em lei, terceiros poderão ter acesso (BRASIL, 2011*, online*).

A classificação “sigilosa” se dá, para aquela informação que possui alguma restrição de acesso, tendo sido classificada por alguma autoridade competente. Em virtude da sua necessidade para a segurança da sociedade, englobando a vida, a segurança e até mesmo a saúde da população, bem como do Estado, perfazendo as necessidades da soberania nacional, relações internacionais e atividades de inteligência.

Baseado na redação da lei, compreende-se como “dado”, toda e qualquer informação, seja registrada em papel, computador, filmes ou outro meio, independente do registro e do sistema onde fora protocolizado, com base nisso, a informação pública pode ser classificada de acordo com seu prazo de sigilo, de acordo com o art.24, § 1º: “I - ultrassecreta: 25 (vinte e cinco) anos; II - secreta: 15 (quinze) anos; e III - reservada: 5 (cinco) anos” (BRASIL, 2011*, online*).

A divulgação de informações dispõe de métodos para facilitar e tornar mais célere o acesso, além de estimular a cultura de transparência e controle social na administração pública. Assim, as informações são disponibilizadas de duas formas, por meio da solicitação específica do interessado e da divulgação pelo setor público independente de requerimento. Como visto no artigo 10 da Lei de Acesso a Informação: “Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida” (BRASIL, 2011*, online*).

É direito do solicitante que a informação pública entregue a ele seja primária: coletada na fonte, detalhada e sem modificações; autêntica: produzida, expedida, recebida ou originada de uma fonte segura; integra: não alterada, a podendo ser adequada de forma que facilite o entendimento, mas sem alterar o conteúdo da informação e atualizada, que engloba os dados mais atuais acerca do tema (UFLA, 2015*, online*).

Conforme aponta Celso Antônio Bandeira de Mello, a responsabilização civil da Administração Pública é diferente da que recai sobre o setor privado, assim

como é imprescindível o tratamento adequado ao intuito de satisfazer as necessidades populacionais, a forma de penalizar erros cometidos em face do mau uso dos dados, também devem ser condizentes. Importante ressaltar que cada setor está sujeito a parâmetros diferentes de responsabilização, conforme o autor supracitado esclarece: “Os órgãos públicos estão no âmbito do regime administrativo, logo estão sujeitos às normas e aos parâmetros deste, e consequentemente respondem administrativa e não judicialmente, daí a necessidade de tratamento específico dentro dos limites das normas administrativas” (2019, p. 142).

A Lei de Acesso a Informação deixou claras as obrigações de quem, no seu dia a dia, tem contato, manipula ou guarda informações públicas. O agente público ou militar que descumprir propositalmente essas obrigações poderá ser punido com, no mínimo, suspensão, além da possibilidade de responder por improbidade administrativa. A lei define como condutas ilícitas que podem ensejar responsabilidade: não fornecer informações públicas e não proteger informações sigilosas.

2.2 Privacidade x transparência

O presente tópico trata da linha tênue que se delimita entre a privacidade dos usuários e a transparência das empresas no tratamento de informações. Traz preposições acerca do uso correto e das consequências quando ocorre abuso no tratamento dos dados.

Tal abuso pode ser feito tanto por parte da esfera privada, quanto da esfera pública, e o intuito da aplicação da lei é justamente que evite que tal erro ocorra, visando uma maior segurança e confiança por parte da população, principalmente no que tange a administração pública, para que haja uma linha bem delimitada da extensão do uso de dados pessoais da população. Conforme aponta Celso Bandeira de Mello: “(...) os órgãos públicos estão no âmbito do regime administrativo, logo estão sujeitos às normas e aos parâmetros deste, e consequentemente respondem administrativa e não judicialmente, daí a

necessidade de tratamento específico dentro dos limites das normas administrativas" (MELLO, 2019, p.412).

Dentro do corpo textual da LAI, não existe até o momento sansão financeira para os entes públicos, diante a Administração Pública direta e indireta, entretanto, o servidor que ocasionar tal erro poderá ser enquadrados na Lei de Improbidade Administrativa, bem como, responder a um Processo Administrativo. Porém, tanto a LAI quanto a LGPD fazem parte da pirâmide de Kelsen, que no qual os agentes, servidores e empregados públicos tem como bussola de orientação a Constituição de 1988.

Um dos maiores problemas acerca do julgamento de erros advindos de uma má utilização dos dados, é o efetivo funcionamento da ANPD (Autoridade Nacional de Proteção de Dados), que ainda tem uma certa obscuridade e omissão no que diz respeito a sua atuação. Com o advento da LGPD, foi estipulada a criação do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), que é um órgão consultivo da ANPD, tendo como maior atribuição propor diretrizes estratégicas e fornecer subsídios para a elaboração e efetivação das leis supracitadas (BRASIL,2018*, online*).

É evidente que ao lidar com dados pessoais o responsável tem consciência que está sendo-lhe concedido um acesso a assuntos com teor privativo, de alta relevância, portanto, cabe a empresa assegurar que tal manuseio seja feito de forma que não ultrapasse os limites permitidos por lei.

Para nortear essa limitação, a legislação brasileira nos traz as duas leis que podem ser correlacionadas no que tange a privacidade e transparência de dados, a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação.

Uma análise certeira deste co-relacionamento entre as duas leis é feita neste trecho:

> Ao contrário do que se observa nas negativas de acesso à informação que se fundamentam na LGPD, a proteção de dados e acesso à informação não se encontram em polos distintos. Isso porque a proteção de dados se diferencia da proteção à privacidade. A lógica da proteção de dados se pauta pela garantia de um fluxo

> informacional adequado, e não da interdição de um fluxo informacional. Ambas as leis analisadas operam pela lente da redução de assimetria informacional entre Estado e cidadão (BIONI, *online*, 2022).

Nos últimos anos, observou-se um novo modelo de negócio no âmbito da rede mundial de computadores. Pôde-se verificar a migração de pessoas jurídicas e físicas para o mundo virtual, o que foi viabilizado pelos avanços tecnológicos e pela globalização. Diversas empresas e pessoas físicas começaram a disponibilizar os seus serviços online, bem como produtos que possuem conectividade com a internet.

Com a evolução tecnológica, foram sendo criadas novas profissões, bem como, transformações no padrão de labor, assim aumentando a capacidade de comunicação e o valor a ela dado. Essa inovação traz consigo uma maior importância para os dados, que se tornam cada vez mais valiosos, principalmente no mundo empresarial.

Pois bem, mesmo havendo diversas medidas para a adequação do mundo empresarial nas diretrizes da LGPD, como explanado no artigo A Evolução do Teletrabalho “(...) há de ser utilizado meios como o *compliance* digital e uma nova forma de cultura organizacional digital, baseada nos preceitos éticos e valores empresariais modernos)”, pois não há melhor forma de prevenção de conflitos que uma efetiva implementação de protocolos de segurança para a regulamentação da lei (ZAVANELLA, 2021, p.41).

Dentro de uma aplicação qualificada do *compliance,* determinadas diligencias devem ser feitas, tais como, mapear os dados manipulados pela empresa, meio de entrada e saída dos dados, o curso dos dados dentro do sistema interno, quem acessa e se está efetivamente autorizado a manipular, bem como, como identificar uma possível irregularidade no seu manuseio, e quando/onde ocorreu, para assim conseguir sanar o erro (VIEIRA, 2022, *online*).

O propulsor jurídico que trouxe o assunto de privacidade digital foi o PL 2126/11, que diz respeito ao Marco Civil da Internet, que mesmo não trazendo consigo qualquer tipo de proteção prática quanto à espionagem internacional, tinha

alguns conceitos e princípios a respeito da privacidade e da proteção de dados pessoais onde trouxe consigo, por exemplo, o artigo 3º, que abordou o princípio da proteção da privacidade e dos dados pessoais: “Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] II - proteção da privacidade; III – proteção dos dados pessoais, na forma da lei.,” (SOARES, 2020, *online*).

Nessa perspectiva, o artigo 7º no inciso VII, VIII e X da LGPD, trás consigo os conceitos:

> [...]
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação;
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.
> [...]
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; (BRASIL, 2018*, online*).

Na esfera pública, o tratamento de dados para o legal cumprimento da obrigação regulatória tem de ser levado em consideração junto a Lei de Acesso a Informação. A regulamentação dos órgãos públicos após a entrada em vigor da LGPD impulsionou a adequação de outras entidades às regras da proteção de dados, fazendo com que haja uma maior materialização dos princípios da eficiência e transparência na administração tanto publica quanto privada (BIONI, *online*, 2022).

Logo, no mesmo sentido, os princípios da necessidade e finalidade também são de extrema importância para a devida aplicação da delimitação de quais dados serão utilizados e compartilhados, dando assim, mais segurança ao requerente, o que traz clareza e limita a extensão do poder público na utilização dos dados pessoais da população (BIONI, *online*, 2022).

2.3 Conflito ou harmonização legal?

O presente tópico aborda principalmente o questionamento acerca das duas leis anteriormente tratadas, se elas se complementam ou divergem juridicamente, trazendo posicionamentos e comentários acerca da maneira como se dará essa harmonização e em casos de inconsonância, qual prevalecerá.

Inicialmente, cabe ressaltar que grande parte da redação da Lei Geral de Proteção de Dados é semelhante ao texto da Lei de Acesso a Informação, porém em alguns artigos o tema é tratado de forma mais aprofundada ou voltada para a aplicação do tratamento de dados. Dentre essas semelhanças, as que mais se destacam são as diretrizes norteadoras destes dispositivos, que juntas formam um tripé de sustentação, são elas: confidencialidade, integridade e disponibilidade, indicadores estes que estão diretamente alinhados aos princípios da prevenção e da segurança (SERPRO, 2020, *online*).

É plausível a preocupação de quem terá maior soberania quando houver divergência entre os interesses públicos e particulares acerca do acesso e liberação de certos dados. Pois mesmo que a LAI trate do acesso público a informações privadas, e a LGPD sobre o tratamento de dados, em algumas situações estes caminhos se cruzarão, principalmente no que tange a Administração Pública tratando de dados para uso com fins de bem coletivo.

Diante disso, Cintia Rosa Lima esclarece que se a informação for pública e de interesse social, o direito à informação tende a predominar:

> Dessa forma, a Lei n. 12.527/2011 oferece subsídios para a interpretação sistemática em que, quando existir conflito entre o direito à privacidade, à intimidade, de um lado, e o direito à informação, de outro, se a informação for pública e de interesse social, esse direito tende a prevalecer. (LIMA, 2020, p.167)

Esta prevalência se dá pois não há nenhum direito que seja absoluto, mesmo que haja as cláusulas pétreas da Constituição, e seguramente há momentos que é necessário deixar de lado direitos fundamentais individuais em detrimento da coletividade. Mas para que não haja ocasiões onde fique obscuro o limiar desta

predominância, há de se ter um crivo perfeitamente claro para elucidar tais dissídios. Pois os direitos a privacidade e a intimidade são garantias constitucionais de todo e qualquer cidadão, elencados no artigo 5º, X, CF/88 (BRASIL,1988*, online*).

Em uma análise perfunctória das duas leis, é passível a compreensão de que a LGPD tem como intuito a proteção do uso de dados pessoais por terceiros. Mas o que se destaca é a flexibilização da proteção no tocante ao exercício de uma atividade da Administração Pública, pois do momento da inserção na esfera governamental, as informações contidas tornam-se de domínio de interesse público, o que deve ser de livre acesso a toda sociedade.

Assim, resta claro que há uma interconexão das bases de dados públicas e privadas que existem atualmente no país, onde são justificáveis o uso de dados sem o consentimento do titular. Tais situações existem quando nas hipóteses de proteção de credito, proteção da saúde e da segurança pública, ou ocasiões excepcionais onde é necessário para o devido andamento organizacional da administração pública brasileira.

Em suma, não existe um conflito entre as leis aqui tratadas e sim uma complementariedade entre elas. Haja vista que, a LAI em sua redação já trouxe a regulamentação do direito a proteção a privacidade com relação ao Estado, e posteriormente quando nasce a LGPD, essa questão é ainda mais detalhada. Bem como, no que tange ao âmbito público será observado o disposto em legislação especifica, ou seja, os prazos e procedimentos serão submetidos aos já especificados na LAI. Assim, a integração entre as duas leis é evidente, visto que, por meio da LGPD a administração pública tem de deixar claro de que forma se dará o tratamento das informações, ampliando a transparência e segurança (INTELIGOV, 2020, *online*).

CAPITULO III – DA RESPONSABILIDADE CIVIL E FISCALIZAÇÃO

O derradeiro capítulo deste trabalho aprofunda inicialmente no tocante a responsabilidade civil, tanto por parte da administração pública, quanto por parte dos agentes de tratamento dos dados. Explanando a respeito do teor jurídico das possibilidades de responsabilização, e posteriormente, elucida sobre a Agência Nacional de Proteção de Dados, esclarecendo sobre o que é o órgão e qual sua funcionalidade.

3.1 Da responsabilidade civil do poder público

É cediço no sistema jurídico da sociedade atual que, toda e qualquer atividade que tem como consequência um prejuízo para outrem, gera automaticamente uma responsabilidade e/ou dever de indenizar. Partindo desta premissa, tem-se o termo responsabilidade civil, que é utilizado para as situações onde a pessoa física ou jurídica, é responsabilizada pelos atos, fatos ou negócios danosos que cometeu.

Inicialmente cabe esclarecer que a Seção III da LGPD que trata da responsabilidade e do ressarcimento de danos, não especifica qual a responsabilidade civil que os agentes sofrerão. Mas em seu artigo 45 diz que permanece as regras aplicadas as relações de consumo, sendo assim, muitos doutrinadores entendem que deve ser aplicada a regra da responsabilidade objetiva na maioria dos casos e apenas nas exceções poderá ser aplicada a responsabilidade subjetiva, como é utilizado no Código do Consumidor (BRASIL, 2018, *online*).

Seguindo nessa mesma linha da responsabilidade objetiva, a intenção da redação da LGPD foi restringir o tratamento dos dados para diminuir o risco de vazamentos, considerando que o próprio tratamento de dados, em si, apresenta risco intrínseco aos seus titulares, os autores Laura Mendes e Danilo Doneda dissertam que:

> A consideração da responsabilidade dos agentes leva em conta, em primeiro lugar, a natureza da atividade de tratamento de dados, que a LGPD procura restringir às hipóteses com fundamento legal (art. 7º) e que não compreendam mais dados do que o estritamente necessário (princípio da finalidade, art. 6º, III) nem sejam inadequadas ou desproporcionais em relação à sua finalidade (art. 6º, II). (DONEDA, MENDES, 2018, p. 479).

Essas limitações ao tratamento de dados, associadas com a verificação de que a LGPD assume como regra a eliminação dos dados quando seu tratamento for encerrado, indicam que a Lei procura minimizar as hipóteses de tratamento, de forma que, a legislação tem como um de seus fundamentos principais a diminuição do risco.

Mas há aqueles que acreditam ser a forma subjetiva a regra geral, e não a exceção. Haja vista, os esforços do legislador em criar diretrizes de conduta para os agentes de tratamento, cumprimento de programas, políticas internas, procedimentos e mecanismos de supervisão.

A vista do art. 6º da LGPD, foram estabelecidos princípios que deverão ser seguidos no exercício do tratamento de dados, assim elencados como princípios a “responsabilização” e a “prestação de contas”. Segundo o art. 6º, inciso X, da LGPD, os agentes deverão demostrar a “adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas” (BRASIL,2018, *online*).

Assim, para Marçal Justen Filho a “responsabilidade é inerente à existência de um dever jurídico”. Quando há a existência do dano, seja ele moral ou material, causado por conduta comissiva ou omissiva antijurídica imputável ao Estado, o autor supracitado expressa sua opinião na mesma obra dizendo que “há

presunção de culpabilidade derivada da existência de um dever de diligência especial” (JUSTEN FILHO, 2015).

Resta, entretanto, considerável questão sobre o nexo de causalidade, visto ser usado como regra geral a aplicação da teoria objetiva. Apenas será considerado o afastamento da responsabilidade quando houver a ocorrência do dano, caso fique demonstrada a inexistência do próprio ato danoso ou do vínculo de causalidade estabelecido entre a conduta da Administração Pública e o dano sofrido pelo particular.

Conforme aponta Marcelo Vinícius Miranda Santos:

> Por derradeiro, o artigo 43 trabalha com as clássicas hipóteses de rompimento do nexo causal por culpa exclusiva da vítima ou de terceiro. Aqui, não há propriamente uma inovação. Tais circunstâncias extinguem ou modificam o direito alegado, dependendo da exposição de novos fatos, de maneira que a sua comprovação já seria imputada ao suposto causador do dano. (2021, *online)*

Atentando-se ao caderno processual da Lei *in casu*, ela não prevê o elemento da culpa, porém não deixa claro e evidente a exclusão do tal elemento. Visto a sua subjetividade em certos pontos onde tenta de forma intrínseca fazer com que o agente de tratamento preste contas de todos os seus atos, restando uma dúvida acerca de que, se tais explicações seriam justamente para caso houver um ato danoso o agente não se responsabilizar.

Ainda, carrega como condição da obrigação de reparar, o fato de que ao tempo do tratamento dos dados, ter sido a operação de tratamento dos dados feita de forma danosa, executada violando à legislação de proteção de dados. Depreende-se como consequência do todo, conforme aponta Gisela Sampaio da Cruz, que são empregados apenas dois preceitos objetivos para fundamentar a responsabilidade, sendo o exercício da atividade de tratamento de dados e a violação da legislação de proteção de dados (CRUZ, 2019).

A Lei aqui tratada não regulamenta minuciosamente o regime de responsabilização da administração por danos decorrentes de tratamentos de dados

pessoais. Prevê em seu artigo 31 e 32 somente que, a ANPD poderá enviar informes, com medidas cabíveis para que a violação seja remediada, bem como solicitar ao Poder Público que publique relatórios de impacto, ou sugerir a observância de padrões e boas práticas (BRASIL, 2018, *online*).

Na era atual em que o poder público deseja planejar políticas públicas com base em dados para garantir a eficiência de sua implementação, este tema tem especial relevância, desde que sejam levados em conta os riscos decorrentes. Desta forma, a análise da responsabilidade do Estado no âmbito das atividades de tratamento de dados pessoais pode ser realizada tanto de acordo com as normas de responsabilidade estrita por condutas impróprias, como tratamento e partilha irregular de dados, como por outro lado, de acordo com as presunção de responsabilidade subjetiva. No caso de comportamento negligente, como o descumprimento de regras de prevenção e segurança da informação, há a possibilidade de vazamento de dados pessoais dos cidadãos.

3.2 Da responsabilidade civil dos agentes de tratamento

No tratamento de dados existem dois sujeitos que compõem a estrutura funcional da LGPD, que são parte primordial para o bom tratamento dos dados pessoais, com responsabilidades distintas dentro deste processo. Assim denominados como controlador, operador e encarregado, essas figuras fazem parte do corpo laboral do tratamento de dados.

Como tratado acima, o tratamento de dados no âmbito da LGPD pode ser feito por dois agentes, o controlador e o operador. Sendo o primeiro aquele quem detém o controle geral sobre as finalidades e as maneiras pelas quais os dados pessoais são e serão tratados, o segundo é a pessoa que realiza o processamento em nome do controlador. Este profissional pode ser uma pessoa natural ou jurídica, podendo pertencer ao setor público ou privado.

Na administração pública, o controlador será a pessoa jurídica de um órgão ou entidade pública legalmente vinculada, representada por uma autoridade competente para tomar decisões sobre o tratamento desses dados.

De acordo com a LGPD, os agentes de tratamento de dados pessoais são assim definidos:

> Art. 5º: [...] VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> Art. 5º, VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018, *online*).

Dessa forma, cabe ao controlador decidir por qual caminho será feito o tratamento e quais ações tomadas para o resultado esperado. Ele é o indivíduo responsável por todo o caminho trilhado pelas informações sob seu tratamento, desde a coleta até a devida exclusão dos dados.

Para uma relação jurídica segura para ambas as partes, é imprescindível a celebração de contrato entre operador e controlador, para o tratamento de um certo banco de dados individualizado. Ou seja, deve ser especificado quem é o controlador e o operador à cada operação de tratamento de dados pessoais. Isto se deve ao fato de uma empresa ter a possibilidade de desempenhar o papel de controladora em um e em outro tratamento (outro banco de dados), agir como operadora (DE CARVALHO, 2020, *online*).

Sobre o controlador, Rony Vainzof esclarece que: “O conceito de controlador contempla absolutamente todas as decisões sobre as atividades que refletem o ciclo de vida dos dados pessoais. Desde o projeto, passando pela coleta ou recepção, todas as formas de processamento, até o descarte” (2019, p. 106).

Ademais, a delegação de obrigações em relação à reparação por danos decorrentes de atos ilícitos é distinta de acordo com a qualificação do agente de tratamento. Isto é, varia de acordo com o cargo ocupado dentro das delegações das tarefas a serem executadas, se o indivíduo atua naquele banco de dados como controlador ou operador, conforme o disposto nos artigos 42 a 45 da LGPD.

Dentre os agentes de tratamento, temos uma terceira figura que é o encarregado. Ele é o profissional que detém um nível de conhecimento jurídico e informático, no qual possui como responsabilidade principal observar, avaliar e organizar a gestão de tratamento de dados pessoais de uma determinada empresa ou ente público, para que se adapte ao sistema defendido pela lei (LIMA, 2019, *online*).

A relação jurídica estabelecida entre os três agentes de tratamento de dados aqui tratados, deve ser norteada pelo princípio da boa-fé objetiva, em que todos os envolvidos colaboram entre si para o devido cumprimento da Lei Geral de Proteção de Dados Pessoais.

Com relação a responsabilidade solidária, o controlador e o operador respondem pela totalidade da obrigação nos termos do art. 42 da LGPD. Já o encarregado responde de acordo com as regras do Direito do Trabalho (se for funcionário) ou Direito Civil/Empresarial (se for uma empresa contratada para tal finalidade). Contudo, tal responsabilização solidária está condicionada a possibilidade de que aquele que reparar o dano ao titular tenha direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso (LIMA, 2019, *online*).

Sendo assim, gerentes, sócios e empregados são vinculados ao controlador e é a figura que responde por todos os atos. Empregados e outras pessoas naturais vinculadas ao operador também agirão em seu nome. E as consequências de atos lesivos sofridos pelo usuário, serão aplicadas de forma judicial e administrativa, como explica no trecho a seguir:

> Portanto, se um empregado, ou gestor, der causa a algum vazamento, o responsável será o agente de tratamento, empresa ou entidade empregadora, restando àquele a possibilidade de sofrer sanções disciplinares, que lhe poderão ser impostas pelo empregador agente de tratamento, desde uma advertência até uma justa causa, dependendo da proporcionalidade, gravidade e reincidência, além da possibilidade de ação regressiva por dolo ou culpa, se houver prévio ajuste contratual, nos termos do artigo 462 da CLT, parágrafo 1º. (ROSSINI, 2021, *online*)

Seguindo a vertente do direito administrativo, a responsabilização será suportada pelo controlador. Que no meio digital, faz o papel de chefe, sendo o operador e o encarregado, apenas subordinados que serão responsabilizados de forma mais branda, fazendo jus a menor carga de importância de seu cargo, sendo forçoso lembrar que, os casos serão analisados com acuidade e as penalidades poderão sofrer alterações de acordo com a gravidade de cada delito.

Conforme prevê o Capítulo VIII que trata da Fiscalização, seguida pela Seção I das Sanções Administrativas em seu artigo 52, disserta que poderão ser aplicadas diferentes tipos de sanções. Tais medidas estarão condicionadas a gravidade e da proporcionalidade do descumprimento, tais como: advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% do faturamento líquido da pessoa jurídica, limitada, no total, a R$ 50 milhões por infração; multa diária; publicação da infração após devidamente apurada e confirmada a sua ocorrência; entre outras medidas (BRASIL, 2018, *online*).

A seção III em seu artigo 42, que trata da responsabilidade e do ressarcimento de danos, legisla que: “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” (BRASIL, 2018, *online*).

Em uma análise ao artigo supracitado, quando o legislador usa a conjunção “ou”, transmite a ideia de alternância na responsabilidade civil entre o controlador e o operador, de modo que os dois seriam responsabilizados somente se atuassem para a conduta lesiva. Logo, em regras gerais, o controlador e operador respondem de maneira individualizada, na medida de suas funções (CAPANEMA, 2020, *online*).

O instituto da inversão do ônus da prova empregado nas relações de consumo, também pode ser visto na Lei Geral de Proteção de Dados. Sendo que, é possível a sua utilização em favor do titular dos dados nos termos do Código de Defesa do Consumidor, se provar ser verdadeiro a sua alegação de ser pessoa natural, ou se ele for hipossuficiente, essa inversão poderá ser autorizada.

No caderno processual, em seu artigo 43 o legislador elencou três ocasiões que pode se excluir a responsabilidade do agente de tratamento. Sendo a primeira onde trata do agente que não realizou o tratamento de dados pessoais que lhe é designado; a segunda acontecerá se o agente, mesmo tendo realizado o tratamento, tenha violado a legislação protetiva, além de não ter observado as normas técnicas adequadas para a segurança da informação; a terceira e última ocorrerá quando se tratar de culpa exclusiva do titular dos dados ou de algum terceiro (BRASIL, 2018, *online*).

Assim como recai sobre o Poder Público, o artigo 45 da LGPD prevê que, na ocorrência de violação dos direitos dos titulares no âmbito das relações de consumo, serão aplicáveis as regras de responsabilidade previstas na legislação pertinente, sendo que tal previsão se trata da responsabilidade objetiva, visto ser expresso pela legislação do CDC.

Em suma, pela análise de diversos segmentos de pesquisa dos doutrinadores especialistas no assunto da responsabilização na LGPD, é possível verificar que a lei em questão adota o instituto da responsabilidade subjetiva, ou seja, a culpa deverá ser observada de caso em caso. Mediante a uma hermenêutica sistêmica e do diálogo das fontes, tal forma de penalização somente deixaria de ser observada quando houvesse aplicação nas relações de consumo, por expressa previsão da própria LGPD e do Código de Defesa do Consumidor, além dos casos que envolvem a Administração Pública, conforme exposto na Constituição.

3.3 Da agência nacional de proteção de dados

A Medida Provisória nº 869/18, criada em 2018, deu origem a Autoridade Nacional de Proteção de Dados (ANPD) e posteriormente em 2019 foi sancionada a Lei 13.853/19 que oficializou tal criação. Mesmo que o texto oficial da Lei Geral de Proteção de Dados já mencionar uma agência nacional que regularia as regras da nova lei, ainda não havia detalhado com precisão sobre qual seria o órgão.

O artigo 5º da LGPD é o primeiro a esclarecer o conceito da ANPD. O texto conceitua genericamente a autoridade nacional em seu inciso XIX como: Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (BRASIL, 2019*, online).*

Assim, se fez necessário estabelecer um órgão independente para que o estado e as empresas com acesso a informações pessoais possam cumprir a lei e sejam realizadas auditorias caso não cumpram o tratamento adequado desses dados. Diante disso, a entidade também tem a responsabilidade de tornar as políticas destinadas a proteger os dados, conhecidas ao público e incentivar as empresas que usam informações pessoais a compreender e aplicar essas regras.

Dentre as diversas funções para o melhor desempenho e funcionalidade desempenhadas pela Autoridade Nacional estão listadas algumas. Tais como, a aplicação de uma padronização de serviços e produtos que facilitem o controle dos titulares sobre os dados, a colaboração com autoridades de visam a regulamentação pública para exercer sua função em setores específicos e a implementação de simplificação de meios para registrar denúncias acerca da inconformidade com a lei. Para exercer este importante papel, a autoridade possui autonomia técnica e decisória assegurada por lei (GETPRIVACY, 2020, *online*).

A ANPD é um órgão independente e faz parte do Poder Executivo do Governo Federal criada com atribuições de fiscalizar e divulgar a forma devida de utilizar toda a informação pessoal e dados pessoais que circulam dentro das empresas. Em suma, fazer com que cumpra-se as diretrizes da LGPD. Assim como, dispor de uma autoridade nacional para regulamentar a lei faz com que o Brasil esteja dentro do Regulamento Geral de Proteção de Dados da União Europeia, credenciando o país a enviar informações e dados para o bloco.

Sua composição é constituída por membros não remunerados, que formam um conselho diretor de cinco pessoas indicadas pelo Poder Executivo e aprovadas pelo Senado e também por outros servidores. Divididos entre órgão consultivo em vinte e três representantes, onde é incluso pessoas da sociedade civil,

órgão de assistência direta e imediata ao Conselho Diretor, órgãos seccionais e os órgãos específicos singulares (GETPRIVACY, 2020, *online*).

Como já dito anteriormente, a ANPD deve zelar pela proteção dos dados pessoais no Brasil, protegendo os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme previsto no decreto nº 10.474 de 26 de agosto de 2020 que estruturou a ANPD**.**

As obrigações da ANPD são diversas e vão além de apenas fiscalizar e aplicar sanções em caso de violação à LGPD. Além deste caráter fiscalizatório e sancionatório, a ANPD também atua com uma interface de natureza normativa e deliberativa. Além de elaborar as diretrizes que regem o tratamento de dados pessoais e fiscalizar e aplicar sanções em caso de descumprimento da lei, a Agência também tem como obrigação informar e fazer com que a população tenha conhecimento das políticas de proteção aos dados, das práticas e dos direitos sobre os dados.

Visto a prematuridade da real vigência da Agência, é perceptível que ela anda perfaz um papel mais conscientizador do que fiscalizador efetivamente. Assim, permite que as pessoas e empresas envolvidas no meio digital conheçam a lei e suas determinações e tenham tempo de adequar seus processos e sistemas internos. O que não caracteriza-se como *vacatio legis*, pois ela já foi sancionada e está em vigor, mas apenas deixa que a sociedade se familiarize com as novas diretrizes trazidas pela globalização (JESUS, 2022, *online*).

A ANPD pôde iniciar as aplicações de sanções em caso de violação da legislação a partir de agosto de 2021. As penalidades variam de acordo com o caso e após processo administrativo que fará a análise da ocorrência, são aplicadas: advertências simples, multas de 2% do valor do faturamento da empresa ou grupo no último exercício, bloqueio ou exclusão dos dados envolvidos na ocorrência e suspensão ou proibição do acesso ao tratamento de dados pessoais (TEIXEIRA, 2021, *online*).

Em relação as sanções a serem aplicadas, devem ainda serem criadas, a própria lei determina que a autoridade nacional deverá criar um regulamento próprio sobre as sanções, que deve ser objeto de consulta pública, como explanado no trecho: “Este regulamento deve incluir as metodologias que vão orientar o cálculo do valor-base das multas, além de estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.” (GETPRIVACY, 2020, *online*)

Tal criação deveria ter sido feita anteriormente ao sancionamento da lei, visto que, não há como aplicar uma penalidade se ainda não houver sequer a base de cálculo ou a mínima estipulação de dias multa, o que reitera que a ANPD vai analisar cada caso individualmente.

As sanções aplicadas aos agentes e empresas que agirem de forma errônea no tratamento de dados serão penalizados basicamente em:

> Advertência, com prazo para corrigir as infrações; Multa simples de até 2% do faturamento da empresa no ano anterior, até o limite de R$50 milhões por infração; Multa diária de até 2% do faturamento da empresa no ano anterior, até um limite de R$50 milhões por infração; Tornar pública a infração cometida; Bloqueio dos dados pessoais relacionados à infração; Eliminação dos dados pessoais relacionados à infração; Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período; Suspensão da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período; Proibição parcial ou total das atividades relacionadas a tratamento de dados. (GETPRIVACY, 2020, *online*)

Se faz necessário reiterar que as sanções somente serão aplicadas mediante abertura de um processo administrativo para que haja a possibilidade de ampla defesa, contraditório e o direito de recurso. Bem como, a cooperação do infrator, a pronta adoção de medidas corretivas e a implementação de mecanismos internos para o tratamento adequado dos dados serão grandes critérios para a aplicação de tais sanções.

Em analise ao art. 55-J, VIII, seu corpo textual confere à ANPD a competência de informar aos órgãos de controle interno o descumprimento da Lei. Tal transgressão que pode ser praticada por órgãos e entidades da administração

pública federal, indica que, o órgão será incumbido por reportar eventuais infrações aos respectivos responsáveis para a tomada das providências cabíveis (FEIGELSON, SIQUEIRA, 2019, p. 146).

O atual Presidente da República do Brasil, Jair Messias Bolsonaro editou a MP- 1124/2022 que altera a LGPD transformando a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão. A Estrutura Regimental da ANPD, como órgão federal, continuará vigente e aplicável até a data de entrada em vigor da Estrutura Regimental da ANPD como autarquia de natureza especial (Art. 4º - MP- 1124/2022).

Como é cediço, quando ocorre tais mudanças haverá um período de transição que será estabelecido pela Secretária-geral da Presidência da República e a Autoridade Nacional de Proteção de Dados Pessoais, que tratará do encerramento das atividades de apoio administrativo desta secretaria à ANPD. A Medida Provisória entrou em vigor na data de sua publicação em 14 de junho de 2022 (OLIVEIRA, 2022, *online*).

Assim, resta claro a importância da efetiva atuação da Agência Nacional de Proteção de Dados no Brasil como órgão regulador de todo e qualquer tratamento que envolva dados pessoais. Mesmo que ainda em fase inicial de aplicação, sua autoridade já é vista com bons olhos pela sociedade, posto que, transmite uma maior segurança de que haverá uma regulamentação das normas e responsabilização em casos de vazamento de dados.

CONCLUSÃO

A Lei Geral de Proteção de Dados é a lei nº 13.709, aprovada em agosto de 2018 e com vigência a partir de agosto de 2020, objetiva criar um cenário de segurança jurídica introduzindo a padronização de normas e práticas que promovem a proteção, de forma igualitária, dentro do âmbito nacional e internacional, aos dados pessoais de todo cidadão que esteja no Brasil.

Com a introdução dessa nova lei, o Brasil passou a fazer parte de um grupo de países que contam com uma legislação específica para a proteção de dados dos seus cidadãos. Diante dos atuais casos de uso indevido, comercialização e vazamento de dados, as novas regras garantem a privacidade dos brasileiros, além de evitar entraves comerciais com outros países.

O foco do presente estudo, no entanto, foi analisar todas essas vertentes voltadas a lei geral de proteção de dados, os seus conceitos e finalidades, os bens tutelados e como o direito civil se ajustou para responsabilizar eventuais danos que o desrespeito das normas possa acarretar. Inclusive ressaltando como harmonizar o direito à privacidade e inviolabilidade de dados pessoais com o direito de acesso a informação.

Devido ao diversos meios e práticas que fazem o uso de dados pessoais, tem sido cada vez mais recorrentes ações de cunho invasivo e discriminatório, o que fortemente concorreu para o fortalecimento do debate quanto à necessidade de regulamentação em todos os âmbitos que envolvem práticas que utilizam e precisam de dados pessoais.

Inicialmente, foram feitas considerações no sentido de introduzir o leitor no âmbito da proteção de dados pessoais, demonstrando os principais conceitos e definições relacionadas à tutela jurídica dos dados pessoais. Restou demonstrada que a realização do tratamento de dados deve pautar-se na boa-fé e nos princípios da finalidade, adequação, necessidade, qualidade dos dados, transparência, livre acesso, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Há também a necessidade de o procedimento estar enquadrado em uma ou mais bases legais elencadas pela lei protetiva, sendo o consentimento do titular uma das bases legitimadoras.

Ainda, verificou-se a necessidade da lei geral de proteção de dados harmonizar com a lei de acesso a informação, esta que visa garantir transparência de informações aos cidadãos ao passo que a outra tem o objetivo de resguardar a intimidade e inviolabilidade de fatos e garantias pessoais, que não devem de forma alguma servir de meio para o seu prejuízo.

Em sua parte final, foi apresentada as figuras do controlador, operador e encarregado e suas respectivas responsabilidades, assim como, apresentou o órgão supervisor, chamado de Agência Nacional de Proteção de Dados (ANPD), e abordou o tema que está intrínseco na norma civil brasileira, percorrendo pelos principais conceitos da responsabilidade civil no ordenamento jurídico brasileiro, apontando seus pressupostos e classificações pertinentes ao tema estudado.

Denota-se que a legislação impõe aos agentes de tratamento uma série de condutas e medidas de segurança a fim de prevenir eventuais danos decorrentes do tratamento de dados. Assim, depreende-se que o regime escolhido foi o de responsabilização subjetiva, haja vista a necessidade de previsão expressa nos casos de responsabilização objetiva.

Bem como, a lei *in casu* trouxe a solidariedade como exceção à regra e o instituto da inversão do ônus da prova, anteriormente previstos no Código de Processo Civil e no Código de Defesa do Consumidor. Contudo, não deixou de assegurar a aplicação do CDC, nos casos em que o tratamento de dados incida

sobre relações de consumo, haja vista que assim como indicado na legislação para casos desta classe, se trata de regulamentação própria e específica.

Restou demonstrado que, a partir da análise da LGPD, conjuntamente com outros diplomas e doutrinas é possível vislumbrar os conceitos fundamentais, princípios, agentes e suas atribuições contidos na legislação, assim como, aliar as leis nacionais que tratam acerca da responsabilidade civil para que corroborem com a Lei de Dados para a efetiva responsabilização decorrentes do vazamento de dados, e analisar os limites e especificidades para reparação dos danos atribuídos aos agentes de proteção de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. 3ª ed. São Paulo: Editora Forense, 2021.

BIONI, Bruno Ricardo; SILVA, P. G. F. D; MARTINS, P. B. L. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso**. Cadernos Técnicos da CGU,** Brasilia, v. 1, n. 1, p. 18, mar./2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/issue/view/39/46. Acesso em: 2 abr. 2022.

BRASIL, **Constituição Federal de 1988** no art. 5º, inc. XXXIII; art. 37, §3º, inc. II; e art. 216, §2º. Disponivel em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 2 abr. 2022.

BRASIL, **Lei nº 12.527**, de 18 de novembro de 2011. Disponivel em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 2 abr. 2022.

BRASIL, **Lei Nº 13.709,** de 14 de agosto de 2018. Brasília, DF: Casa Civil, Subchefia para Assuntos Jurídicos, 2018. Capitulo I – Disposições Preliminares, Art. 5,II. Disponível em: http://www.planalto.gov.br/. Acesso em: 21 nov. 2021.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**: Direito Digital e proteção de dados pessoais. São Paulo, ano 21, n. 53, p. 163-170, jan./mar. 2020. Disponível em <https://core.ac.uk/reader/322682320>. Acesso em: 28 jun de 2022.

CRUZ, Gisela Sampaio da. Responsabilidade civil da Lei de Proteção de Dados Pessoais. In: **CONGRESSO INTERNACIONAL DE RESPONSABILIDADE CIVIL DO IBERC**, 3, 2019, São Paulo. Palestras […]. [S. l.]: Iberc, 2019.

DE CARVALHO, Stefani. **Quem são os agentes de tratamento de dados pessoais, de acordo com a Lei Geral de Proteção de Dados?.** 1 jun. 2020. Disponível em: https://stefanidecarvalho.jusbrasil.com.br/artigos/1137566621/quem-sao-os-agentes-de-tratamento-de-dados-pessoais-de-acordo-com-a-lei-geral-de-protecao-de-dados. Acesso em: 28 jun. 2022.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (Coords.). **Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018.** p. 146. São Paulo: Editora Revista dos Tribunais, 2019.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileir**o [livro eletrônico], coordenação. -- 2. ed. -- São Paulo: Thomson Reuters Brasil, 2020.

BRASIL, **Ministério da Justiça e Segurança Pública**. Sobre a Lei de Acesso à Informação - LAI. Disponível em: https://www.justica.gov.br/Acesso . Acesso em: 1 mar. 2022.

BRASIL, LGPD e LAI: uma análise sobre a relação entre elas. Disponível em: https://www.**serpro.gov.**br/lgpd/noticias/2020/lei-acesso-informacao-lai-lei-geral-protecao-dados-pessoais-lgpd. Acesso em: 5 abr. 2022.

GROSSI, Bernardo Menicucci. **Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial** [recurso eletrônico] - Porto Alegre, RS: Editora Fi, 2020.

INTELIGOV. LGPD e Lei de Acesso à Informação. Disponível em: https://blog**.inteligov**.com.br/lgpd-e-lai/. Ano 2020. Acesso em: 15 mai. 2022.

JESUS, Andreia T. S. ANPD – **Autoridade Nacional de Proteção de Dados. Como funciona o órgão responsável por aplicar a LGPD?.** 10 fev. 2022. Disponível em: https://arquivei.com.br/blog/anpd-autoridade-nacional-de-protecao-de-dados-como-funciona-o-orgao-responsavel-por-aplicar-a-lgpd/. Acesso em: 28 jun. 2022.

JUSTEN FILHO, Marçal. **Curso de direito administrativo**. 11. ed. São Paulo: RT, 2015, p.1382, 1409 e 1396.

BRASIL, **LEI Nº 13.709**, DE 14 DE AGOSTO DE 2018. Brasília, DF: Casa Civil, Subchefia para Assuntos Jurídicos, 2018. Capitulo I – Disposições Preliminares, Art. 5º, XIX. Disponível em: http://www.planalto.gov.br/. Acesso em: 28 jun. 2022. Redação dada pela Lei nº 13.853, de 2019.

LIMA, C. R. P. D. **Autoridade nacional de proteção de dados e a efetividade da Lei geral de proteção de dados:** de acordo com a Lei geral de proteção de dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco civil da internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015). 1. ed. São Paulo: Almedina, 2020. p. 167.

LIMA, Cíntia Rosa Pereira de. **Os agentes de tratamento de dados pessoais na LGPD.** 3 nov. 2019. Disponível em: https://iapd.org.br/os-agentes-de-tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 28 jun. 2022.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais**. RM Digital Education. 1ª Edição. Goiânia – GO. 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Ópice. **LGPD Comentada**. 3ª ed. São Paulo: Revista do Tribunais, 2021.

MELLO, C. A. B. D**. Curso de direito administrativo**. 34. ed. São Paulo: JusPodivm, Malheiros Editores, 2019. p. 412.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. Revista De Direito Do Consumidor, v. 120, p. 469-483, 2018

GETPRIVACY, **O que é a ANPD e quais são as suas funções**. [*S. l.*], 8 ago. 2020. Disponível em: https://getprivacy.com.br/anpd-o-que-e/. Acesso em: 28 jun. 2022.

OLIVEIRA, Damião. **ANPD Torna-se autarquia especial**. [*S. l.*], 15 jun. 2022. Disponível em: https://damiaosomaxi.jusbrasil.com.br/noticias/1541947459/anpd-torna-se-autarquia-especial. Acesso em: 28 jun. 2022.

PINHEIRO, Patricia Peck. **Direito Digital:** rev., atual. e ampl. 2. ed. São Paulo: Saraiva, 2007.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** São Paulo: Saraiva Educação, 2018.

ROSSINI, Selma Regina Carloto Martins Guedes**. Descomplicando os agentes de tratamento com base na Lei Geral de Proteção de Dados.** [*S. l.*], 17 dez. 2021. Disponível em: https://www.migalhas.com.br/coluna/migalha-trabalhista/356737/descomplicando-os-agentes-de-tratamento-com-base-na-lgpd. Acesso em: 28 jun. 2022

SANTOS, Marcelo Vinícius Miranda. Critérios de Imputação da Responsabilidade Civil na Lei Geral de Proteção De Dados Pessoais**. Revista Conversas Civilísticas,** Salvador, v. 1, n. 2, jul./dez. 2021. Disponivel em: https://periodicos.ufba.br/index.php/conversascivilisticas/article/view/47539. Acesso em: 28 de jun. 2022.

SOARES, Rafael Ramos. **Lei geral de proteção de dados – LGPD: direito à privacidade no mundo globalizado.** Repositório Acadêmico da Graduação, Goiânia, v. 1, n. 1, p. 13, nov./2020. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/1201. Acesso em: 3 mar. 2022.

TEIXEIRA, Álvaro. **O que é ANPD? [Autoridade Nacional de Proteção de Dados]:** Entenda o que é a ANPD e como funciona o órgão responsável por aplicar a Lei Geral de Proteção de dados, a LGPD. 1 jul. 2021. Disponível em: https://tecnoblog.net/responde/o-que-e-anpd-autoridade-nacional-de-protecao-de-dados/. Acesso em: 28 jun. 2022.

UFLA - UNIVERSIDADE FEDERAL DE LAVRAS. **Lei de Acesso à Informação Orientações Gerais.** Disponível em: https://www.ufla.br/acessoainformacao/wp-content/uploads/2015/12/ApresentacaoLAI.pdf. Acesso em: 1 mar. 2022.

VAINZOF, Rony. Disposições preliminares. In: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **LGPD – Lei Geral de Proteção de Dados Comentada**. São Paulo: Thomson Reuters Brasil, 2019.

VIEIRA, C. G. R. de O. J.; ALMEIDA, I. N. de; FREIRE, M. N. de M.; SIMÕES, M. de L.; LIMA FILHO, P. do N. A Lei Geral de Proteção de Dados (LGPD) e o *compliance* no âmbito trabalhista. **Ensino em Perspectivas,** *[S. l.]*, v. 3, n. 1, p. 1–20, 2022. Disponível em: https://revistas.uece.br/index.php/ensinoemperspectivas/article/view/7360. Acesso em: 03 abril. 2022.

ZAVANELLA, Fabiano; PINTO, L. O. C. **A Evolução do Teletrabalho:** Tomo I - Aspectos Jurídicos. 1. ed. Campinas - SP: Lacier Editora, 2021. p. 40.