LEI GERAL DE PROTEÇÃO DE DADOS E OS PRINCÍPIOS DA LEI

Cezar Augusto Cardoso Bratifisch GOMES[1]

RESUMO: O presente artigo apresenta alguns esclarecimentos a respeito sobre a Lei Geral de Proteção de Dados (LGPD) que foi sancionada em agosto de 2018 e foi aprovado em agosto de 2020. Esta lei entrará em vigor em setembro de 2020 e irá produzir efeitos para quem descumprir os métodos necessários condizente no texto da lei a partir do dia 1 do mês de agosto de 2021 também. Está lei prevê um aumento significativo de segurança dos dados quando os mesmos forem sujeitados aos tratamentos e coletas por agentes responsáveis. Sendo assim, para a realização deste trabalho foram utilizados referências bibliográficas e análises de princípios que regem a LGPD.

Palavras-chaves: Dados pessoais. Dados pessoais sensíveis. Princípios. LGPD.

1 – INTRODUÇÃO

Atualmente a maioria da população de todo o mundo tem acesso à internet, seja por conexão em suas próprias casas ou em praças públicas, este é o momento dos dias atuais e a perspectiva para o futuro é de um avanço tecnológico maior e consequentemente a dependência da população será maior do que já se encontra nos dias atuais.

O presente trabalho tem como objetivo analisar os princípios da Lei Geral de Proteção de Dados (LGPD) que foi sancionada em 2018, entrou em vigor em setembro de 2020 e a produção efeitos a partir do dia 1 de agosto de 2021.

Com o passar do dia a dia, meses e anos vários cadastros são realizados pela população em lojas, sites, aplicativos e entre outros meios que requerem cadastros. Para a realização de um cadastramento é necessário que seja fornecido os dados pessoais de um determinado indivíduo e a LGPD será responsável para que se obtenha um tratamento de forma correta, mais segura para que não tenha vazamento destes, sendo assim evitar um futuro prejuízo ou vexame para os donos dos destes dados vazados. Vale ressaltar que o vazamento pode acarretar em sanções a quem fez a coleta dos dados.

---

[1] O autor é graduando em Direito, cursando o 8º termo da instituição Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente.

O Brasil já possuí leis que tratam da questão de privacidade como a Lei 12.737/2012 chamada de Lei Carolina Dieckmann, que surgiu diante de um fato a qual um hacker invadiu o celular da atriz e a chantageou por obter dinheiro da atriz para a não publicação das fotos. Outra lei é a Lei 12.965/2014 chamada de Lei do Marco Civil da Internet que também prevê proteção de crimes na internet.

É importante ressaltar que esta lei tratará sobre os dados pessoais principalmente no meio digital, por uma pessoa física ou jurídica que seja de direito privado ou público. O respeito a privacidade deve ser sempre respeitado, salvo em situações que constituição brasileira permite o aceso de forma forçada.

Sendo assim, a LGPD entra para dar um respaldo, proteção maior aos tratamentos destes dados pessoais, como se fosse um reforço, como já dito acima o mundo hoje tem uma dependência grande com a tecnologia e se não houver uma certa cautela nos dias atuais o futuro guardará situações nada agradáveis.

2 – DADOS PESSOAIS

Cada pessoa natural é detentora de seus próprios dados pessoais, estes são os responsáveis pela identificação de uma pessoa natural no mundo, seja diretamente ou indiretamente. Os dados pessoais são utilizados para identificar uma pessoa natural viva, o vazamento destes pode causar o rompimento da privacidade de uma determinada pessoa, entre várias outras situações extremamente prejudiciais

A definição de dados pessoais nas palavras de Patrícia Peck Pinheiro:

> Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva (2018. P.25, 26)

As pessoas identificadas ou identificáveis não se limitam somente pelo nome, sobrenome e além dos meios de identificação citados acima, a imagem de uma pessoa natural é passível de ser um elemento para tal função.

Os dados pessoais de uma determinada pessoa natural antes de serem transmitidas elas são consideradas um tipo de pré-informação, por Danilo Doneda:

> Assim, o ´´dado`` apresenta conotação um pouco mais primitiva e fragmentada, como se observa em um autor que o entende como uma informação em estado potencial, antes de ser transmitida. O dado, assim, estaria associado a uma espécie de ´´pré-informação`` anterior à interpretação e a um processo de elaboração (2020. P. 136).

Ou seja, os dados pessoais antes de serem transmitidos são pré-informações de um indivíduo, possuem um potencial lesivo a pessoa natural que irá transmitir esses dados ao domínio de um controlador. Partindo da premissa de que todos os dados pessoais possuem um potencial lesivo, deve ter um cuidado com o compartilhamento destes.

Após o compartilhamento, esse estado potencial ainda está presente e ainda maior, pelo simples fato de que ainda se caso seja vazado, os dados podem ser utilizados para qualquer intenção de quem é o possuidor destes. Um exemplo claro de potencial destes dados é quando uma determinada pessoa possui o número de celular, CPF, RG ou foto de uma pessoa, esses dados possuem a capacidade de identificar uma pessoa, nesse caso pode ser utilizados para o bem, ou caso o detentor pense em fazer alguma coisa ilícita.

2.1 – Dados Pessoais Sensíveis

Os dados pessoais são fotos, número de celular, data de nascimento CPF, RG entre outros meios, já os dados sensíveis são os dados que discriminam a pessoa natural, seja pela sua etnia, cor de pele, crença religiosa entre outros meios de identificação, como está descrito no inciso II, Artigo 5°, da LGPD:

> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Trazendo mais uma definição de dados pessoais pelo professor Bioni: *“uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade, discriminação" (Bioni, 2018, p. 84).*

Desta forma, dados sensíveis e dados pessoais são um conjunto de uma mesma esfera dos dados pessoais, ambas possuem a capacidade de identificar uma pessoa natural e serem lesivas ao proprietário desses dados, por exemplo o acesso de contas em caixas de agências bancárias, é necessário que o solicitante do serviço tenha que se utilizar do nome de pai ou mãe em algumas agências. Portanto, o uso do nome dos pais já se encontra no campo dos dados sensíveis, outro exemplo a ser levado em conta são as opções de orientação sexual que podem vir a gerar uma descriminalização grande, sendo prejudiciais ao proprietário dos dados.

2.2 – Dados pessoais anonimizados

Os dados pessoais anonimizados tem o conceito completamente ao contrário dos dados pessoais e os dados sensíveis aos quais já foram trabalhados neste presente trabalho, de forma que não possui um meio de identificação. Por exemplo em pesquisas para eleições, quem tiver acesso à está pesquisa não terá a mínima ideia de quem participou, estes dados não estarão sujeitos as sanções que a LGPD irá impor. Para melhor esclarecimento a explicação de dados anonimizados se encontra no inciso III, do Artigo 5° da Lei 13.709 de 2018: “dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”

Para mais um entendimento doutrinário seguimos o conceito trazido pela professora Patrícia Pinheiro Peck, “são os dados relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento” (Pinheiro, 2018, p.26).

Os dados anonimizados eles necessitam ter um equilíbrio, nem sempre todos os dados devem ser ocultados, podem ser diferenciados com a pseudoanonimização do Artigo 13° da LGPD, pelo fato de que na anonimização não

tem como chegar ao titular dos dados em questão, já na pseudoanonimização se houver um cruzamento destes será possível chegar ao titular deste.

3 - TRATAMENTO DOS DADOS

Tratamentos dos dados são todas as operações baseados nestes dados pessoais, o inciso X, do Artigo 5° da Lei 13.709 de 2018 elenca as possibilidades:

> X - tratamento: 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;

Esse rol não é taxativo, pode ser que outras formas de tratamento dos dados, como por exemplo gravação de áudio, emissão de relatório, qualquer operação com base em dados pessoais é considerado o tratamento.

3.1 – Princípios aos tratamentos dos dados

A Lei Geral de Proteção de Dados em seu artigo 6° estabelece princípios a serem seguidos para manter um regramento da lei, estes não são taxativos, pelo simples fato de que podem existir outros princípios no mundo jurídico.

É importante salientar que os tratamentos desses dados pessoais não podem ocorrer de forma alguma diferente dos demais tipos de dados pessoais, sendo assim, deve haver um limite para que os dados coletados não sejam usados para gerar uma situação de descriminalização ou uso abusivo dos dados.

O tratamento dos dados pessoais deve ter o consentimento do titular desse, só haverá tratamento destes dados com o consentimento, caso contrário não será legítimo esse tratamento, podendo ter sanções contra quem utilizar os dados sem consentimento do titular.

3.2 – Princípio da boa-fé

Este princípio é o principal da LGPD como também do âmbito jurídico, em quaisquer relação, seja de coleta de dados, compra e venda, entre outras, deve-se haver uma boa-fé para que ninguém seja prejudicado. Para o professor Eduardo Tomasevicius Filho: ´´*Assim, pelo princípio da boa-fé, proíbe-se a mentira, o abuso, o oportunismo, a falta de consideração e a incoerência de comportamento, e impõem-se a transparência e a preservação da confiança legitimamente despertada*``. Este princípio é muito relevante para a LGPD haja vista que tanto para a pessoa natural que irá fornecer seus dados tanto para o coletor destes dados é necessário estar presente este princípio de boa-fé.

3.3 – Princípio da finalidade

O princípio da finalidade está no inciso I, do Artigo 6° da Lei 13.709 de 2018: “I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”.

O princípio em questão também é considerado um dos mais importantes na LGPD, pelo fato de que já está presente a finalidade para a qual está sendo feito o recolhimento dos dados da pessoa natural, além da finalidade, já é previsto que os dados recolhidos não terão nenhum destino a não ser aquele dado no início do fornecimento, assim define o professor Marcio Pestana ´´*realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades*``. Por exemplo não é possível pegar o celular de um cliente dizendo que irá deixar apenas registrado no banco de dados para entrar em contato quando necessário e cadastrar o número em alguma operadora de aparelho telefônico.

3.4 – Princípio da adequação

O princípio da adequação está no inciso II, do Artigo 6° da Lei 13.709 de 2018: “adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento”

Este princípio anda junto com o princípio da finalidade, deve estar de acordo com a finalidade a qual os dados serão destinados, caso aconteça de precisar utilizar os dados da pessoa natural para uma nova finalidade, terá que ser solicitado ao dono desses dados uma anuência para reutilizar estes dados. Para o professor Marcio Pestana ´´ *vocábulo* adequação*, como se sabe, apresenta diversas acepções. Para nós, no ambiente da LGPD, refere-se ao nexo de pertinência lógica de conformidade que se estabelece entre o tratamento e a finalidade objetivada*``. Por exemplo não é aceitável que se os dados foram recolhidos para uma ´´X`` situação, se caso for necessário utilizar os dados para ´´Y`` deve chegar ao conhecimento do proprietário desses dados.

3.5 – Princípio da necessidade

O princípio da necessidade está no inciso III, do Artigo 6° da Lei 13.709 de 2018: “III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados”.

Este princípio ele aumenta a responsabilidade de quem faz as coletas dos dados, apenas será coletado o que for essencial para as devidas finalidades para aos quais os dados forem destinados. O motivo para que este princípio esteja na base legal da LGPD é o simples fato de que quanto maior a quantidade de dados coletados, maiores são as chances de vazamentos destes, dessa forma fica explícito que a coleta não deva extrapolar o limite necessário, e caso ultrapasse o limite de dados necessários o coletor de dados não deve ser enquadrado no caso de abuso de direito, ainda que o mesmo se responsabilize por essa coleta. Para o professor Marcio Pestana *´´consubstancia-se na limitação da realização do tratamento mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidade do tratamento*``.

Dessa forma, fica claro que os dados coletados em excesso à necessidade é prejudicial.

3.6 – Princípio do livre acesso aos dados pelos titulares

O princípio do livre acesso aos dados pelos titulares está no inciso IV, do Artigo 6° da Lei 13.709 de 2018: “IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”.

Aqui basicamente o acesso é garantido a qualquer hora pelo titular destes dados pessoais, de forma gratuita, integral e de uma maneira sem complicações. O titular destes dados também deve ser informado por qual o período de duração e de que qual maneira os dados serão tratados, assim os dados não ficariam esquecidos com o tempo e o titular consegue ter um autocontrole de seus dados também. Os dados fornecidos pelo titular podem ser revogados a partir do momento em que o mesmo não concorde com as alterações feitas durante o período de tratamentos destes dados, e não somente se houver uma alteração, o titular pode revogar uma concessão cedida anteriormente. Para o professor Marcio Pestana este princípio ´´*um dos princípios cardeais da LGPD no tocante ao tratamento é que os titulares dos dados tenham a garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento*``. Mesmo os dados estando em poder do controlador, o titular deve ter o acesso até ele facilmente.

3.7 – Princípio da qualidade dos dados

O princípio da qualidade dos dados está no inciso V, do Artigo 6° da Lei 13.709 de 2018: “V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento”

Aqui fica claro que os dados apresentados pelo titular dos dados necessitam ser de qualidade, os dados devem ser verídicos e atualizados. O

controlador dos dados deve fazer uma verificação de correção para que não ocorra nenhum equívoco nos procedimentos e operações realizadas. É necessário também a atualização constante dos dados apresentados não apenas em atualização de uso de dados de forma unilateral, para que não seja necessário apagar dados coletados equivocadamente. Para o professor Marcio Pestana ´´*consubstancia-se na garantia, assegurada aos titulares dos dados, de exatidão, clareza, relevância, e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade*``. Assim os dados devem ser corretos para caso ocorra alguma coisa conseguir resolver facilmente.

Em caso de erro na coleta destes dados deve ser corrigido os eventuais erros de maneira imediata, salvo em casos que não é possível a correção destes. Dados equivocados podem ser prejudicial para ambas as partes, tanto para quem coleta tanto para quem fornece os dados, em um ato de cobrança geralmente quem cobra é quem coleta os dados, se forem coletados equivocadamente a cobrança não terá efeito pois os dados não estão em conformidade com os dados corretos.

3.8 – Princípio da transparência

O princípio da transparência dos dados está no inciso VI, do Artigo 6° da Lei 13.709 de 2018: “VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”.

Este princípio, impõe como o próprio nome diz uma transparência no tratamento de dados, todos os dados que forem coletados devem estar explícito na hora da coleta dos mesmos, as finalidades para a qual eles irão se destinar e o fácil acesso a estes dados e informações claras. Para o professor Marcio Pestana ´´ *aos titulares dos dados deve ser garantido e assegurado informações claras, precisas e facilmente acessíveis sobre a realização do tratamento*``. Este princípio deixa claro que não pode ser usado para funções diversas das quais estão exposta no contrato, basicamente está em paralelo com o princípio do livre acesso e da finalidade.

Aqui impõe-se um limite que fica claro conforme o estudo deste presente artigo, de que os dados coletados não devem ser compartilhados com terceiros sem o mediante consentimento do titular destes dados.

3.9 – Princípio da segurança

O princípio da segurança dos dados está no inciso VII, do Artigo 6° da Lei 13.709 de 2018: “segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão”

O princípio da segurança estabelece a quem faz o tratamento desses dados que tenha responsabilidades pelos procedimentos adotados na coleta dos dados. A segurança na coleta é primordial para evitar situações desconfortáveis como perda, invasão ou situações acidentais futuras que envolva os dados coleados, a quebra dessa segurança pode levar a sanções a esta empresa que faz o tratamento. A partir do momento que ocorre uma quebra de segurança e terceiros que não estejam autorizados a ter acesso a estes consigam obter acesso, deve ser informado imediatamente para as autoridades responsáveis tomarem as medida necessárias para evitar que essa situação piore, quanto mais rápido for a reação, menos tempo quem obteve o acesso irregular a estes dados terá para obter vantagem indevida. Para o professor Marcio Pestana ´´ *no tratamento deverão utilizar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão*``. Fica evidente que este princípio visa a proteção dos dados sem que pessoas não autorizadas possam chegar até eles.

Percebe-se que a lei foca muito na questão de segurança, pelo simples fato que para o tratamento dos dados acontecer de maneira correta, a segurança é de suma importância, forma de evitar o acesso por terceiros de maneira equivocada.

3.10 – Princípio da prevenção

O princípio da prevenção dos dados está no inciso VIII, do Artigo 6° da Lei 13.709 de 2018: “prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”

O princípio em questão, ele tende a montar um esquema para prevenir futuras quebras de sigilos em relação a coleta de dados feitas, não deve correr atrás do prejuízo após o vazamentos dos dados, precisa ter uma forma para evitar, prevenir, a segurança dos dados devem ter três estágios, que são a prevenção, durante o tratamento e posteriormente caso tenha ocorrido a quebra de segurança para evitar uma propagação destas informações de uma maneira rápida demais por conta de que nos dias atuais a internet com um clique as informações são repassadas de fora ultra veloz. Para o professor Marcio Pestana ´´*no processo de tratamento, sejam adotados as medidas de necessárias para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais*``. Este princípio já está um passo à frente da proteção, aqui é um meio para prevenir, técnicas para prevenção, por exemplo evitar que funcionários de uma empresa tenha o acesso.

3.11 – Princípio da não discriminação

O princípio da não discriminação dos dados está no inciso IX, do Artigo 6° da Lei 13.709 de 2018: “não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”

O princípio em questão não deve ser utilizado para discriminação contra o seu titular, como no tratamento de dados pessoais sensíveis, que possuem informações como, orientação sexual, origem racial ou étnica, opção política e religiosa entre outros meios de identificação que possa geral um desconforto emocional para os donos destes. Para o professor Marcio Pestana ´´*a impossibilidade de admitir a prática do ilícito, evidentemente, é intrínseca à ordem jurídica, e a LGPD não discrepa de tal valor ínsito ao direito*``. A coleta de dados pessoais sensíveis podem gerar uma discriminação, por exemplo a orientação sexual da pessoa natural, esse é um meio de identificação e podem gerar desconforto.

Também deve-se levar em conta que não deve deixar de ser realizada a coleta de um determinado dado pessoal pelo simples fato de os dados do titular não for de acordo com as convicções de quem faz a coleta, dessa forma não incorrerá na discriminação dos dados pessoais sensíveis, sendo assim a coleta de dados é lícita e não ilícita.

3.12 – Princípio da responsabilização

O princípio da responsabilização dos dados está no inciso X, do Artigo 6° da Lei 13.709 de 2018:

> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

O princípio da responsabilização prevê que todas as medidas tomadas pelo controlador dos dados seja feito um relatório para ficar demonstrado todos os passos que foram tomados no tratamento desses dados para ficar claro se as medidas que foram adotadas para o tratamento foi eficaz, se não houve nada que possa vir a prejudicar alguém no futuro.

Este princípio faz com que o controlador tenha uma responsabilidade na hora do tratamento, caso pense em fazer alguma coisa errada ele saiba que por este princípio ele irá sofrer algum tipo de sanção, então é uma forma de já se precaver se algum controlador querer usufruir dos dados de uma determinada pessoa. Para o professor Marcio Pestana ´´ *Trata-se da demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas*``. Esse princípio deixa claro que o controlador possui responsabilização, caso os dados vazem ele será responsabilizado, seja de forma direta ou indireta.

9 – CONCLUSÃO

Com o referido artigo, podemos concluir que a LGPD vem forte para garantir a segurança dos dados pessoais das pessoas naturais, os meios para esta proteção são baseados por meio dos princípios aplicáveis ao tratamento dos dados e diante a proteção. A regra é clara, porém muitos precisam conhecer esta lei, o desconhecimento pode causar prejuízos para ambas as partes. Os titulares desses dados conhecendo essa lei, garantem a proteção e assim saibam como agir para evitar que os dados cheguem as pessoas errados.

Além de obter os conhecimentos sobre lei, ainda falta muito para entrar em conformidade diante desse novo cenário de proteção de dados pessoais, tanto para quem coleta tanto para quem fornece os dados.

Esta lei desde que tudo esteja dentro da conformidade, tem tudo para ser benéfico, é uma lei que está presente para dar segurança a quem quer que seja, desde que possuam dados pessoais. A tecnologia está presente em todos os lugares do planeta, com um clique a informação chega ao outro lado do mundo, sendo assim a conclusão é que normas que estão presentes são fundamentais para o presente.

BIBLIOGRAFIA

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014**. Disponível em: . Acesso em: 2 de novembro 2020.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento.** Brasil: Editora Forense, 2019.

CAVALCANTI, Natália Peppi; SANTOS, Luiza Mendonça da Silva Belo. **A Lei Geral de Proteção de Dados do Brasil na era do Big Data**. In Tecnologia Jurídica & Direito Digital - II Congresso Internacional de Direito, Governo e Tecnologia. 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Revista do Tribunais, 2020.

LIMA, Cíntia Rosa Pereira. **Comentarios a Lei Geral de Proteção de Dados - Lei N. 13.709/2018, com Alteração da Lei N. 13.853/2019.** Brasil: Almedina Brasil, 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

MOTA, Fabricio da. **"Proteção de dados pessoais é a evolução da privacidade"**. Disponível em: https://www.serpro.gov.br/lgpd/noticias/protecao-dados-evolucao-privacidade. Acesso em: 09 nov. 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários a Lei n. 13.709/2018 (LGPD).** São Paulo: Saraiva educação, 2018.

SELEME, Mariana Pigatto. **Lei geral de proteção de dados - Por que precisamos dela?** Disponível em: https://migalhas.uol.com.br/depeso/305072/lei-geral-de-protecao-de-dados---por-que-precisamos-dela. Acesso em: 06 nov. 2020.

SILVA, Felipe. Gestão de Identidades e Acessos.In CABRAL, Carlos; CAPRINO, Willian (org.). **Trilhas em Segurança da Informação, Caminhos e Ideias para a Proteção de Dados**. Rio de Janeiro: Brasport, 2015.

PESTANA, Marcio. **Os princípios no tratamento de dados na Lei Geral de proteção de Dados Pessoais.** Consulto Jurídico. Maio, 2020. Disponível em: https://www.conjur.com.br/2020-mai-25/marcio-pestana-principios-tratamento-dados-lgpd. Acesso em: 07/09/2021

TOMASEVICIUS, Eduardo. **O princípio da boa-fé na Lei Geral de Proteção de Dados.** Consultor Jurídico. Março, 2020. Disponível em: https://www.conjur.com.br/2020-mar-09/direito-civil-atual-principio-boa-fe-lgpd#author. Acesso em: 07/09/2021