

**CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE**

CURSO DE DIREITO

**ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS ACERCA DAS RELAÇÕES
TRABALHISTAS**

Victor Spera de Lucca

Presidente Prudente/SP
2020

**CENTRO UNIVERSITÁRIO
ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE**

CURSO DE DIREITO

**ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS ACERCA DAS RELAÇÕES
TRABALHISTAS**

Victor Spera de Lucca

Monografia apresentada como requisito parcial de conclusão do curso e obtenção do grau de Bacharel em Direito, sob a orientação do Prof. Lucas Pires Maciel.

Presidente Prudente/SP
2020

ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS ACERCA DAS RELAÇÕES TRABALHISTAS

Monografia apresentada como requisito parcial para obtenção do grau de Bacharel em Direito.

Lucas Pires Maciel - Orientador

Rafael Aragos - Examinador 1

Wilton Boigues Corbalan Tebar - Examinador 2

Presidente Prudente, 24 de novembro de 2020.

Agir, eis a inteligência verdadeira. Serei o que quiser. Mas tenho que querer o que for. O êxito está em ter êxito, e não em ter condições de êxito. Condições de palácio tem qualquer terra larga, mas onde estará o palácio se não o fizerem ali?

Fernando Pessoa

Dedico este trabalho aos meus pais,
que sempre foram minha base
e fizeram o possível
para que realizasse este sonho.

AGRADECIMENTOS

Agradeço primeiramente a Deus que esteve sempre ao meu lado iluminando cada uma das minhas decisões e me ajudando a tornar-me mais forte a cada dificuldade enfrentada.

Agradeço aos meus pais, Wagner e Jaci que além de me proporcionarem a possibilidade de concluir mais um sonho, o fizeram através de todo amor, carinho, cumplicidade e cuidado para que, como sempre, eu tivesse o melhor possível. Serei eternamente grato a eles por nunca deixarem agir para que minhas vontades fossem feitas e, principalmente, por me apoiarem em todas elas.

Agradeço também a minha família, que sempre esteve ao meu lado e me apoiou durante toda a caminhada do curso, se preocupando e oferecendo toda a ajuda possível.

Agradeço aos meus verdadeiros amigos que sempre estiveram ao meu lado me aconselhando, principalmente diante de um ano tão difícil que foi 2020 para mim e sempre buscaram me levantar, para que eu nunca desistisse e estiveram ao meu lado presenciando cada vitória e cada progresso na minha vida.

Agradeço, ainda, todo o corpo docente do curso de direito da Toledo Prudente Centro Universitário, em especial ao meu orientador, Lucas Pires Maciel, que entendeu durante esse ano toda a dificuldade que passei e, diante dessa situação, tornou-se também um amigo. Sou muito grato por toda atenção, disposição e preocupação que teve comigo, não poderia ter escolhido um orientador melhor.

Enfim, serei eternamente grato a todos que passaram na minha vida durante esse período, que me ensinaram, que estiveram ao meu lado e que principalmente colaboraram para que eu me tornasse quem sou hoje.

RESUMO: A presente monografia tem por objetivo analisar a Lei Geral de Proteção de Dados. Com o intuito de auferir tal objetivo, será retratada a história da Lei Geral de Proteção de Dados no Brasil, bem como o que levou à necessidade de sua criação, suas características, princípios, estrutura, além das sanções previstas para aqueles que descumprirem suas determinações. Tal estudo será revelado através do método dedutivo pautado no raciocínio lógico visando explicar a reação que a criação dessa lei gerará no ordenamento jurídico brasileiro tendo como foco principal explicar seu impacto nas relações trabalhistas. Dessa forma, ficará claro todo o caminho percorrido para que essa lei viesse a ter vigência no país. Sua criação tem impacto direto na estruturação das empresas no que diz respeito ao armazenamento dos dados de seus clientes. Tal impacto corresponde principalmente à questão da proteção e privacidade dos usuários, que a cada dia cresce frente ao ambiente tecnológico, principalmente durante a pandemia. Essas questões ligadas à privacidade estendem-se também aos empregados, ex-empregados e candidatos das companhias, os quais precisam fornecer informações para que seu empregador possa preencha diversas determinações legais. Ocorre que informações íntimas do empregado como por exemplo, opinião política, dados de saúde, opção sexual, entre outras, devem ser mantidas em sigilo, uma vez que não há interesse vinculado ao trabalho quanto a essas informações.

Palavras-chave: Aplicação. Lei Geral de Proteção de Dados. LGPD. Relações Trabalhistas.

ABSTRACT: This article aims to analyze the General Data Protection Law and explain its impact on labor relations. In order to achieve this goal, the history of the General Data Protection Law in Brazil will be portrayed, as well as what led to the need of its creation, its characteristics, principles, structure, other than the sanctions provided for those who fail to comply its determinations. The creation of this law has a direct impact on the structuring of companies regarding the storage of their customers' data. This impact corresponds mainly to the issue of the protection and privacy of users. Such issue is also extended to employees, former employees and candidates of the companies, who are required to provide information for their employer to fill in various legal requirements. Intimate information of the employee, such as political opinion, health data, sexual orientation, among others, must be kept confidential, since there is no interest linked to the job regarding this information.

Keywords: Application. General Data Protection Law. LGPD. Labor relations.

SUMÁRIO

1	INTRODUÇÃO	9
2	A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL	10
2.1	A Lei Geral de Proteção de Dados em Conformidade com a Constituição Federal de 1988	15
3	ANÁLISE DOS PRINCÍPIOS GERAIS DO DIREITO E SUA APLICAÇÃO NA LEI GERAL DE PROTEÇÃO DE DADOS	17
4	PANORAMA ATUAL DA LEI GERAL DE PROTEÇÃO DE DADOS	21
4.1	Os Primeiros Julgados a Partir da Vigência da LGPD	25
5	A PANDEMIA DO CORONA VÍRUS E A LEI GERAL DE PROTEÇÃO DE DADOS	28
6	A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS ORGÃO RESPONSÁVEL PELA FISCALIZAÇÃO DA APLICAÇÃO DA LGPD	32
7	O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS RELAÇÕES TRABALHISTAS	35
7.1	O Impacto da LGPD nas Relações de Trabalho a Distância	41
7.2	O Fim do Contrato de Trabalho e o Armazenamento de Dados	44
8	CONCLUSÃO	45
	REFERÊNCIAS	48

1 INTRODUÇÃO

É nítido o crescimento diário ao acesso à tecnologia e *internet* em todo o mundo. Por se tratar de um mecanismo mais rápido, de fácil acesso e operacionalidade simplificada, há cada vez mais a busca por essa opção, o que gera uma série de preocupações tais como a segurança e a privacidade dos indivíduos que optam por essa ferramenta.

O crescimento em busca de tecnologia e acesso à *internet*, aumentou significativamente durante o período de pandemia no ano de 2020. Muitas empresas tiveram de recorrer a vendas *on-line* para que pudessem se manter em funcionamento.

Apesar de esse crescimento exponencial durante esse período, sempre foi uma prática corriqueira das empresas, *sites*, grupos na *internet*, requisitar dados de seus usuários para que possam acessar determinada página ou ferramenta.

O maior problema nessa questão é a segurança dos dados de cada usuário, a maneira como são armazenadas suas informações e o risco que isso pode gerar à privacidade de cada indivíduo. Um pequeno deslize de uma empresa com os dados de um usuário pode causar danos irreversíveis a sua imagem, por exemplo.

Com o intuito de fiscalizar a maneira como as organizações lidam com os dados pessoais de seus usuários e trazer maior segurança à proteção desses, o Brasil optou pela criação da Lei nº 13.709/2018 que dispõe sobre a proteção de dados pessoais no país. Sua premissa é a proteção do cidadão por intermédio da proteção de seus dados naturais.

Através do método dedutivo será explicado como a referida lei será aplicada no ordenamento jurídico brasileiro. Sua aplicação irá abranger pessoas físicas e pessoas jurídicas que de um modo ou de outro lidam com o armazenamento de dados pessoais de terceiros, acarretando impactos em diversas esferas do direito como por exemplo contratos, responsabilidade dos empresários, relações trabalhistas, entre outros.

2 A LEI GERAL DE PROTEÇÃO DE DADOS NO BRASIL

A Lei Geral de Proteção de Dados surgiu no Brasil com a medida provisória 869/18 com o escopo de garantir segurança e privacidade virtual frente aos dados pessoais dos usuários de empresas públicas ou privadas.

Além da proteção da privacidade dos usuários, explica (DC, 2020, s.p.):

A LGPD proíbe o uso de forma indiscriminada dos dados pessoais informados por cadastros, garantindo aos usuários o direito de saber como e por que será feito o tratamento de seus dados, além de ser necessário obter o consentimento do proprietário das informações antes da utilização. Assim, os cidadãos poderão solicitar às empresas que informem se possuem seus dados armazenados, bem como, exigir a exclusão deles.

Visando efetivar essa proteção, além da lei, criou-se também a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela fiscalização o qual tem sua composição e competências estruturadas na própria LGPD.

Quanto a questão, pontifica (OLIVIERI, 2019, s.p.):

A LGPD não se destina, precipuamente, às relações de trabalho, mas sim às relações jurídicas em geral que envolvem qualquer manuseio de dados, ou informações, entre as pessoas naturais detentoras desses dados, e pessoas naturais ou jurídicas que de alguma forma têm ou obtêm acesso a esses dados. Seu campo de aplicação, por excelência, são as relações de consumo, ou comerciais, do universo virtual, desde aplicativos, redes sociais, a grandes Bancos comerciais. Seu objetivo principal é a proteção da privacidade dos indivíduos num mundo em que a informação circula em altíssima velocidade, muitas vezes sem controle e com consequências indesejadas para o titular das informações; um mundo em que, com um toque na tela do smartphone, toda a vida de uma pessoa pode ser exposta, denegrada, ou usada para finalidades que o titular daquelas informações ignora ou não deseja.

Como citado, a LGPD visa a proteção dos dados pessoais, e a própria lei, em seu artigo 5º, traz um rol esclarecendo o que entende por esses dados:

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

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

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;
III - 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;
IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

A própria LGPD, como se pode constatar, traz em seu texto uma breve explicação do que trata cada um dos dados que devem ser mantidos em sigilo, tais como os dados pessoais; sensíveis e anonimizados. Porém, por tratarem do foco principal da lei, é necessário que sejam explicados de uma forma mais aprofundada.

O legislador estabelece, no artigo 5º, a necessidade da proteção de dados dos usuários que os fornecem. Esses dados se revelam de três maneiras: dados pessoais; dados sensíveis e dados anonimizados.

Os dados pessoais são informações que podem ser obtidas de uma pessoa viva, identificada ou identificável, ou os dados que podem levar a identificar determinada pessoa.

Pessoa identificável segundo, (OLIVEIRA, 2019, s.p.):

é aquela que pode ser identificada, direta ou indiretamente, por referência a um identificador como um nome, número de identificação, dados de localização, identificador *on-line* ou a mais fatores específicos da física, fisiologia, identidade genética, mental, econômica, cultural ou social da pessoa.

Já no que se refere aos dados pessoais sensíveis, este dispõe-se de informações que, se expostas, poderiam causar uma discriminação ao detentor da mesma, ou seja, são informações que possuem um grande poder lesivo, de caráter subjetivo, como, por exemplo, orientação sexual; orientação religiosa; dados referentes a saúde, entre outros. Entende OLIVEIRA, (2018, n.p):” Um dado sensível é aquele que não só possui informações que você não gostaria que fossem compartilhadas, como também que pode causar um alto risco de exposição tanto na sua vida social quanto profissional”.

Pontifica ainda (BARAKAT, 2020, s.p.):

Dados são informações, estatísticas, características ou atributos de algo ou alguém, cuja interpretação, conforme a liberdade do analista, suporta determinada conclusão ou apenas registra um acontecimento. Nos termos da Lei Geral de Proteção de Dados (Lei 13.709/2018), ainda que não em vigor, quando um dado, por si só, permite identificar uma pessoa natural ou facilita uma posterior identificação, este será um dado pessoal. Ressalta-se que, nesta era da informação, dados pessoais são valiosos, na medida em que agregam assertividade a qualquer tipo de algoritmo.

Portanto, é indispensável para a LGPD que estes dados sejam armazenados e assim mantidos, podendo ser compartilhados apenas com expresso consentimento de seu titular.

Quanto aos dados anonimizados, esses pertencem a um titular que não pode ser identificado (OLIVIERI, 2019, s.p) esclarece o que seriam esses dados: “o dado anonimizado, que é aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa.”

Para o *site*, um dado anonimizado não estará sujeito à legislação da LGPD, porém, para que isso ocorra, não pode ser possível que se identifique o titular desses dados de maneira alguma.

Caso seja possível reconstruir um caminho para descoberta do titular desse dado, ele deixará de ser anonimizado e passará a ser um dado pseudonimizado.

Sobre o tema ensina (OLIVIERI, 2019, s.p):

Vale frisar que um dado só é considerado efetivamente anonimizado se não permitir que, via meios técnicos e outros, se reconstrua o caminho para "descobrir" quem era a pessoa titular do dado - se de alguma forma a identificação ocorrer, então ele não é, de fato, um dado anonimizado e sim, apenas, um dado pseudonimizado e estará, então, sujeito à LGPD.

Fica clara a preocupação do Brasil com relação aos dados pessoais, tal qual culminou na criação de uma legislação específica para que seja protegido este valioso bem jurídico.

Buscando garantir uma efetiva proteção, a lei estabelece limites para o que é legal ou ilegal na utilização dos dados. E, para tanto, o consentimento do usuário para o uso de seus dados deve ser inequívoco, sendo de responsabilidade da empresa o uso de dados pessoais sem a devida concordância.

No que diz respeito ao que seria o consentimento para a LGPD, leciona (SILVERIO, 2020, s.p.):

consentimento é tudo aquilo que o indivíduo autorize a empresa a usar os seus dados pessoais para alguma finalidade. Tendo como exemplo, um cliente compra algo pela *internet* e envia todos os seus dados e no formulário, declarou que tem interesse em receber *e-mails* promocionais, ofertas da empresa, etc. No entanto, quando pede a solicitação do consentimento ao usuário, vem da seguinte maneira: "Gostaria de receber *e-mails* promocionais da empresa" ou "Li e estou de acordo com os termos de uso e privacidade". Assim, recomenda-se que a coleta de dados sempre se dá ao consentimento da pessoa.

A autora indica ainda outros dois importantes fatores para que haja um consentimento efetivo por parte do usuário, o legítimo interesse e o contrato.

Quanto ao legítimo interesse entende (SILVERIO, 2020, s.p.):

permite o uso dos dados, sem precisar, necessariamente, do consentimento. Em outras palavras, o legítimo interesse afirma que está considerando e protegendo o interesse tanto do cliente quanto da empresa. Com isso, é preciso fazer um teste de proporcionalidade, na qual faz uma análise e vê os interesses de ambas partes.

Já ao que se refere ao contrato, explica (SILVERIO, 2020, s.p) "Ele ocorre em relação ao tratamento de dados, onde se dá a pedido do titular dos dados para garantir a execução de um contrato e também, serve para a validação e início de vigência de tal acordo".

Percebe-se que o consentimento para que haja o tratamento dos dados do usuário é mais complexo do que parece ser, visando que seja efetiva a proteção, a segurança e a intimidade de cada usuário.

Isso significa dizer que o usuário terá o direito de autorizar ou negar a utilização de seus dados serão, para o que poderão ser disponibilizados, quem poderá ter acesso a eles ou até mesmo como serão expostos.

O Brasil não foi o primeiro país a adotar uma legislação específica no tocante à proteção de dados pessoais dos indivíduos. O pioneiro a tratar do assunto foi a União Europeia, que já possui em seu ordenamento jurídico uma lei nesse sentido, a *General Data Protection Regulation* (GDPR).

O surgimento dessa lei, em 2018, gerou impactos imediatos em países como o Brasil, que precisou aplicar as regras dessa lei por ser um parceiro comercial da União Europeia e, eventualmente, trabalhar com a coleta de dados do país. Ou

seja, para que haja a transferência de dados entre as sociedades europeias com outros países, estes devem observar as diretrizes da norma (GDPR), sob pena de sofrerem medidas corretivas ou até mesmo pecuniárias.

Embora a lei 13.709/2018 tenha sido criada em 2018, esta somente teve sua vigência decretada em setembro de 2020. Isso significa dizer que, a partir desta data, as empresas deverão aderir às regras da legislação e, além de alterar a forma como tratam os dados pessoais, deverão, ainda, alterar sua estruturação, uma vez que a lei disciplinou a necessidade da criação de novos cargos para aqueles que tratarão do modo como os dados pessoais serão movimentados.

Frente a sua vigência, caberá às empresas desmistificar a ideia de que a LGPD veio para trazer ainda mais burocracia para o cenário empresarial do país. A lei surgiu com o escopo de assegurar maior privacidade aos usuários, o que é garantido constitucionalmente a todo cidadão, fazendo com que haja uma maior confiança do usuário com o agente controlador de dados.

Com essa ideia, elucida (SILVERIO, 2020, s.p.):

A internet nos dias de hoje não é mais a mesma, pois muitas pessoas não conseguem mais controlar seus dados e deixar de uma forma mais protegida. Por esse motivo, a LGPD faz com que isso se torne ao contrário, para que os indivíduos de má-fé não consigam utilizar as informações de outras pessoas. Dessa forma, a LGPD ajuda as empresas melhorarem sobre como controlar a gestão de dados, pois faz com que tomem mais cuidados e sempre agindo de acordo com as normas.

Assim sendo, a vigência da LGPD no país tem muito a agregar no ordenamento jurídico, tanto do Brasil quanto de qualquer outro país que venha a adotar uma lei que proteja os dados dos usuários, haja vista que este vem se tornando um bem jurídico mais valioso a cada dia.

A tendência é de que essa estatística só aumente e que sua proteção seja cada vez mais cobrada pelos usuários, ao passo que estes começarão a entender o valor que o mero fornecimento de um número de telefone, para fazer um cadastro virtual, possui.

2.1 A Lei Geral de Proteção de Dados em Conformidade com a Constituição Federal de 1988

Percebe-se que o ordenamento jurídico brasileiro, ao tratar da Lei 13.709/2018, tem como foco principal, além de proteger os dados pessoais, assegurar a segurança e a privacidade do indivíduo.

Atualmente ao fazer uma simples compra na *internet*, por exemplo, inúmeros dados pessoais e particulares são exigidos, trazendo um inerente risco à vida das pessoas.

A partir disso, é nítido que a LGPD deve estar de acordo com princípios gerais do ordenamento jurídico e, ainda, encontrar uma base constitucional.

A Carta Magna de 1988, em seu artigo 5º, inciso X, assegura a proteção à intimidade do indivíduo:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Do mesmo modo que a Constituição Federal assegura o direito à privacidade, a atual Lei Geral de Proteção de Dados acaba por firmar ainda mais sua importância no artigo 2º da referida lei, trazendo como destaque em seu inciso I o respeito à privacidade.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I – o respeito à privacidade;
II – a autodeterminação informativa;
III – a liberdade de expressão, de informação, de comunicação e de opinião;
IV – a inviolabilidade da intimidade, da honra e da imagem;
V – o desenvolvimento econômico e tecnológico e a inovação;
VI – a livre iniciativa, a livre concorrência e a defesa do consumidor;
VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais

Como entende (TEIXEIRA, 2020, s.p.):

Assim, a proteção da privacidade, nos termos da LGPD, tem como escopo garantir ao titular dos dados o controle sobre o acesso de terceiros à sua vida privada, razão pela qual a legislação versa sobre as condições e hipóteses de tratamento dos dados pessoais.

A redação do artigo 1º da Lei Geral de Proteção de Dados traz os objetivos da lei e, além da privacidade, busca proteger a liberdade e o livre desenvolvimento da personalidade da pessoa natural.

O direito à liberdade é amplamente tratado na Constituição Federal de 1988 em seu artigo 5º em diversos incisos.

Dentre esses incisos, dois deles possuem ligação com o que preceitua a LGPD, sendo eles os incisos IX e X da Carta Magna.

O inciso IX garante a liberdade de atividade intelectual, artística, científica e de comunicação, conforme cita em sua redação: IX – [...] “é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença”.

Já o inciso X trata de direitos invioláveis, dentre eles a intimidade, a vida privada, a honra e a imagem das pessoas.

O legislador, ao criar a LGPD, embasou-se em diversos preceitos fundamentais garantidos pela Constituição Federal e buscou dar ainda mais força a esses dispositivos, como citado anteriormente pelo artigo 2º desta lei.

A liberdade, a intimidade, a vida privada, a imagem e a honra das pessoas estão diretamente ligadas ao meio tecnológico que cada indivíduo usa para se manifestar. Por essa manifestação ser livre, sua proteção é indispensável uma vez que são inúmeros os casos em que indivíduos se excedem nesse meio e acabam causando danos à imagem de outrem, ensejando em crimes como injúria, difamação, racismo, dentre outros.

Em vista do exposto, percebe-se que há uma ligação direta entre a legislação pátria e a LGPD, uma vez que esta, ao encontrar embasamento na Carta Magna, enfatizou a necessidade da proteção de direitos indispensáveis para o desenvolvimento da personalidade humana.

3 ANÁLISE DOS PRINCÍPIOS GERAIS DO DIREITO E SUA APLICAÇÃO NA LEI GERAL DE PROTEÇÃO DE DADOS

O ordenamento jurídico brasileiro está calcado na ideia de princípios e regras, tópicos que no ponto de vista jurídico apresentam diferenças quanto a suas classificações.

Explica ÁVILA (2005, p.70):

princípios são normas imediatamente finalísticas, primariamente prospectivas e com pretensão de complementariedade e de parcialidade, para cuja aplicação se demanda uma avaliação da correlação entre o estado de coisas a ser promovido e os efeitos decorrentes da conduta havida como necessária à sua promoção.

Com a ideia de princípios tratarem de normas finalísticas, para Ávila, essa ideia de “fim”, estabelece um estado ideal de coisas a ser atingido, como forma geral para enquadrar os vários conteúdos de um fim.

Portanto, por seu entendimento, o fim tem como determinação encontrar um meio, entendido como uma condição (uma situação ou conduta) que traz o conteúdo do fim, como, por exemplo, princípio da boa-fé que exige uma conduta pautada na lealdade para que se atinja o objetivo do princípio.

Desse modo, há de se pontuar que, para um princípio ser efetivamente positivado, condutas deverão ser praticadas com o escopo de garantir a sua eficácia na sociedade.

No que se refere à eficácia dos princípios, esta pode ser garantida internamente de forma direta ou indireta.

Sobre a questão, manifesta ÁVILA (2005, p.78): “A eficácia direta traduz-se na atuação sem intermediação ou interposição de um outro subprincípio ou regra”.

Assim, fica claro que a eficácia direta é aquela que garante a aplicação de um princípio sem que este necessite estar amparado por um outro subprincípio ou regra, como é o caso, por exemplo, do princípio do devido processo legal, que não necessita de outras regras no ordenamento que o resguardem para que seja garantida sua aplicabilidade em um caso concreto.

Com relação à eficácia indireta, esta se revela de forma contrária à eficácia direta. Por ela, vemos que o princípio “traduz-se na atuação com

intermediação ou interposição de um outro subprincípio ou regra”, conforme ensina ÁVILA. (2005, p.78).

No tocante às regras, segundo entende ÁVILA (2005, p.78)

[...] são normas imediatamente descritivas, primariamente retrospectivas e com pretensão de decidibilidade e abrangência, para cuja aplicação se exige a avaliação da correspondência, sempre centrada na finalidade que lhes dá suporte ou nos princípios que lhes são axiologicamente sobrejacentes, entre a construção conceitual da descrição normativa e a construção conceitual dos fatos.

Com isso, ÁVILA (2005. p.78) pontifica: “os princípios são normas importantes para a compreensão do sentido das regras”.

Uma regra, portanto, poderá ser interpretada da forma mais correta caso esteja em acordo com um princípio que lhe é sobrejacente.

Destaca-se, então, a importância dos princípios para o ordenamento jurídico e para as leis que o revestem.

Para tanto, a Lei Geral de Proteção de Dados, buscando dar maior eficácia aos seus efeitos, institui em seu artigo 6º princípios que a revestem e que dependerão da prática de condutas pela sociedade para que esta não venha a sofrer punições em caso de inobservância desses princípios e das regras trazidas por essa norma.

São 10 os princípios elencados textualmente pela LGPD, tais quais:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Embora o próprio artigo 6º traga em seus incisos uma breve explicação do que preceitua cada um desses princípios, é importante fazer outras observações quanto a cada um deles.

O princípio da finalidade busca estabelecer que cada dado informado seja utilizado para uma finalidade específica, ou seja, aquela para a qual o usuário forneceu a informação. É possível citar como exemplo uma situação em que o usuário fornece seu *e-mail* para realizar o cadastro em uma plataforma para efetuar seu *log-in*. Nesse caso, a finalidade é apenas efetuar o *log-in*.

Caso a empresa venha a enviar *e-mails* com promoções para o *e-mail* desse usuário, estará extrapolando os limites da finalidade para qual o fornecimento do *e-mail* se limitava.

O princípio da adequação está ligado também com o da finalidade. Para este princípio, as informações prestadas pelo usuário devem estar em conformidade com a finalidade informada pela empresa. Caso não seja compatível, o tratamento será inadequado.

Quanto ao princípio da necessidade, este busca a restrição dos dados informados, ou seja, que seja informado apenas aquilo que é conveniente para sua finalidade específica.

Já o princípio do livre acesso visa assegurar ao usuário a possibilidade de consultar a qualquer hora os dados que determinada empresa possui sobre si, além da alternativa de saber o modo como a empresa está tratando suas informações.

No que se refere aos princípios da qualidade dos dados e da transparência, estes garantem ao usuário que as informações que determinada empresa detém sobre ele sejam atualizadas e verdadeiras, além de assegurar que a empresa não forneça esses dados para outras empresas sem que o usuário saiba. Ou seja, caso a empresa forneça dados para terceiros, será imprescindível que o

usuário tenha conhecimento e que tenha consentido a transferência dessa informação para determinada finalidade.

Tem-se o princípio da segurança como o principal foco deste trabalho, uma vez que esse princípio determina a necessidade de as empresas garantirem a segurança dos dados de seus usuários, sejam eles empregados ou clientes.

Será de responsabilidade das empresas buscarem métodos que propiciem a efetiva segurança de seus usuários ao ataque de hackers, por exemplo e, ainda, buscar medidas que certifiquem a não ocorrência de situações acidentais, como, por exemplo, a perda de algum arquivo do usuário.

O princípio da prevenção está ligado com a ideia da segurança, uma vez que determina a necessidade de as empresas agirem de forma antecedente quanto a proteção dos usuários, ou seja, devem agir antes que sobrevenha algum problema.

No tocante ao princípio da não discriminação, este veda a possibilidade de as empresas utilizarem os dados de determinado usuário para discrimina-lo. Aqui, há de se falar em dados sensíveis, como por exemplo opção sexual, religião, origem racial, dentre outros.

Para finalizar, o princípio da responsabilização e prestação de contas institui que as empresas, além de adotarem medidas assecuratórias e cumprirem a lei, deverão constituir provas de que agiram de boa-fé e que realmente adotaram tais medidas.

Frente à explicação dos princípios, não há como negar a necessidade da conformidade desses com a LGPD e o ordenamento jurídico. Tais princípios norteiam o modo como as empresas deverão tratar seus usuários sob a possibilidade de sofrerem penalidades em caso de descumprimentos dos mesmos.

Há que se destacar ainda que o princípio da finalidade, topografado como o primeiro princípio do artigo 6º, da LGPD, é o princípio que orienta os demais, uma vez que todos os outros, de certo modo, englobam a finalidade específica da lei.

4 PANORAMA ATUAL DA LEI GERAL DE PROTEÇÃO DE DADOS

Resta nítido que a lei geral de proteção de dados tem como intenção assegurar o tratamento dos dados sensíveis dos usuários frente a exposição desses dados diariamente e a possibilidade de crimes cibernéticos.

Diante esse cenário, expõe (REBELLO, 2019, s.p.):

A LGPD é resultado de um movimento espontâneo da sociedade e autoridades brasileiras. Desde o início da década, empresas e usuários vêm buscando respostas para as questões de segurança virtual, que ganham relevância em função da escalada do cibercrime. Em 2018, segundo um estudo da McAfee publicado na revista *Veja*, o Brasil registrou perdas progressivas com crimes virtuais, chegando a R\$ 10 bilhões por ano. Somos uma das “potências” mundiais nesse quesito, ao lado de Índia, Vietnã, Rússia e Coreia do Norte. Assim sendo, a LGPD surge do esforço conjunto de diversas instâncias no sentido de combater as fraudes e crimes *on-line* que, com o tempo, crescem vertiginosamente no Brasil. É por isso que a lei é considerada um avanço, até mesmo por se aplicar em todo o território nacional.

Portanto, pelo fato de o Brasil encaixar-se como uma potência frente ao uso da tecnologia e visando ainda adequar-se as legislações de parceiros negociais como a União Europeia, o legislador brasileiro optou pela criação da LGPD.

A lei foi sancionada em 14 de agosto de 2018, tendo uma forte relação com o “marco civil da *internet*” que surgiu em 2014. Porém, para elevar a proteção e segurança dos usuários, optou-se pela criação da LGPD.

Por ter sido sancionada em 2018, acreditava-se que entraria em vigor no mês de agosto de 2020, o que não ocorreu.

Devido à complexidade de adequar-se a esta legislação, foi concebido um prazo de *vacatio legis* para que as empresas entendessem as diretrizes e o tratamento da norma.

Ocorre que, no ano de 2020, todo o mundo foi acometido pela pandemia do COVID-19.

Por causa das medidas de proteção que deveriam ser tomadas para diminuir a proliferação do vírus, a grande maioria das empresas fecharam suas portas, precisaram dispensar funcionários, dando início a outras preocupações, sendo necessário um prazo maior para que se adequassem às diretrizes da LGPD.

Importante destacar que, com a pandemia, o modo de vida das pessoas mudou e grande parte delas passou a procurar a *internet* de forma mais recorrente, seja para lazer, diversão, compras, trabalho, entre outros.

Ocorre que, para fazer uso de qualquer dessas ferramentas, é necessário o fornecimento de dados, o que ensejou um crescimento exponencial da quantidade de dados que as empresas vêm obtendo nesse cenário.

Conforme essas observações, destaca (FREITAS, 2020, s.p.):

Nessa mesma linha de transformação, as empresas dos diversos portes e setores promoveram, da noite para o dia, verdadeira mudança de procedimentos com adoção da tecnologia digital, possibilitando que os colaboradores desenvolvessem suas atividades de forma remota e, muitas vezes, sem a correta adequação de processos para garantia da segurança e inviolabilidade de propriedades industriais e segurança da informação. Por outro lado, a intensificação do uso da *internet* possibilitou a coleta de dados com intensa facilidade, tornado estas informações em bens imateriais de elevado valor e fundamental importância estratégica para diversos órgãos públicos e empresas das mais variadas modalidades. Considerando isto, as atividades empresariais estão sendo repensadas e reorganizadas para o efetivo desenvolvimento de uma sólida 'cultura da segurança da informação'.

Assim sendo, cabe a cada indivíduo entender e compreender o valor de seus dados sensíveis, visto que que a banalização desses dados poderá ensejar situações desagradáveis para o usuário. Desse modo, é de extrema importância, principalmente nesse período de adaptação, que sejam escolhidas empresas que realmente se importam e já estão se adequando às diretrizes da nova norma para que a segurança dos dados se dê de maneira eficaz, atingindo seu objetivo.

Pontua (FREITAS, 2020, s.p.):

Referida cultura deverá ser de fundamental importância para superação do atual estado de calamidade pública, respaldando a grande preocupação com a privacidade de dados pessoais decorrente da maciça coleta, tratamento e manipulação de dados sensíveis e ligados à saúde. Isso pode gerar um efeito discriminatório intenso aos portadores de vírus, demandando, portanto, critérios efetivos e diferenciados contra incidentes de vazamentos desses dados pessoais.

Dessarte, foi aprovado o projeto de lei 1.179/20, visando o adiamento da LGPD por conta dos danos causados pela COVID-19. Além de as empresas estarem despreparadas no momento para se adequar à LGPD, o próprio órgão fiscalizador (ANPD) ainda não estava completo, o que acabaria por prejudicar ainda mais as empresas, pois não teriam onde se embasar, criando uma insegurança jurídica.

Diante esse cenário, explica (AZEREDO, 2020, s.p):

A entrada em vigor da LGPD será um marco no desenvolvimento na cultura de proteção de dados pessoais, e exigirá enorme dedicação dos controladores de dados, titulares, autoridades de fiscalização, entre outros, motivo pelo qual a entrada em vigor da lei, sem que lhe seja dado o foco necessário, pode causar efeito deletério no desenvolvimento dessa cultura. Para os detratores do adiamento, a LGPD é fundamental neste momento de pandemia para auxiliar o poder público a mapear os casos e proteger os dados pessoais e privacidade das pessoas diante do uso de tecnologias como geolocalização e reconhecimento facial. A ausência de regulamentação detalhada sobre a proteção de dados aumenta o risco de abusos, mas esse risco é mitigado diante da existência de dispositivos legais no Código Civil, Código de Defesa do Consumidor, Marco Civil da *Internet* e Constituição Federal, que tratam da proteção da intimidade e vida privada dos indivíduos. Nesse contexto, o adiamento infelizmente é medida necessária neste momento em que a prioridade das diferentes partes interessadas deve ser a saúde pública e contenção do coronavírus e, uma vez superada a crise, dar o foco necessário à LGPD.

Desse modo, teve-se de abrir mão da adequação a LGPD pelas empresas em prol da saúde pública, situação compreensível no momento em que vivemos. Verifica-se, porém, que mesmo diante do cenário atual, o Presidente da República, Jair Bolsonaro, sancionou no dia 17/09/2020 a Lei Geral de Proteção de Dados (Planalto, 2020, *on-line*).

No que diz respeito às sanções previstas na lei, estas seguem a redação originária da mesma, devendo ser aplicadas somente a partir de agosto de 2021, o que não exime as empresas de responsabilidade, haja vista que diversas obrigações já estão em vigência.

Com relação a esse ponto, explica (MEIRA, 2020, s.p):

Além disso, as empresas que não estiverem *compliance* com a lei e não tratarem adequadamente os dados, estão sujeitas a sério risco reputacional, que pode ser ainda mais prejudicial do que as próprias sanções. Ainda, importante que todo e qualquer produto e serviço seja pensado, criado e lançado no mercado com a privacidade resguardada, incorporada às novas tecnologias

Direcionado por essa ideia, fica claro que as empresas que se adequarem a LGPD o quanto antes sairão ganhando, podendo, inclusive, usar dessa premissa como uma forma de marketing para sua empresa, uma vez que a busca do usuário é a efetiva proteção de seus dados.

Como exemplo de adequação de empresas à LGPD de forma diligente no Brasil, podemos citar grandes empresas como o *Facebook*, *WhatsApp* e *Instagram*. Com o advento da nova lei, tais empresas emitiram e enviaram comunicados para seus usuários explicando como seus dados seriam tratados, quais dados seriam usados e para o que seriam utilizados. Um dos avisos emitidos pelo *Facebook* (2020, *on-line*), por exemplo, contém em seu texto a seguinte mensagem: “As leis sobre dados pessoais estão mudando no Brasil, e queremos facilitar para você a visualização de algumas das suas configurações.” e complementa:

Se você escolher adicionar ao seu perfil do Facebook sua religião, preferência política ou seu interesse em homens ou mulheres, queremos ter certeza de que você sabe que esses são dados considerados sensíveis pela LGPD. Se decidir manter essas informações no seu perfil, nós as compartilharemos com quem você escolher e usaremos esses dados para personalizar recursos e produtos.

Já o *Whatsapp*, notificou:

Este Aviso de Privacidade – Brasil (“Aviso”) se aplica às atividades de tratamento de dados pessoais sob a legislação brasileira e complementa nossa Política de Privacidade.

De acordo com a Lei Geral de Proteção de Dados (“LGPD”) do Brasil, você tem o direito de acessar, corrigir, portar, eliminar seus dados, além de confirmar que tratamos seus dados. Saiba mais sobre seus direitos e como você pode exercê-los acessando nossos artigos de ajuda para iPhone, Android e KaiOS. Em determinadas circunstâncias, você também tem o direito de se opor e restringir o tratamento de seus dados pessoais. Nossa Política de Privacidade fornece informações sobre como compartilhamos seus dados com terceiros. Para solicitar mais informações sobre nossas práticas de dados, clique aqui.

O *WhatsApp* Inc. é o controlador de dados responsável por suas informações. Para entrar em contato com o Encarregado de Proteção de Dados do *WhatsApp* clique aqui. Você também tem o direito de enviar um requerimento à Autoridade Nacional de Proteção de Dados (“ANPD”) entrando em contato diretamente com a ANPD.

Fica claro por parte das empresas a preocupação em adotar as diretrizes da norma e, ainda, abrir vista para o usuário escolher quais dados sensíveis deseja ou não exibir em sua página, como orienta a LGPD.

4.1 Os Primeiros Julgados a Partir da Vigência da LGPD

Pelo fato de a lei já estar em vigência, iniciam-se as demandas processuais baseadas na LGPD. A primeira sentença proferida com base nessa lei ocorreu no dia 22 de setembro de 2020 na 5ª Vara Cível de Brasília.

O caso retrata um *site* que estaria comercializando dados sem a devida observância das diretrizes da LGPD. Dentre esses dados estavam presentes nomes, idade, *e-mails*, cidades, etc.

Aproveitando a entrada da LGPD em vigor, o MP promoveu uma ação alegando que o *site* estaria violando a privacidade dos usuários, uma vez que estes não haviam permitido previamente o tratamento desses dados de tal maneira.

Ocorre que o juiz julgou extinta a ação sem resolução do mérito pois antes do julgamento dos pedidos do MP o *site* que comercializa os dados encontrava-se em manutenção e para o juiz, essa manutenção se deu cautelarmente pelo site para que se adequasse a LGPD uma vez que esta estava em vigência há pouco tempo.

Na sentença aduz o juiz (Migalhas, 2020, s.p):

A presente ação não merece prosperar. Com efeito, para que haja viabilidade jurídica da pretensão deduzida em Juízo, é preciso que a demanda atenda às condições da ação, estas consubstanciadas no interesse processual e na legitimidade das partes. No caso dos autos, não se vislumbra a presença do interesse processual, que tem viés jurídico-processual e se deslinda pela concomitância da necessidade e utilidade do processo e na adequação da via eleita. Isso porque, através de consulta realizada, nesta data, à rede mundial de computadores, este Juízo constatou que o sítio intitulado "lembrete digital", com o domínio lojainfortexto.com.br, está em manutenção (documento em anexo). Esse fato, provavelmente, decorre da circunstância de que, com o recente início de vigência da Lei 13.709/18, ocorrido em 18/09/2020 (sexta-feira passada), os responsáveis pelo sobredito sítio devem estar buscando adequar os seus serviços às normas jurídicas de proteção de dados pessoais.

Neste contexto, impõe-se reconhecer, ao menos neste momento, a ausência de interesse processual do autor para agir através desta ação civil pública. É que, em virtude da manutenção realizada no sítio intitulado "lembrete digital", com o domínio lojainfortexto.com.br, não restou evidenciada nenhuma lesão ou ameaça de lesão apta a justificar a pretensão de tutela inibitória deduzida na inicial, com o que a presente ação se torna inútil.

Perante a decisão do magistrado, rebate o Ministério Público "o simples ato de ter colocado o *site* em manutenção não afasta a utilidade do processo".

Conforme ainda entende o MP, é possível que o *site* tenha entrado em manutenção antes do processo, o que não afastaria sua utilidade, uma vez que

embora estivesse em manutenção ainda deteriam as informações de seus usuários, podendo vir a comercializar de forma indevida novamente. Poderá o MP recorrer da decisão para que seja reavaliado o caso.

Outro recente caso (processo 1080233-94.2019.8.26.0100) que ocorreu em São Paulo, (Migalhas, 2020, *on-line*), envolvendo a LGPD, decorreu da venda de um imóvel por parte de uma empresa que veio a compartilhar os dados do comprador com empresas alheias à relação jurídica.

O compartilhamento desses dados gerou danos de natureza extrapatrimonial ao comprador que ajuizou a ação, visando uma indenização por danos morais. A juíza sentenciou o caso baseando-se na LGPD e no CDC, que estariam em consonância.

Para a juíza (Migalhas, 2020, s.p):

Não há dúvida que a relação entre as partes é de natureza consumerista como restou assentado na decisão de fls. 627/630 de sorte que um dos direitos fundamentais do consumidor é de acesso à informação adequada acerca dos serviços que lhes são postos à disposição. Especificamente sobre o assunto referente ao tratamento de dados, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados LGPD) prescreve que são fundamentos da disciplina da proteção de dados, dentre outros, o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade e a dignidade (art. 2º).

Explica também que “nesse contexto que os dados surgem como bens jurídicos tutelados pela ordem jurídica, porquanto relacionados a diversos outros direitos também fundamentais, conforme o supracitado art. 2º da LGPD.”

Impõe, ainda:

Patente que os dados independentemente de sensíveis ou pessoais (art. 5º, I e II, LGPD) foram tratados em violação aos fundamentos de sua proteção (art. 2º, LGPD) e à finalidade específica, explícita e informada ao seu titular (art. 6º, I, LGPD). O contrato firmado entre as partes prescreveu apenas a possibilidade de inclusão de dados do requerente para fins de inserção em banco de dados (“Cadastro Positivo”), sem que tenha sido efetivamente informado acerca da utilização dos dados para outros fins que não os relativos à relação jurídica firmada entre as partes. Entretanto, consoante prova documental acima indicada, houve a utilização para finalidade diversa e sem que o autor tivesse informação adequada (art. 6º, II, LGPD). Nesse mesmo sentido tuitivo, o disposto no artigo 6º, III e IV, do Código de Defesa do Consumidor. Isto posto, a responsabilidade da ré é objetiva (arts. 14, caput, CDC e 45, LGPD). Inexiste suporte para a exclusão de responsabilidade (art. 14, § 3º, I a III, CDC), de sorte que caracterizado o ato ilícito relativo a violação a direitos de personalidade do autor, especialmente

por permitir e tolerar (conduta omissiva) ou mesmo promover (conduta comissiva) o acesso indevido a dados pessoais do requerente por terceiros.

Em sua sua fundamentação, entendeu a juíza que a empresa deve pagar um valor correspondente a R\$ 10.000,00 a título de danos morais sofridos pelo comprador pelo vazamento de seus dados sem a devida autorização, conforme dispõe a LGPD.

Em poucos dias de vigência, as ações envolvendo a LGPD começaram a surgir. Tal situação demonstra o despreparo e a falta de interesse de muitas empresas em se adequar às diretrizes da lei.

Mesmo que não vigentes as penas de multas até o momento, constatou-se que aquele que violar as normas da LGPD durante esse período, não se eximirá de responsabilidade, arcando com os danos causados ao usuário que teve seus dados divulgados.

Frente ao caso em questão, interpreta (SILVERIO, 2020, s.p.):

Vale evidenciar também, um ponto ocorrido neste caso, é que a parte ré alegou em sua fala que está devidamente enquadrada aos parâmetros que a LGPD traz. Em contraponto, é de extrema relevância que o que a Juíza diz, no sentido de que não é suficiente que a empresa se adeque à LGPD, mas que também mantenha a postura correta diante à proteção e tratamento de dados. Desta forma, é importante que as empresas tenham esse pensamento e esse posicionamento diante o tratamento de dados. Para que evitem de se enganar, que apenas implementando a proteção de dados, já é o suficiente para não sofrer com as fiscalizações e possíveis problemas. Contudo, as empresas devem além de tratar os dados recebidos, devem também mantê-los protegidos

Demonstra-se a partir da situação narrada que todo o sistema brasileiro que lida com o tratamento de dados terá um trabalho pela frente para que consiga se enquadrar adequadamente ao que preceitua a LGPD e, ainda, manter os dados de seus usuários em sigilo.

5 A PANDEMIA DO CORONA VÍRUS E A LEI GERAL DE PROTEÇÃO DE DADOS

Como anteriormente exposto, a pandemia alterou o modo de viver de toda a sociedade e a *internet* que já era comum na vida dos indivíduos, passou a ser ainda mais.

Devido ao impacto da pandemia as empresas precisaram se adequar ao cenário atual, aumentando suas produções, alterando sua organização para que passassem a vender cada vez mais pela *internet*.

Embora seja um meio eficaz, a *internet* envolve o principal objeto da LGPD: a proteção dos dados sensíveis. O compartilhamento de dados dos usuários com as empresas aumentou consideravelmente durante esse período, ensejando um risco ao usuário que até então não podia gozar da LGPD por esta não estar em vigor.

Durante esse período ainda se discutia se a LGPD entraria em vigor durante o ano de 2020, até que, no dia 17/09/2020, o presidente da república a sancionou.

Porém, enquanto não se tomava uma decisão, milhares de dados foram compartilhados, inclusive dados de órgãos públicos, que também tiveram que se adequar à nova realidade para que pudessem exercer seu trabalho, como por exemplo as audiências *on-line*, cartórios funcionando de forma eletrônica, dentre outros.

Ocorre que essa mudança ocorreu de forma tão repentina que não houve tempo para que as pessoas se preocupassem com a efetiva proteção dos dados e segurança de suas informações.

Sobre a questão, afirma (FREITAS, 2020, s.p):

a intensificação do uso da *internet* possibilitou a coleta de dados com intensa facilidade, tornado estas informações em bens imateriais de elevado valor e fundamental importância estratégica para diversos órgãos públicos e empresas das mais variadas modalidades. Considerando isto, as atividades empresariais estão sendo repensadas e reorganizadas para o efetivo desenvolvimento de uma sólida 'cultura da segurança da informação.

Ou seja, a partir da vigência da nova legislação, as empresas terão um grande caminho a ser percorrido para que possam garantir proteção aos dados de

seus usuários por conta da quantidade de dados que veem sendo e ainda serão arrecadados nesse período.

Importante destacar nessa questão, que além dos dados adquiridos pelas empresas privadas, seja por meio de compras na *internet*, cadastro em *sites*, entre outros, as empresas públicas também passaram a obter cada vez mais dados das pessoas por conta da pandemia.

Podemos citar, por exemplo, o conhecimento do Estado sobre a quantidade de casos de infectados nas cidades, estados e municípios, quantidade de mortes pela COVID-19, entre outros. Esses são dados que, se não forem tratados da forma correta, poderão indicar quem são seus titulares.

Muito embora a divulgação desses dados seja em prol da população, com o escopo de atualizar a todos sobre a situação caótica em que vivemos, não se pode deixar de lado a proteção de dados, que envolve a privacidade e a liberdade individual de cada um.

Destaque-se, nesse sentido, uma situação em que se chega de algum modo a uma pessoa infectada pela COVID-19 pela divulgação desses dados, o impacto para essa pessoa pode ser extremamente negativo, podendo sofrer represálias, sem ao menos ter culpa por essa condição.

Com relação à questão, pontua (DONEDA, 2020, s.p.):

Em primeiro lugar, a própria existência de um marco normativo em proteção de dados torna o processo de tratamento de dados em situações emergenciais mais seguro e caracterizado por maior segurança jurídica. Estando a proteção de dados vocacionada à proteção o cidadão, a sua disciplina compreende dispositivos capazes de legitimar a utilização de seus dados pessoais em situações nas quais o seu interesse ou o da sociedade é prioritário, como ocorre em situação como a que estamos passando. Assim, com a legislação de proteção de dados, ao proporcionar base legal e legitimidade para que dados pessoais sejam usados neste contexto, os controladores e demais responsáveis passam a ter segurança jurídica para que os forneçam e tratem para esta finalidade.

Portanto, se houvesse uma legislação específica tratando da questão, antes mesmo da pandemia, seria plausível que o tratamento de dados e as informações sobre a pandemia andassem juntos, de forma segura e respeitando a privacidade de cada indivíduo.

Esclarece (DONEDA, 2020, s.p.):

A LGPD possui, portanto, instrumentos capazes de cuidar das demandas advindas da emergência por qual passamos em um quadro de manutenção de direitos e garantias individuais e coletivas e, além disso, será um elemento fundamental para a reestruturação que advirá após a crise. É imprescindível e urgente que contemos com ela o quanto antes, assim como com a Autoridade Nacional de Proteção de Dados para a exemplo de seus pares no mundo, proporcionar liderança, definir parâmetros e organizar o debate, a exemplo das demais autoridades nacionais.

Sobre a questão, entende (BARAKAT, 2020, s.p):

O que merece cuidado, todavia, é a correta avaliação das características dos dados divulgados. Há dados pessoais na base ofertada à comunidade? Provavelmente sim. E com o adiamento da vigência da LGPD formalizada pela MP 959/2020, não temos ainda um instrumento normativo dotado de força suficiente para impor aos agentes de tratamento de dados a observância de padrões de conduta quando das atividades de tratamento.

Complementa, ainda (DONEDA, 2020, s.p):

A legislação de proteção de dados oferece dois elementos fundamentais para o debate atual: o primeiro, já mencionado, é que, ao contrário das normas tradicionais de confidencialidade e sigilo, a normativa de proteção de dados convive bastante bem com regimes complexos de autorizações e limitações específicas para uso de dados conforme os atributos presentes, como a sua finalidade e, desta forma, é capaz de proporcionar legitimidade e segurança jurídica para a utilização de dados pessoais no combate ao vírus – favorecendo, inclusive, o uso destes dados para tal fim.

Atualmente a LGPD já se encontra em vigência, mas não se tem muito *feedback* de como vêm agindo os agentes de tratamento de dados nos dias de hoje. É uma situação que deverá ser acompanhada no dia a dia das empresas.

Há de se ponderar que a pandemia não será para sempre, porém, os dados que foram coletados durante a mesma deverão ser tratados de alguma forma, preferencialmente excluindo-os, uma vez que foram adquiridos por conta de uma situação excepcional.

Pontua (DONEDA, 2020, s.p):

a uma situação que surgirá após o vírus: diversos tratamentos de dados pessoais no combate ao vírus não de ser pontuais e somente se justificam neste contexto. A ideia de um legado de vigilância e hipertrofia do uso de dados pessoais para outras finalidades, cessada a emergência, há de ser combatida com vigor e, hoje, um marco regulatório e uma cultura estabelecida

de proteção de dados são o maior remédio de que uma sociedade possa dispor para evitar o risco da consolidação de um estado de “vigilância crônica”.

Resta claro, portanto, que a pandemia deixará diversas marcas no que diz respeito ao tratamento de dados, ficando a ANPD e as empresas públicas/privadas responsáveis para sanar esse legado.

6 A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS ORGÃO RESPONSÁVEL PELA FISCALIZAÇÃO DA APLICAÇÃO DA LGPD

Mediante a criação da LGPD é de suma importância que haja uma fiscalização da atuação das empresas no que diz respeito às atitudes que estas estão tomando para tratarem os dados sensíveis de seus usuários. Para tanto, criou-se a “ANPD” – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, órgão que ficará responsável pela fiscalização, orientação e penalização das empresas.

A própria LGPD em seu artigo 5º, inciso XIX traz a figura da ANPD, [...]“órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional”.

Ainda, em seu artigo 55-A, §1º explica a natureza jurídica: [...] “A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República”.

Embora seja um órgão novo, a própria LGPD em seu texto trata das competências da ANPD, sendo elas:

Art. 55-J. Compete à ANPD:

- I - zelar pela proteção dos dados pessoais, nos termos da legislação;
- II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
- III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
- VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
- VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
- VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
- IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional
- X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;
- XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico

sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;

XII - elaborar relatórios de gestão anuais acerca de suas atividades;

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

Com relação à competência da ANPD, o que mais se discute é o disposto no inciso IV do artigo 52, que trata da aplicação de sanções em desfavor das empresas que descumprirem as diretrizes da LGPD.

Vale frisar que, embora tenha esse poder sancionatório, deverá orientar às empresas para que estas estejam em conformidade com a legislação, afim de não sofrerem com as multas.

Como orienta a lei em seu artigo 52, as multas poderão chegar no valor de até R\$ 50.000.000,00 de reais, tendo como base o faturamento da pessoa jurídica

de direito privado. Salienda em seu §1º que essa multa não será imposta de uma hora para outra contra a empresa.

Como a própria lei diz, as empresas terão o direito de se defender antes da aplicação da multa:

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios.

Desse modo, caberá às empresas e a ANPD trabalharem juntas para que a LGPD alcance um “sucesso” na legislação brasileira, por meio da adoção da lei por cada empresa, seja ela pública ou privada.

A lei ainda complementa trazendo a composição deste órgão.

Art. 55-C. A ANPD é composta de:

- I - Conselho Diretor, órgão máximo de direção;
- II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade;
- III - Corregedoria;
- IV - Ouvidoria;
- V - órgão de assessoramento jurídico próprio; e
- VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

Diante essa questão, há um empecilho por conta da pandemia, conforme traz o *site* (VERDÉLIO, 2020, s.p):

Há um descompasso, entretanto, já que a nomeação do Conselho Diretor e do diretor-presidente, órgão máximo de direção da ANPD, deve passar pela aprovação do Senado Federal. Mas as atividades das comissões permanentes da Casa estão suspensas em razão da pandemia de covid-19.

Portanto, a ocupação de cada cargo se dará mediante o avanço da situação no país e a necessidade de ocupação desses cargos, uma vez que a lei já se encontra em vigor.

7 O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS NAS RELAÇÕES TRABALHISTAS

Como citado anteriormente, o Brasil inspirou-se na GDPR para criação da LGPD.

Diferentemente do Brasil, a GDPR disciplina em seu texto a aplicação desta lei nas relações de trabalho. A falta dessa previsão causa uma certa insegurança aos empregadores, pois é incerto o tratamento que deverão dar aos dados de seus empregados, devendo agir da forma mais cautelosa possível para evitar uma multa milionária.

Embora a legislação brasileira de proteção de dados seja omissa no que diz respeito às relações de trabalho, ao analisarmos os artigos 1º e 5º, inciso X da LGPD, podemos constatar que esta terá aplicação nas relações de trabalho.

Dispõe o artigo 1º (PLANALTO, 2020, s.p):

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

Já o artigo 5º, inciso X, (PLANALTO, 2020, s.p) expõe:

[...] 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;

As relações de trabalho no Brasil são garantidas pela Consolidação das Lei dos Trabalho (CLT).

Em seus artigos 2º e 3º, a CLT traz uma breve definição dos sujeitos que compõe uma relação trabalhista, sendo eles empregado e empregador.

Para a CLT, “empregador é considerado a empresa, individual ou coletiva, que, assumindo os riscos da atividade econômica, admite, assalaria e dirige a prestação pessoal de serviço”.

Já o empregado seria “toda pessoa física que prestar serviços de natureza não eventual a empregador, sob a dependência deste e mediante salário”.

Quando se analisam ambas legislações conjuntamente, constata-se que o empregador se encaixa como um agente controlador dos dados de seus empregados, candidatos a vagas de emprego e ex funcionários, uma vez que desenvolve diversas das ações previstas no inciso X, que possui um rol exemplificativo.

Já esses funcionários, candidatos e ex-empregados são denominados como titulares dos dados os quais devem ser tratados para destinação específica que os justifica.

Na grande maioria das vezes, a relação empregatícia é regida por um contrato de trabalho firmado entre as partes que, diante da vigência da LGPD, pode ser considerado um “fluxo de dados”.

De acordo com esse contrato, o empregado acaba por fornecer dados dos quais é titular, para que o empregador possa cumprir com diversas determinações legais, como por exemplo registrar o empregado. Ocorre que, além desses dados, determinadas empresas exigem também dados sensíveis, como por exemplo a crença religiosa do indivíduo. Tal informação não tem relação alguma com a finalidade que se busca no contrato de emprego, portanto, é de extrema importância que as empresas comecem a se policiar quanto à quantidade de dados exigidas aos seus empregados.

Quanto a esse ponto, expõe (OLIVIERI, 2019, s.p):

Há um intenso fluxo de “Dados Pessoais”, tal qual definido na LGPD, envolvendo o contrato de trabalho, diretamente entre o Empregado-Titular e o Empregador-Controlador/Operador, desde (a) as fases anteriores à sua celebração (informações sobre o candidato, currículo, histórico, etc.), passando (b) pela celebração do contrato de trabalho (dados cadastrais, filiação a sindicato, endereço, nomes dos genitores, escolaridade, situação familiar, nomes dos filhos, idade, tipo sanguíneo etc.), e ainda (c) durante a execução do contrato de trabalho (jornada de trabalho, valor do salário, descontos, faltas, motivos das faltas, doenças, acidentes, situações conjugais que podem ter reflexos em providências da empresa, como o pagamento de pensão, inclusão de um dependente no plano de saúde, etc.), e por fim (d) ao término do contrato de trabalho (motivo do desligamento, valor das verbas rescisórias, etc.).

Explica ainda (OLIVIERI, 2019, s.p):

A Lei Geral de Proteção de Dados Pessoais (LGPD) é uma norma de caráter geral e amplo, destinada a todas as relações jurídicas que envolvam a presença dos requisitos por ela indicados - a saber: todas as relações

jurídicas que permeiem a manipulação de informações de pessoas físicas (artigo 1º).

Assim, a LGPD não foi projetada especificamente para as peculiaridades do trâmite de informações entre patrão e empregado. Ela foi projetada para a vida virtual em geral, para o trânsito de informações dos cidadãos nas redes sociais, aplicativos, cadastros de clientes.

Quanto ao que foi apontado, (TORRES e CALCINI, 2020, s.p) ilustram:

considerando que o empregado é o titular dos dados e que o empregador é o controlador, porquanto realiza o manuseio dos dados (tratamento) fornecidos pelo obreiro por força do contrato individual de trabalho, a LGPD é aplicável às relações laborais, devendo o empregador observar as regras sobre proteção de dados pessoais de seus empregados e adotar as medidas de segurança, técnicas e administrativas para a proteção dos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, conforme previsão do caput do art. 46. Com isso, destaca-se a previsão do art. 46, que obriga a observância das medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais desde a fase de concepção do produto ou do serviço até a sua execução. Em uma interpretação extensiva (trata-se de norma de proteção), vale dizer que o empregador deve fazer uso do tratamento adequado das informações pessoais contidas nos dados de inscrição (fase pré-contratual), dados inseridos no contrato de trabalho (fase contratual) e no Termo de Rescisão de Contrato de Trabalho (fase pós-contratual).

Pode-se ponderar, no que diz respeito ao envolvimento do empregador com os dados do empregado, que o controlador destes deverá seguir o que pretendeu o legislador ao escrever a nova lei: proteger e armazenar os dados de forma a assegurar a privacidade de seus funcionários.

Outro dispositivo que deixa clara a aplicação da LGPD nas relações de trabalho é o artigo 3º:

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:

[...] II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional

Portanto, se um contrato de trabalho for firmado em território nacional, deverá respeitar as diretrizes da LGPD, devendo o empregador armazenar e proteger

os dados de seus funcionários sob pena de sofrer multa de até 2% do faturamento da empresa, conforme preceitua o artigo 52 desta lei.

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

Desse modo, a partir do momento em que o empregador, pessoa física ou jurídica, consolida um contrato com o empregado e passa a ter acesso aos seus dados sensíveis, deverá observar os termos da LGPD quando for transmitir esses dados a um terceiro, seja um órgão público, seja outro empregador que venha a ter interesse nesses dados, pois, com o advento da nova lei os dados pessoais deverão ser operados com finalidades específicas que demonstrem sua necessidade.

Importante ressaltar que, durante o período em que a LGPD não esteve em vigor e também durante o período em que suas sanções administrativas não estejam em vigência, os empregadores ainda assim possuem responsabilidade pelos dados de seus empregados à luz do Código Civil em seus artigos 186 e 927.

Ou seja, em caso de violações aos direitos de um empregado por conta de um dano causado a ele decorrente de vazamento de seus dados, a empresa será responsabilizada pelos danos materiais ou morais causados a este empregado.

Quanto a necessidade de adaptação dos empregadores, expõe (OLIVIERI, 2019, s.p)

O que era antes somente uma “ficha de registro” do empregado, passa a ser, à luz da LGPD, um conjunto de dados pessoais, alguns deles, inclusive, dados pessoais sensíveis cujo tratamento, nos termos da lei, não observa necessariamente a mesma rotina que aqueles dados pessoais não sensíveis.

Em vista disso, o empregador terá, em um mesmo documento, dados com categorias diversas, ensejando em diferentes consequências frente a LGPD.

Conforme explicado, a lei estava em seu período de *vacatio legis*. Ocorre que no dia 17/09/2020, o presidente da república sancionou a Lei Geral de Dados, que passou a surtir efeitos.

Esses efeitos estão ligados à necessidade da proteção dos dados sensíveis encaixando nesse meio as relações trabalhistas.

As empresas deverão adequar-se as diretrizes da nova lei para que não sofram as sanções administrativas impostas pela ANPD, que serão aplicadas a partir de agosto de 2021.

Essa adequação deverá ocorrer sem muita demora, havendo um destaque nas empresas que vierem a se adequar às diretrizes da nova lei de forma contenciosa.

Para que isso ocorra, as empresas deverão alertar seu departamento de recursos humanos, para proteger os dados de seus clientes e funcionários.

Sobre a questão, esclarece (GRECO, 2020 s.p):

Dada a complexidade do Direito do Trabalho e sua evolução, a utilização de dados pessoais do empregado pelo empregador, definidos como “sensíveis”, demandará dos Departamentos de Recursos Humanos das empresas a realização de verdadeiro inventário das informações pessoais dos empregados, dado o alto poder lesivo de eventual tratamento irregular.

A implementação de gestão dos dados sensíveis pelo RH, com possibilidade de limitação ao acesso e o correto descarte, será medida urgente e necessária.

Isso porque, em todas as fases que compõem as relações laborais, seja na fase de recrutamento e seleção, seja durante a vigência ou após o término do contrato de trabalho, o empregador lida com dados pessoais tidos como sensíveis.

Como parte do processo de adequação, as empresas devem revisar esse fluxo de dados pessoais sensíveis e, mais do que isso, estabelecer controles dos níveis de acesso às informações, para a garantia da segurança e da privacidade dos seus titulares, nos termos do que dispõe a LGPD.

Essa necessidade de limitação ao acesso dos dados de seus empregados é o principal objetivo da nova lei, ao passo que terá o empregado o direito de saber como seus dados estão sendo tratados, por quanto tempo ficarão armazenados e com quem serão compartilhados.

Explica ainda (GRECO, 2020, s.p):

No âmbito das relações regidas pela Consolidação das Leis do Trabalho, a LGPD demandará que o empregador informe ao empregado sobre o modo como trata seus dados, por quanto tempo os guarda e com quem os compartilha, já que o tratamento dos dados pessoais deve observar os princípios da licitude, lealdade e transparência.

Relativamente ao tratamento lícito, o titular dos dados pessoais sensíveis deve emitir seu consentimento para uma ou mais finalidades, quando for aplicável, a depender da finalidade.

A necessidade dessa adequação ressalta o intuito do legislador frente a criação da LGPD, qual seja, a vontade de tratar os dados sensíveis dos empregados como uma máxima proteção frente a realidade que vivemos, em que a exposição dos indivíduos na sociedade está sendo cada vez mais recorrente.

Com relação ao tratamento desses dados, impõe (GRECO, 2020, s.p):

A nova Lei imporá às empresas que os procedimentos envolvendo os dados pessoais dos empregados devam ser desenvolvidos de forma a garantir tratamento seguro, a privacidade dos titulares e mecanismos de tratamento adequado às especificidades do empreendimento.

Portanto, para que haja uma efetiva proteção e a garantia de um tratamento seguro, caberá às empresas escolherem a melhor forma de proteção, seja através de uma empresa especializada, seja pela contratação de um funcionário responsável por toda questão de tratamento dos dados dentro da mesma.

Para isso, poderão ser adotadas boas práticas de governança dentro da própria empresa, conforme ilustra (GRECO, 2020, s.p):

Recomenda-se que sejam criadas regras de boas práticas e de governança, que estabeleçam procedimentos, normas de segurança e ações educativas para a mitigação de riscos, além de uma política de privacidade acessível e que descreva todos os processos relacionados a dados sensíveis dos empregados.

Assim sendo, deverá cada empresa, baseada em sua realidade, escolher a melhor maneira para lidar com os dados de seus funcionários, devendo reavaliar os contratos de trabalho já vigentes, além de alertar os funcionários sobre a necessidade de seu consentimento para a publicação ou divisão de seus dados. Além disso, é preciso informá-los do direito que lhes cabe de saberem como e para que finalidade seus dados serão manejados. E, em caso de desvio de finalidade, deverá haver um novo consentimento do empregado, titular dos dados.

7.1 O Impacto da LGPD nas Relações de Trabalho a Distância

Com o advento da reforma trabalhista em 2017, o legislador previu na nova legislação trabalhista a possibilidade do empregado em domicílio e do *teletrabalho*.

Em seu artigo 83, (PLANALTO, 2020, sp.) a CLT entende: “ É devido o salário mínimo ao trabalhador em domicílio, considerado este como o executado na habitação do empregado ou em oficina de família, por conta de empregador que o remunere”.

Para MARTINS (2018, p. 241) empregado em domicílio:

É o trabalho que uma pessoa, designada como trabalhador em domicílio, realiza em seu domicílio ou em outros locais que escolher, mas distintos dos locais de trabalho do empregador, em troca de remuneração, com o fim de produzir um produto ou prestar um serviço, conforme as especificações do empregador, independentemente de quem proporcione os equipamentos, materiais ou outros elementos utilizado.

Complementa MARTINS (2018, p. 241):

O domicílio é o lugar escolhido pelo empregado para a prestação dos serviços ao empregador ou até na casa do intermediário. Poderia ser até o realizado no interior de um presídio. Desde que o trabalho seja desenvolvido fora da fiscalização imediata e direta do empregador, estará caracterizado o trabalho em domicílio.

Portanto, para que seja caracterizado o trabalho em domicílio, basta que o empregado execute seu serviço fora das dependências de seu empregador mediante remuneração. O trabalho em domicílio difere do trabalho autônomo, uma vez que o trabalhador autônomo não goza de subordinação.

No que diz respeito ao *teletrabalho*, a CLT em seu artigo 75-B (PlanaltoGov, *on-line*) considera *teletrabalho* “[...] a prestação de serviços preponderantemente fora das dependências do empregador, com a utilização de tecnologias de informação e de comunicação que, por sua natureza, não se constituam como trabalho externo.”

Expõe MARTINS (2018, p. 245):

Teletrabalho é o trabalho a distância com uso de tecnologia e de recursos eletrônicos. O trabalho não é realizado na sede da empresa. É feito a distância, que é o elemento espacial. É fundamental a utilização de meios telemáticos.

Não será teletrabalho o enviado ao empregador por meios de comunicação comuns, como telefone, correios.

Complementa o autor (2018, p. 246):

É chamado o teletrabalho de trabalho periférico, a distância, remoto. O computador é um instrumento do trabalho.

O teletrabalho não se confunde com certos trabalhadores da área de informática, como analistas, programadores, digitadores e operadores, pois é o realizado a distância, fora do ambiente normal de trabalho, que é feito dentro da empresa. O trabalho daquelas pessoas também pode ser realizado fora da empresa, mas não é feito por meio de comunicação eletrônica, mas desenvolvido no tomador de serviços.

Ainda nas palavras de MARTINS (2018, p. 246): “Todo *teletrabalho* é considerado trabalho a distância, mas nem todo trabalho a distancia pode ser considerado *teletrabalho*.”

Mediante o que foi apontado, pode-se ponderar que o *teletrabalho* e o trabalho em domicílio se tornaram tendências na sociedade brasileira, tanto pela praticidade quanto pela economia que isso pode gerar aos empregadores.

Esse cenário tornou-se ainda mais comum diante da pandemia que assola o mundo. Atendendo a necessidade de fechamento das empresas por um período determinado, em função da pandemia e a contenção de pessoas circulando nas ruas, os empregadores viram como única opção para seus empregados e para a continuidade das atividades empresariais o “*home office*” que retrata atualmente uma espécie do *teletrabalho*, o qual seria gênero.

Embora essa seja uma opção, para a LGPD isso pode acarretar problemas para as empresas, uma vez que seus empregados passarão a ter dados, como senhas e outras informações da empresa que antes não faziam parte de seu ambiente de trabalho “natural”.

Nesse caso, se um empregado, no teletrabalho, vazar alguma informação sobre algum cliente, por exemplo, a empresa pode vir a ser responsabilizada, uma vez que como preceitua o ordenamento jurídico, ela é

responsável pelos atos de seus empregados, vindo a responder solidariamente pelos danos causados ao depender do caso concreto.

Conforme explica (FLEURY, 2020, s.p):

Em um primeiro momento, o empregador que desejar ter empregados em teletrabalho deve ficar atento no momento da contratação, pois o teletrabalho pode representar um perigo considerável quanto à segurança dos dados coletados e armazenados pela empresa, uma vez que é um ponto de acesso externo aos dados e sistema do empregador, para produzir o trabalho imposto a esta modalidade. Será preciso que a empresa mapeie e controle rigorosamente os dados pessoais relacionados às suas atividades, tais como senhas e criptografia, em atenção especial aos teletrabalhadores que terão acesso à informações e sistema da empresa fora do seu ambiente, impossibilitando acessos não autorizados por tais trabalhadores e vazamentos dos dados armazenados pelo empregador.

Complementa (GRECO, 2020, s.p):

Há que ser considerando que o trabalho à distância não exime o empregador de ser responsabilizado por conta de fatos que sejam decorrentes da sua falta de vigilância sobre aquilo que está sendo feito ou sentido pelo seu empregado.

Além desse risco, para que seja efetuado, o teletrabalho o empregado deve possuir uma certa qualificação para tanto, ser capacitado para executar o serviço, o que fez com que muitas empresas precisassem demitir diversos empregados durante esse período.

Diante da vigência da LGPD, a contratação ou continuidade de um contrato de um trabalho com um empregado que não demonstra conhecimento na área tecnológica e de dados no teletrabalho, as empresas podem estar sofrendo um grande risco.

Sobre a questão, ensina (MARTINS, 2018, p. 250):

O teletrabalhador deverá ser uma pessoa que tem certa qualificação ou escolaridade, pois precisará ter conhecimentos de certas tecnologias para usar o computador, acessar a *Internet*, etc.

O empregador não terá como saber quem tem efetivamente acesso ao computador utilizado pelo trabalhador. Isso pode representar um problema em relação à segurança de dados.

Desse modo, mesmo mediante poucas opções, o empregador deverá tomar as devidas precauções no que diz respeito à LGPD e o teletrabalho, pois além de uma maior troca de informações e pelo fato de não haver uma grande supervisão,

como ocorreria no ambiente comum de trabalho, essa modalidade de labor também se encontra amparada pela LGPD.

7.2 O Fim do Contrato de Trabalho e o Armazenamento de Dados

O contrato de trabalho e o vínculo empregatício pode se dar por decisão do empregado ou do empregador, podendo advir de justa causa ou não.

Para Martins (2018, p. 581) “A cessação do contrato de trabalho é a terminação do vínculo de emprego, com a extinção das obrigações para os contratantes”.

Como explicado, o candidato a uma vaga de emprego, ou o empregado durante a vigência de seu contrato de trabalho fornecem diversos dados para que possam ser admitidos na empresa, a qual deverá armazená-los e tratá-los de modo que se tornem sigilosos. A falta de cuidado com esses dados poderá ensejar em multa, como já mencionado.

Ocorre que o empregado, ao ser desligado da empresa, acaba por deixar seus dados no banco de dados da mesma, sem se importar com o descarte deles.

Com a vigência da LGPD, é importante que o empregador, ao firmar um contrato de emprego com o empregado, busque coletar a menor quantidade de dados possíveis, para que futuramente não venha a ter problemas com essa questão por conta da LGPD.

Esses dados coletados, quando o empregado deixa a empresa, devem também ser descartados pelo que preceitua a LGPD, uma vez que esses deixam de ter uma finalidade: o contrato de trabalho.

Esse descarte pode se dar por uma determinação legal ou por pedido do trabalhador, uma vez que é titular do direito.

Ocorre que nem sempre esses dados serão descartados no momento em que o empregado é desligado da empresa. Muitos dados, no entanto, devem continuar sendo armazenados, para que o empregador possa cumprir com imposições legais, razão pela qual cada caso deverá ser analisado particularmente.

Desse modo, quanto menos tempo a empresa retiver dados de seus empregados, melhor será, com exceção daqueles que são amparados legalmente para que as empresas os detenham por um período de tempo maior.

8 CONCLUSÃO

Em virtude dos fatos mencionados conclui-se ser indispensável uma lei que reitere a necessidade de proteção frente a privacidade e segurança dos indivíduos nas plataformas *on-line*, uma vez que a privacidade é tida como um direito fundamental assegurado pela Constituição Federal de 1988 e sua violação pode acarretar danos irreversíveis ao usuário.

Além disso, constata-se que leis protegendo os dados estão surgindo a cada dia em novos países, uma vez que existe uma demanda global em relação a esse assunto. Trata-se das relações globais via *Internet*, quando, inclusive, os dados pessoais são compartilhados pelo mundo inteiro rapidamente, sendo necessário estabelecer um padrão mínimo frente à realidade de cada país.

Fica claro, portanto, que a partir da vigência da LGPD um sujeito ao acessar e informar seus dados pessoais à uma plataforma digital, terá uma maior segurança ao fazê-lo, uma vez que ficará a cargo da empresa ou *site* dispor de meios para evitar que esses dados sejam expostos à terceiros. A lei garante, ainda, que os dados sejam utilizados apenas para a finalidade específica a que se destinam, sob pena de a empresa sofrer represália por parte da ANPD, vindo a ter de pagar uma multa por sua conduta e também ressarcir o usuário pelos possíveis danos que este venha a sofrer pela sua exposição.

Sua necessidade revela-se no surgimento de casos práticos logo após sua vigência, o que constata o desinteresse e a falta de cuidado por parte das empresas públicas ou privadas, que mesmo diante de um longo período de *vacatio legis* acabaram por não se adequar às diretrizes da nova lei.

No cenário atual, onde as sanções administrativas previstas na lei ainda não se encontram vigência, é provável que o cenário do ordenamento jurídico brasileiro se mantenha assim, com o crescimento de casos a cada dia envolvendo a LGPD.

Não se pode negar que em meio a sociedade em que vivemos os dados possuem valores inestimáveis, principalmente para as empresas que, muitas vezes, veem o usuário como um produto.

Pelo fato de as sanções administrativas da LGPD não estarem em vigor, muitas empresas estão ignorando a vigência da LGPD e procrastinando sua adequação. Sendo assim, por atualmente haver uma legislação que prevê uma

segurança maior aos usuários, as empresas que saírem à frente e adequem-se o mais rápido possível ao que sugere a LGPD, poderão, inclusive, utilizar dessa prática como uma forma de marketing, uma forma de atrair clientes e até mesmo melhorar sua imagem frente a uma atualidade tão difícil.

A partir do surgimento da pandemia, as pessoas passaram a usar a *internet* para fazer compras, o que acabou por gerar uma maior preocupação do usuário com os seus dados e que sabendo encontrar respaldo jurídico para essa proteção, acabarão por optar pelas empresas adeptas a LGPD.

Importante destacar que os impactos que serão gerados pela LGPD não se limitam apenas à *internet*. Como explicado, uma das áreas que sofrerão grandes mudanças por meio dessa legislação serão as relações trabalhistas, que abrangem uma grande quantidade de informações pessoais pertencentes ao empregado e que devem ser fornecidas ao empregador, o qual deverá adaptar-se para protegê-las.

Assim como nas relações de consumo, o empregado nas relações trabalhistas, não está na mesma posição de igualdade que o empregador. Isso acaba por ser um problema, uma vez que devido à subordinação que o empregado deve ao empregador, este pode vir a consentir o tratamento de seus dados para finalidades que fogem de sua convicção, o que poderá ensejar no aumento de ações trabalhistas envolvendo a LGPD.

Caberá ao agente controlador dos dados procurar a melhor forma para sua empresa adequar-se ao que preceitua a lei. Essa adequação poderá dar-se seja por meio de contratação de uma empresa especializada, seja por meio de advogados e vistorias periódicas dentro das empresas, seja até mesmo alterando o modo de coleta de dados feito pelo RH da empresa.

Pelo fato de a LGPD ter um impacto geral no ordenamento jurídico é imprescindível a necessidade de seu estudo frente à todas as áreas do direito visto que no Brasil, a partir de sua vigência, diversos casos práticos começaram a surgir, revelando a necessidade de uma legislação nesse sentido.

Embora a LGPD esteja em vigor e os casos estejam começando a surgir, não existem muitas jurisprudências, tampouco doutrinas que a regulamentem as situações cotidianas, tornando mais difícil prever os impactos que a LGPD gerará na sociedade. A realidade que vem surgindo demanda muita atenção, e é nítido que as empresas sofrerão um grande impacto.

O que pode ser garantido é que, com a vigência dessa lei os cuidados das empresas deverão ser redobrados. Tais cuidados deverão ocorrer em contratos, relações de trabalho, *sites*, entre outros, pois estarão lidando com informações sensíveis de pessoas que terão o direito e a liberdade de escolher para o que seus dados serão utilizados, para quem serão repassados, e agora encontram respaldo jurídico para tanto.

Pela importância das relações de trabalho e pela quantidade de dados que nelas circulam, é plausível que a LGPD tenha um caráter subsidiário para decisões em outras áreas do direito, dada a complexidade da coleta de dados nessa esfera.

Importante também que haja um caminho para que o titular dos dados possa manusear suas informações, ter um livre acesso a elas, visto que a relação do empresário com o particular deve ser transparente, uma vez que o controlador poderá ser responsabilizado pelo fato de estar manuseando de forma errada um bem que não lhe pertence. Destaque-se, nesse particular, a importância do armazenamento desses dados pelo menor tempo possível, eliminando-os de sua base de dados, para que não haja um mau uso desses.

REFERÊNCIAS

- Agência Brasil. **Governo aprova estrutura da Autoridade Nacional de Proteção de Dados**. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-08/governo-aprova-estrutura-da-autoridade-nacional-de-protecao-de-dados>. Acesso em: 28 set. 2020.
- ANDRADE, Bruno. **Privacidade e proteção de dados: impactos da LGPD e GDPR**. Disponível em: <https://blueprintt.co/blog/2019/05/24/protecao-de-dados-lgpd/>. Acesso em: 13 mar. 2020.
- ARAÚJO, Carvalho Andrade Carvalho Cristiane e CALCINI, Ricardo. **O impacto da LGPD nas relações de trabalho**. Disponível em: <https://www.conjur.com.br/2020-set-17/lgpd-impactos-trabalhistas>. Acesso em 20 out. 2020.
- ÁVILA, Humberto. **Teoria dos Princípios: da definição à aplicação dos princípios jurídicos**. 4ª ed. São Paulo. Malheiros Editores, 2004.
- AZEREDO, João. **Covid-19 e o adiamento necessário da LGPD**. Disponível em: <https://www.migalhas.com.br/depeso/324456/covid-19-e-o-adiamento-necessario-da-lgpd>. Acesso em 24 set. 2020.
- BARAKAT, Nagib. Covid-19: **O uso de dados na pandemia e o adiamento da LGPD**. Disponível em: <https://ambitojuridico.com.br/noticias/covid-19-o-uso-de-dados-na-pandemia-e-o-adiamento-da-lgpd/> Acesso em: 24/09/2020
- BIONI, Bruno Ricardo **Proteção de Dados Pessoais - A Função e os Limites do Consentimento (Português)**. Rio de Janeiro: Editora Forense, 2018.
- DC, Blog. **Lei Geral de Proteção de Dados (LGPD): saiba por que sua empresa precisa entender sobre ela**. Disponível em: <https://dclogisticsbrasil.com/lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 10 out. 2020
- BRITO DE CASTRO, Bárbara. **Direito Digital na Era da Internet Das Coisas – O Direito à Privacidade e o Sancionamento da Lei Geral de Proteção de Dados Pessoais**. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-civil/direito-digital-na-era-da-internet-das-coisas-o-direito-a-privacidade-e-o-sancionamento-da-lei-geral-de-protecao-de-dados-pessoais/>. Acesso em 22 mai, 2020.
- CALCINI Souza, Ricardo e TORRES, Lucas. **Os impactos da Lei Geral de Proteção de Dados nas relações de trabalho**. Disponível em: <https://migalhas.uol.com.br/depeso/332108/os-impactos-da-lei-geral-de-protecao-de-dados-nas-relacoes-de-trabalho>. Acesso em: 15 out, 2020.
- COTS Marcio; OLIVEIRA Ricardo **Lei Geral de Proteção de Dados Pessoais Comentada** 2ª ed. São Paulo. Thomson Reuters Revista dos Tribunais, 2019.
- CUNHA, Mario Leonardo **Comentários à Lei Geral de Proteção de Dados** Brasília: Mauro Leonardo Cunha, 2018. E-book Kindle disponível em <https://www.amazon.com.br/Coment%C3%A1rios-Geral-Prote%C3%A7%C3%A3o->

Dados-Profissionais-ebook/dp/B07KY3LPFQ?ie=UTF8&ref_=ku_mi_rw_edp. Acesso em: 28 jun, 2020.

DONEDA, Danilo. **A proteção de dados em tempos de coronavírus.** Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/a-protacao-de-dados-em-tempos-de-coronavirus-25032020>. Acesso em 24 set. 2020.

FAUSTINO, André. **A proteção de dados pessoais no Brasil: Breve histórico do direito comparado até a atual realidade brasileira.** Disponível em: <https://ambitojuridico.com.br/edicoes/revista-154/a-protacao-de-dados-pessoais-no-brasil-breve-historico-do-direito-comparado-ate-a-atual-realidade-brasileira/>. Acesso em 13 mar. 2020.

FCR LAW. **Os Impactos trabalhistas da LGPD: como se preparar para o impacto nas relações de trabalho.** Disponível em: <https://www.covidfclaw.com.br/os-impactos-trabalhistas-da-lgpd-como-se-preparar-para-os-impactos-nas-relacoes-de-trabalho/#:~:text=COMPLIANCE%20TRABALHISTA&text=As%20san%C3%A7%C3%B5es%20por%20infra%C3%A7%C3%A3o%20previstas,elimina%C3%A7%C3%A3o%20de%20dados%20tratados%20irregularmente>. Acesso em: 20 out. 2020.

FREITAS Adriano, Nelson. **A LGPD e a pandemia.** <https://www.migalhas.com.br/depeso/325556/a-lgpd-e-a-pandemia>. Acesso em: 24 set. 2020.

GED e Serviços. **A história por trás da LGPD.** Disponível em: <https://arquivar.com.br/blog/a-lei-geral-de-protacao-de-dados-e-a-gestao-de-documentos/>. Acesso em: 22 mai. 2020.

GRECO, Elizabeth. **Os impactos da LGPD nas relações de trabalho.** Disponível em: <https://lawinnovation.com.br/os-impactos-da-lgpd-nas-relacoes-de-trabalho/>. Acesso em 23 set. 2020.

GRECO, Elizabeth. **O teletrabalho sob a ótica da LGPD e recomendações técnicas do MPT para as empresas.** Disponível em: <https://lopecastelo.adv.br/o-teletrabalho-sob-a-otica-da-lgpd-e-recomendacoes-tecnicas-do-mpt-para-as-empresas-2/>. Acesso em 20 out. 2020

KOROKU, Yuka Tonia. **Decisão LGPD.** Disponível em: https://migalhas.uol.com.br/arquivos/2020/9/B05F37C296A643_decisaoLGPD.pdf. Acesso em: 15 out. 2020.

MACIEL, Rafael Fernandes **Manual prático sobre a Lei Geral de Proteção de Dados Pessoais:** Atualizado com a Medida Provisória nº 869/18. Goiânia: RM Digital Education, 2019. E-book Kindle disponível em: https://www.amazon.com.br/Manual-pr%C3%A1tico-sobre-Prote%C3%A7%C3%A3o-Pessoais-ebook/dp/B07QWHS193?ie=UTF8&ref_=ku_mi_rw_edp. Acesso em 28 jun. 2020.

MARTINS Nunes, Natália. **10 princípios da LGPD para o tratamento de dados pessoais.** Disponível em: <https://ndmadogados.com.br/artigos/10-principios-da-lgpd-para-o-tratamento-de-dados-pessoais>. Acesso 28 jun. 2020.

MARTINS Pinto, Sérgio. **Direito do Trabalho**. 34^a.ed. São Paulo: SaraivaJur, 2018.

MEIRA, Fabiola. **Após sanção do governo, Lei Geral de Proteção de Dados começa a valer**. Disponível em: <https://www.conjur.com.br/2020-set-18/sancao-governo-lgpd-comeca-valer-nesta-sexta>. Acesso em 24 set. 2020.

OLIVEIRA, Sandro **Guia inicial de aplicação da LGPD: Segurança em plataformas digitais**. E-book Kindle Disponível em: <https://www.amazon.com.br/Guia-inicial-aplica%C3%A7%C3%A3o-LGPD-plataformas-ebook/dp/B082DQZDMC>. Acesso em: 25 jun. 2020.

OLIVIERI, Nicolau. **Rotinas e contratos de trabalho serão impactados pela LGPD?** Disponível em: <https://www.serpro.gov.br/lgpd/noticias/impactos-lgpd-rotinas-trabalhistas-contrato-de-trabalho>. Acesso em 23 jun. 2020.

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

PLANALTO, **Presidente Jair Bolsonaro Sanciona a LGPD**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 15 out. 2020.

PLANALTO, **Consolidação Das Leis do Trabalho**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 20 out. 2020.

SILVERIO, Karina. **A LGPD JÁ COMEÇOU A SURTIR EFEITOS NO JUDICIÁRIO**. Disponível em: <https://tutelas.com.br/a-lgpd-ja-comecou-surtir-efeitos-no-judiciario/>. Acesso em: 20 out. 2020.

SILVERIO, Karina. **7 MITOS DA LGPD MAIS COMUNS**. Disponível em: <https://tutelas.com.br/7-mitos-da-lgpd-mais-comuns/>. Acesso em 20 out. 2020.

TEIXEIRA, Tarcísio. **Afinal, o que são dados (pessoais) à luz da LGPD?** Disponível em: <https://www.ecommercebrasil.com.br/artigos/afinal-o-que-sao-dados-pessoais-a-luz-da-lgpd/>. Acesso em: 22 mai. 2020.

TEIXEIRA Ferraz, João Pedro. **LGPD 101 - Comentários à Lei Geral de Proteção de Dados**. Disponível em: <https://joaopedrofteixeira.jusbrasil.com.br/artigos/753086549/lgpd-101-comentarios-a-lei-geral-de-protacao-de-dados?ref=feed>. Acesso em 22 mai, 2020.

TEPEDINO, Gustavo; FRAZÃO Ana; OLIVA Milena Donato - **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo. Thomson Reuters Revista dos Tribunais, 2019.

VENTURA, Felipe. **Facebook mostra aviso sobre dados pessoais e LGPD no Brasil**. Disponível em: <https://tecnoblog.net/361328/facebook-mostra-aviso-sobre-dados-pessoais-e-lgpd-no-brasil/>. Acesso em: 02 out. 2020.

VERGILI Machado, Gabriela. **Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados.** Disponível em: <https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados/>. Acesso em: 11 jun. 2020.