CENTRO UNIVERSITÁRIO FAMETRO

CURSO DE DIREITO

REGINALDO SALES HISSA FILHO

LEI 13.719/2018 - LGPD
LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NA SOCIEDADE

Fortaleza-CE

2020

REGINALDO SALES HISSA FILHO

LEI 13.719/2018 - LGPD
LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NA SOCIEDADE

Artigo apresentado à banca examinadora e à Coordenação do Curso de Direito da Faculdade Metropolitana da Grande Fortaleza – FAMETRO – como requisito para a obtenção do grau de bacharel, sob a orientação da Prof.ª. Drª. Maria Neurilane Viana Nogueira.

Fortaleza-CE

2020

REGINALDO SALES HISSA FILHO

LEI 13.719/2018 – LGPD
LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NA SOCIEDADE

Esse artigo científico, foi apresentado no dia 16 de dezembro de 2020 como requisito para obtenção do grau de bacharel em Direito da Faculdade Metropolitaba de Grande Fortaleza – FAMETRO – tendo sido aprovado pela banca examinadora composta pelos professores abaixo:

BANCA EXAMINADORA

_____

Prof.a. Dra. Maria Neurilane Viana Nogueira
Orientadora – Faculdade Metropolitana da Grande Fortaleza

_____

Prof. Esp. Flávio Ribeiro Brilhante Junior
Membro - Faculdade Metropolitana da Grande Fortaleza

_____

Prof. Me. Vanilo Cunha de Carvalho Filho
Membro - Faculdade Metropolitana da Grande Fortaleza

AGRADECIMENTOS

A Deus, por todas as graças que alcancei na vida. A minha família, em especial meu pai Reginaldo Sales Hissa e minha mãe Maria Astânia Vieira Hissa, que sempre estavam presentes nos momentos em que precisei, aos meus filhos que sempre me dão força para tudo o que faço.

A minha orientadora, Neurilane Viana Nogueira, pela sua dedicação e paciência que com seu grande conhecimento acadêmico me deu segurança e direção nesse projeto.

LEI 13.719/2018 - LGPD
LEI GERAL DE PROTEÇÃO DE DADOS E SEUS IMPACTOS NA SOCIEDADE
LAW 13.719 / 2018 - LGPD
GENERAL DATA PROTECTION LAW AND ITS IMPACTS ON SOCIETY

Reginaldo Sales Hissa filho[1]

RESUMO

O presente artigo discorre sobre o impacto da implementação da Lei 13.709/18, LGPD (Lei Geral de Proteção de Dados), que entrou em vigor em Setembro de 2020. O presente estudo perpassou por uma abordagem histórica dos processos de tratamento de dados pessoais, mostrando seus princípios norteadores e legislação comparada europeia que foi base para elaboração da LGPD. Também demonstrou os impactos da nova lei no cotidiano social, bem como, analisou-se o tratamento dos dados pessoais pelas empresas de todo porte, e suas consequências jurídicas pela adequação à nova norma. Após apresentado o contexto histórico, sua evolução legislativa, foi mostrado todos os impactos sofridos nas relações entre os dados pessoais e seus controladores, suas consequências e sanções por que não seguir a nova lei de proteção de dados. Por fim foi feita as considerações finais projetando um possível cenário para o tratamento de dados pessoais no Brasil. Foi desenvolvido um estudo qualitativo, bibliográfico e documental na doutrina, legislação e jurisprudência existente sobre a tema.

Palavras-chave: Proteção de dados Pessoais. Impactos. LGPD. Privacidade. Tratamento de dados.

ABSTRACT

This article discusses the impact of the implementation of Law 13.709 / 18, LGPD (General Data Protection Law), which came into force in September 2020. The present study went through a historical approach to the processes of processing personal data, showing its guiding principles and comparative European legislation that was the basis for the elaboration of the LGPD. It also demonstrated the impacts of the new law on social life, as well as the treatment of personal data by companies of all sizes, and its legal consequences for adapting to the new standard. After presenting the historical context, its legislative evolution, it was shown all the impacts suffered in the relationship between personal data and its controllers, its consequences and sanctions for not following the new data protection law. Finally, the final considerations were made designing a possible scenario for the treatment of personal data in Brazil. A qualitative, bibliographic and documentary study was developed on the existing doctrine, legislation and jurisprudence on the subject.

Keywords: Protection of Personal Data. Impacts. LGPD. Privacy. Data processing.

[1] Discente do Curso de Direito da Faculdade Metropolitana da Grande Fortaleza – FAMETRO.

1. INTRODUÇÃO

Para entendermos a Lei Geral de Proteção de Dados, temos que fazer uma dilação histórica dos conceitos de dados pessoais e sua proteção jurídica ao longo do avanço das relações comerciais eletrônicas.

Estamos vivendo a era da informação e da computação em nuvem, todas as transações comerciais estão cada vez mais sendo realizadas de forma eletrônica. Em escala crescente, estamos fazendo nossas compras pela internet, pedindo comida por aplicativos. À medida que vamos nos digitalizando, nossos dados estão sendo armazenados por várias empresas, em seus servidores espalhados mundo a fora.

Uma empresa que comercializa seus produtos no Brasil não necessariamente tem suas operações digitais hospedadas em nosso país, ela pode guardar todas as nossas informações pessoais em *data centers* na Europa, na Ásia, ou seja, em qualquer parte do mundo.

Diante desse contexto de informatização da vida, o grande questionamento é: de que forma as empresas coletam e armazenam nossos dados? Que fazem com eles? Estão guardados de forma segura? Nossos dados apenas ficam guardados ou são comercializados para outras empresas?

A preocupação com a proteção da privacidade remonta há muito tempo. A Constituição do Império de 1824 já falava, de certa maneira, sobre o direito à privacidade, quando protegia o "segredo da carta" e a "inviolabilidade da casa", protegendo assim o meio físico e não o conteúdo propriamente dito. (MACIEL, 2019)

A respeito dessa temática, os advogados americanos Samuel Warren e Louis Brandeis, no ano de 1890, escreveram o artigo "The Right Privacy", que é considerado embrião do direito à privacidade e inviolabilidade à vida privada. (MACIEL, 2019)

Avançando um pouco, em 1970, na Alemanha, o estado de Hesse criou a primeira lei tratando especificamente da proteção de dados pessoais, saindo muito a frente do resto do mundo. Onze anos depois, em 1981, o Conselho da Europa criou o *Data Protection Convention (Treaty 108)*, sendo assim o primeiro instrumento legal internacional a proteger a pessoa contra qualquer abuso na coleta e no processamento de dados pessoais, prevendo ainda a regulação do fluxo desses dados entre os países europeus. No ano de 1983, a Corte Constitucional Alemã declarou inconstitucional a Lei do Censo, que obrigava os alemães a fornecerem seus dados pessoais ao estado. (MACIEL, 2019)

Avançando mais um pouco no tempo, e voltando nossa análise para o Brasil, na década de 1990 surgem os primeiros diplomas legais versando sobre a proteção dos dados pessoais. O nosso Código de Defesa do Consumidor regulamentou o uso de banco de dados de consumidores, prevendo ao consumidor o acesso a "informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele", o verdadeiro embrião da nossa LGPD. Em 1996 entra em vigor a Lei 9.296/96, Lei de Interceptação Telefônica e Telemática, que restringiu esse método investigativo apenas para algumas hipóteses e sempre com autorização de ordem judicial. Logo em seguida, em 1997, surge no nosso ordenamento a Lei do Habeas Data (Lei 9.507/97), que regula o acesso e a correção de informações pessoais. (MACIEL, 2019)

O nosso Código Civil de 2002 trouxe um importante avanço, quando inclui um capítulo sobre os Direitos da Personalidade. No ano de 2011, tivemos duas importantes leis incorporadas ao nosso ordenamento jurídico: a Lei do Cadastro Positivo e a Lei de Acesso a Informação. Em 2014, tivemos em nosso ordenamento jurídico a introdução do Marco Civil da Internet, que foi a última lei sobre o tema antes da Lei Geral de Proteção de dados. (MACIEL, 2019)

Importante frisar que, em 2018, tivemos a criação da GDPR (*General Data Protection Regulation)*, o regulamento do direito europeu sobre a privacidade e a proteção de dados pessoais, que se aplica a todos os indivíduos na União Européia e Espaço Econômico Europeu, e que aborda também a regulamentação do envio de dados pessoais para fora da EU (*Europian União*) e EEE (Espaço Econômico Europeu).

Acerca da temática em epígrafe, cumpre pontuar dois conceitos básicos: o primeiro sobre Bancos de Dados, e o segundo sobre informações de dados pessoais. O primeiro se caracteriza por um conjunto de arquivos armazenados, contendo registros de pessoas, lugares ou coisas, podendo ser chamado também de base de dados. Uma vez organizados os dados, eles se relacionam, de forma a criar algum sentido, fornecendo uma informação, com a finalidade de dar mais eficiência durante uma pesquisa ou estudo científico. Para se gerir esses dados, existem diversos softwares, chamados de SGDB (Sistema de Gerenciamento de Bancos de Dados). Eles possuem recursos capazes de manipular as informações do banco de dados, interagindo com o usuário. Eles podem ser pagos como Oracle e Microsoft SQL Server, ou software livre como MySql ou PostfreSql. (MACIEL, 2019)

Segundo Sartori, dados pessoais são as informações relativas a uma pessoa viva, identificada ou identificável. Também pode constituir dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa, senão vejamos:

> A questão dos dados pessoais é uma das mais tormentosas quando se fala em internet, porquanto tudo na rede mundial de computadores são dados. Dados são coletados, armazenados e, principalmente, são transformados em mercadoria, por possuir valor econômico. [...] A disciplina dos dados pessoais, obviamente, não é novidade. pois não se relaciona apenas ao processamento de dados pessoais realizado na internet, englobando também cadastros de indivíduos com os mais diversos fins. como estatísticos, censos estatais e arquivos de consumo, automatizados ou não. Todavia, a problemática envolvendo a tutela de dados pessoais ganhou, e ganha diariamente, novas nuances com a internet e a onipresença da tecnologia (SARTORI, 2016, p. 49).

Com essa abordagem, o presente trabalho estabelece como objetivo geral analisar os impactos da Lei Geral de Proteção de Dados, descrevendo sua evolução até a data de sua entrada em vigor. Como objetivo específico, vamos mostrar a evolução das leis de proteção de dados no Brasil e no mundo. Depois, mostraremos o surgimento da lei no Brasil, suas implicações, seus impactos no nosso ordenamento jurídico e suas consequências no cotidiano das empresas e das pessoas proprietárias dos dados pessoais.

Metodologicamente, esta análise vai extrair os dados de que necessita de diversas fontes: livros, revistas jurídicas, artigos, leis e até mesmo jurisprudências - que abordem e reflitam sobre viabilidade, adequação e suas consequências. Em outras palavras, o trabalho utilizou pesquisas bibliográficas e documentais, para expor o tema abordado sob a visão de vários autores, apresentando opiniões no mesmo sentido ou contrárias a respeito da sua eficácia.

Na realização da pesquisa, utilizou-se o método dedutivo de abordagem, partindo das leis e teorias para expor suas consequências. Desenvolve-se uma pesquisa do tipo explicativa, na qual se analisa e reflete sobre o objeto estudado. Com relação à aplicação dos resultados, optou-se por uma pesquisa pura, de natureza qualitativa.

No tocante à forma de distribuição dos dados, já devidamente sistematizados, obtidos neste artigo, o segundo capítulo, que sucede esta introdução, numerada como primeiro capítulo, retrata desde a sua evolução até sua criação. O terceiro capítulo vai apresentar um estudo comparativo entre a LGPD e a GDPR. O quarto capítulo irá analisar a sua introdução no ordenamento jurídico, suas penalidades para as empresas por não se adequarem à norma e seus impactos para a sociedade. Por fim, o quarto capítulo apresenta os aspectos conclusivos extraídos do estudo, reunidos sob a denominação de considerações finais.

2. A EVOLUÇÃO DAS LEIS DE PROTEÇÃO DE DADOS

Legislação para proteção de dados pessoais não é algo novo no ordenamento jurídico do Brasil e do mundo. O primeiro registro legal de proteção de dados aconteceu em 1824, na Constituição do Império, na qual se mencionava a proteção do "segredo da carta" e da "inviolabilidade da casa". Um conceito mais voltado para a propriedade, protegendo claramente o meio físico e não seu conteúdo, mas indiretamente sendo protegido. (MACIEL, 2019)

Dando um salto temporal, chegamos ao ano de 1988, onde foi promulgada nossa Constituição, que em seu inciso X do artigo 5º, fala: - "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*. Como podemos observar, esse inciso escrito há 32 anos atrás nunca fora tão atual, pregando a inviolabilidade da intimidade, da vida privada, sua honra e imagem das pessoas, que nos dias atuais são tão expostas.

Logo em seguida, no ano de 1990, entrou em vigor nosso Código de Defesa de Consumidor, Lei 8.078/1990, pois em nossa Constituição houve uma preocupação com o consumidor, definindo esse direito como garantia fundamental.

> No seu artigo 5º, inciso XXXII, esta Constituição prevê que o Estado deve promover, na forma da lei, a defesa do consumidor. Define ainda no artigo 170, inciso V, o direito do consumidor como um princípio da ordem econômica brasileira, uma vez que esta deveria proteger a parte mais frágil frente à voracidade do mercado financeiro. Demonstrando a necessidade de uma regulamentação específica sobre o assunto através de uma norma infraconstitucional, há no Ato das Disposições Constitucionais Transitórias da Constituição de 1988, no seu artigo 48, regulamentado que em cento e oitenta dias da promulgação da Constituição, seria elaborado o código de defesa do consumidor. (BRASIL, Constituição Federal, 1988).(SEBALHOS, 2015, Pg.5)

Os três anos após a promulgação da Carta de 1988 foram bem intensos em relação à produção de leis que protegiam a privacidade da pessoa. No ano de 1991, foi editada a Lei dos Arquivos Públicos (8.259/1991), que trata sobre a política nacional de arquivos públicos e privados. Vale que ressaltar que, logo em seu Art. 1º, fala na proteção especial a documentos de arquivos, que é o "*core*" da Lei Geral de Proteção de dados: *"É dever do Poder Público a gestão documental e a proteção especial a documentos de arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova e informação".*

Chegando ao ano de 1996, temos incorporado ao nosso ordenamento jurídico a Lei de Interpretação Telefônica e Telemática (Lei 9.296/96), que apesar de ser uma lei que regulava a interceptação telefônica, reconhecia o direito à privacidade, pois restringia a investigação por esse meio a determinadas situações, e sempre usando uma ordem judicial. Transpassando para o ano de 1997, chegamos à Lei do Habeas Data (Lei 9.507/97), remédio constitucional que regula o acesso e a correção de informações pessoais. (MACIEL, 2019)

No ano de 2002, tivemos um marco histórico no Direito Brasileiro: o novo Código Civil (Lei 10.406/2002). Muitas mudanças e modernizações foram incorporadas no referido Código. Entre essas atualizações, podemos destacar a inclusão do capítulo sobre os Direitos da Personalidade, que inclui a vida privada como direito, proibindo a sua violação. Com isso, a privacidade se tornou um direito subjetivo não mais focado no direito à propriedade. (MACIEL, 2019)

Mais um breve salto no tempo para chegar ao ano de 2011, onde entraram em nosso ordenamento duas importantes leis: a Lei do Cadastro Positivo (Lei 12.414/11) e a Lei de Acesso a Informação (Lei 12.527/11). A Lei do Cadastro Positivo foi concebida para que se formasse em nosso sistema financeiro um banco de dados com todas as informações de adimplemento de pessoas físicas e jurídicas, formando, assim, um histórico de crédito do bom pagador, uma espécie de contraponto ao cadastro negativo. (MACIEL,2019)

Uma questão muito importante nessa lei se dá na permissão por parte do consumidor na inclusão do seu nome no referido cadastro, visto que, sem a devida autorização, o nome da pessoa não é incluído no Cadastro Positivo. Essa autorização é um dos pilares da LGPD. No seu Artigo 7º, incisos I e X, há essa previsão e a proteção ao crédito como forma de proteção de dados pessoais, o que tornou a Lei do Cadastro Positivo obsoleta nesse sentido, tendo que ser atualizada no ano de 2019, com a Lei Complementar 166:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Com a Lei de Acesso à Informação (Lei 12.527/11), temos de uma maneira bem específica a definição de informação pessoal, sendo esta relacionada à pessoa natural identificada ou identificável. Já na seção V da lei, há um capítulo sobre informações pessoais, ficando bem definido seus princípios e direitos, assuntos bem abordados dentro LGPD.

> CAPÍTULO V
> DAS RESPONSABILIDADES
> Art. 32. Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar:
> II - utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;
> IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;

Dentro dessa cronologia, vale a pena citar a Lei 12.737/12, conhecida erroneamente como Lei Carolina Dieckman, já que seu verdadeiro nome é: Lei de Tipificação Criminal de Delitos Informáticos. Este Diploma Legal acrescentou ao nosso Código Penal os artigos 154-A(*Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita*:) e 155-B. Como o próprio nome da lei fala, criminaliza a invasão dos dispositivos informáticos, nesses dispositivos que contém dados pessoais. (MACIEL,2019)

Chegando ao fim da saga cronológica legislativa, no ano de 2014 tivemos a criação do Marco Civil da Internet (Lei 12.965/2014), a última Lei antes da Lei Geral de Proteção de Dados. Em seu livro Manual Prático Sobre a Lei Geral de Proteção de Dados, o professor Rafael Fernandes Maciel fala de maneira cirúrgica sobre o Marco Civil da Internet:

> Foi com o Marco Civil da Internet que o Brasil passou a constar em seu sistema jurídico a palavra "privacidade". Embora curioso, essa fato em nada inova, já que "vida privada", no frigir dos ovos, possui o mesmo sentido. Com o MCI entrando em vigor em 2014, a internet no Brasil passou a ser melhor disciplinada, prevendo como princípios a proteção da privacidade e dados pessoais(art.3º), nem como garantindo aos usuários, dentro outros os seguintes direitos(art.7º):
> *Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:*
> *VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;*
> *VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:*
> *a) justifiquem sua coleta;*
> *b) não sejam vedadas pela legislação; e*
> *c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;*O MCI estabeleceu, na Seção II do Capítulo III, regramento para a guarda e disponibilização dos dados pessoais, demandando ordem judicial para o acesso ao conteúdo e ainda trouxe os princípios da finalidade e adequação, vedando a guarda, provedores de aplicações, dos "*registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente"* e *"dados pessoais que sejam em relação à finalidade para a qual foi dado consentimento pelo seu titular (art.16)*(MACIEL, 2019, pgs. 14-15)

Como podemos observar, a caminhada legislativa para chegarmos à LGPD foi longa, porém extremamente importante para sua gestação. Apesar de ser uma lei nova, ela já nasce bem madura em relação aos seus objetivos pretendidos. Não podemos falar, logicamente, que é uma lei completa, bem robusta devido ao seu amadurecimento legislativo e por ter sido inspirada na legislação europeia, a GDPR.

2.1 Princípios basilares de proteção de dados pessoais

No Artigo 6º da LGPD, vêm elencados 10 princípios norteadores para aplicação da Lei em nosso ordenamento jurídico. Observando a evolução da legislação sobre proteção de danos no mundo, podemos notar que várias regras procedimentais contidas no *Report of the Seaetary Advisory Committee on Automated Personal Data System, de I973*, foram usadas repetidamente em várias legislações internacionais de proteção de dados, formando, assim, a base do sistema europeu. Tal repetição consolidou os princípios das normas de proteção de dados.

> 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.

Não por acaso, o primeiro princípio do artigo 6º é o da "*finalidade"*, sendo ele o principal princípio, pois exige a correlação entre o tratamento de dados e a finalidade informada.

O princípio da "*adequação"*, por sua vez, fala que os dados têm que ser tratados de acordo com a informação passada ao usuário. Já o da *"necessidade"*, prega que os dados devem ser tratados minimamente para atingirem as suas necessidades, impedindo que haja uma extrapolação do seu uso.

O *"livre acesso*", garante ao usuário o acesso à informação de como seus dados estão sendo tratados e por quanto tempo, tudo de maneira gratuita. O "*princípio da qualidade*" dos dados garante ao titular uma informação precisa e clara da real necessidade do cumprimento da finalidade de seu tratamento. (COTS, 2019)

O da "*transparência*" fornece ao titular dos dados todas as informações necessárias sobre como estão sendo tratados seus dados e por quem, resguardando os segredos comerciais e industriais. (COTS, 2019)

Já o da "*segurança"*, objetiva mostrar de forma técnica ao titular de que maneira estão sendo protegidas suas informações, evitando, assim, que sejam perdidos, subtraídos ou divulgados. O princípio da "*prevenção*" adota medidas que previnem qualquer dano relacionado ao tratamento de dados. Bastante interessante é o princípio da "*não discriminação*", pois prevê que o tratamento de dados não seja usado para promover qualquer ato discriminatório, ilícito ou abusivo. E como último princípio, a "*responsabilização e prestação de contas*" fala que o agente de tratamento de dados têm que demonstrar que todas as medidas tomadas para a proteção de dados pessoais foram eficazes:

> Um princípio fundamental que todas as atividades de processamento de dados devem seguir é o princípio da finalidade, que indica a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados. Esse princípio é essencial para se limitar o acesso de terceiros ao banco de dados. De forma semelhante, ele também serve como parâmetro para julgar se determinado uso dos dados pessoais é adequado e razoável, de acordo com a finalidade informada no primeiro momento ao interessado (DONEDA, 2006, p. 216).

No mesmo sentido, Rossnagel coloca que:

> Por fim, esse princípio exige que o responsável pelo tratamento de dados estabeleça de forma expressa e limitada a finalidade do tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas (ROSSNAGEL ,2003, p. 140).

Todos os princípios mencionados na LGPD derivam de outros princípios já incorporados em nosso ordenamento jurídico, como o da transparência, respeito à intimidade, à vida privada, à honra, à imagem das pessoas, e um dos mais importantes, que é o das liberdades e garantais individuais.

Dessa maneira, a Lei Geral de Proteção de Dados consolida preceitos encontrados em outras normas brasileiras que tratam ou tratavam da proteção de dados pessoais.

3. A NOVA LEI DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Muitos são os motivos para inclusão de uma Lei de Proteção de dados no Brasil. O principal motivo apontado por vários estudiosos dessa temática foi uma previsão na Lei Europeia GDPR (*General Data Protection Regulation*) que proíbe qualquer tipo de relação comercial com países que não tenham em seu ordenamento uma lei de proteção de dados, para proteger qualquer transferência de dados pessoais entre as organizações, países e a União Europeia. Ou seja, para trafegar esses, dados tem que seguir as regras da GDPR. (NÓBREGA, 2018)

Assim, como a entrada em vigor no dia 25 de maio de 2018, após 2 anos de sua aprovação, em 15 de abril de 2016, vários países apressaram a elaboração de sua legislação. Essa decisão para adequação baseada na legislação europeia pode ser extraída do *considerando nº 103*[9] e *Art. 45º*. A GDPR é dividida em 173 Considerandos e 99 Artigos, que são subdivididos em 11 capítulos. Cumpre ressaltar que os considerandos têm uma função interpretativa nos contratos, como podemos observar no considerando 109. (NÓBREGA, 2018)

> 109.A possibilidade de o responsável pelo tratamento ou o subcontratante utilizarem cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controle não os deverá impedir de incluírem estas cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas contratuais-tipo adotadas pela Comissão ou por uma autoridade de controlo, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados. Os responsáveis pelo tratamento e os subcontratantes deverão ser encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas-tipo de proteção. (https://www.privacy-regulation.eu/pt/28.htm)
>
> *Artigo 45.***Transferências com base numa decisão de adequação**. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica. (https://www.privacy-regulation.eu/pt/28.htm)

A nossa lei de proteção de dados está lastreada por nossa Constituição, pelo Código Civil e pelo Código de Defesa do Consumidor, sendo este de suma importância para completar possíveis lacunas.

Nossa LGPD irá também forçar que essas legislações façam uma atualização de vários de seus artigos, que foram redigidos numa época de pensamentos e relações analógicas. O mundo e suas relações estão a cada dia, e a passos largos, mais digital. O comércio, em um breve momento, será todo digital, os contratos serão digitais, até mesmo o dinheiro será eletrônico. Logo, o Direto terá que ir nesse caminho. (NÓBREGA, 2018)

3.1 A proteção de dados e seu reflexo na Responsabilidade Civil

Como foi dito anteriormente, o mundo e suas relações estão cada dia mais digitais, e essa evolução tecnológica apresenta uma velocidade nunca antes vista, o que se reflete em uma profunda alteração nas relações jurídicas. Como bem observou o Juiz de Direito em seu artigo sobre Responsabilidade Civil e a LGPD, Fernando Antônio Tasso coloca que:

> Diferentemente das anteriores, em que a constatação de sua ocorrência e identificação de seus fatores determinantes foi feita mediante análise de fatos pretéritos, a Quarta Revolução Industrial foi cunhada a partir do vislumbre de seu alvorecer pelo engenheiro e economista Klaus Schwab, fundador do Fórum Econômico Mundial, que a elegeu como tema da edição de 2016. Tem por pressupostos a eliminação dos limites entre os mundos físico, digital e biológico em decorrência do desenvolvimento das novas tecnologias em cada uma dessas áreas. Nesse contexto se estabelecem as novas perspectivas da responsabilidade civil, em tempos que Anderson Schreiber reputa caracterizado pela erosão dos filtros da responsabilidade civil que, ao lado da crescente ampliação das hipóteses de responsabilidade objetiva, a jurisprudência tem amalgamado na ampliação das hipóteses de indenização pelo dano presumido. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. (TASSO, 2016, Pgs. 100-101)

A responsabilidade civil está prevista na Seção III do capítulo VI da LGPD, nomeada "Da Responsabilidade e do Ressarcimento de Danos", que não necessariamente será absorvida pela responsabilidade civil, a depender do caso específico, abraçada pelo Código de Defesa do Consumidor, como deixou claro o Art. 45º da Lei: "*As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.".* Portanto, esse artigo esclarece que nem todo dano causado pelo uso indevido dos dados pessoais será absorvido pela Responsabilidade Civil, visto que muitos ficarão na esfera do Código de Direito do Consumidor.

O Capítulo VI, Seção III, Art 42º da LGPD, trata especificamente da responsabilidade civil e seu devido ressarcimento por danos causados pelos agentes de tratamento: "*Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo"*.

Prevendo claramente a reparação por danos patrimoniais, morais, individuais ou coletivos de maneira solidária, em seu parágrafo 1º, I e II, esmo não prevendo de maneira clara a culpa, não faz a exclusão de maneira tácita.

> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Além das responsabilidades civis previstas, a lei prevê aplicação de penalidades administrativas decorrentes da violação da legislação:

> 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: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; § 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: I - a gravidade e a natureza das infrações e dos direitos pessoais afetados; II - a boa-fé do infrator; III - a vantagem auferida ou pretendida pelo infrator; IV - a condição econômica do infrator; V - a reincidência; VI - o grau do dano; VII - a cooperação do infrator; VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas; e XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

As penalidades têm previsão de multas até R$ 50.000.000,00 (cinquenta milhões de reais). Mesmo com aplicação das sanções administrativas, não impede a cumulação com a responsabilidade civil, pois esse instituto possui múltiplas funções, como bem argumenta o professor Cristiano Chaves Farias:

> Cremos que no Direito Brasileiro do alvorecer do século XXI a conjunção destas orientações permite o estabelecimento de três funções para a responsabilidade civil: (1) função reparatória: a clássica função de transferência dos danos do patrimônio do lesante ao lesado como forma de reequilíbrio patrimonial; (2) função punitiva: sanção consistente na aplicação de uma pena civil ao ofensor como forma de desestímulo de comportamento reprováveis; (3) função precaucional: possui o objetivo de inibir atividades potencialmente danosas. (FARIAS, 2018, p. 62.)

Podemos observar que, no sistema judicial brasileiro, essas funções, reparatórias punitivas e precaucionais, são deixadas de lado e são pouco usadas, fazendo com que as indenizações tenham um valor bem inferior em relação ao dano causado. Assim, nas sanções administrativas há um relevante progresso, pois se usa uma série de critérios para que a penalidade seja aplicada de maneira mais coerente e proporcional à extensão do dano. (FARIAS. 2018)

3.2 Reflexões sobre a sistemática da proteção de dados no cenário jurídico brasileiro.

Com a entrada em vigor da LGPD em agosto de 2020, houve uma grande mudança na forma de tratar os dados pessoais por parte das empresas e pelo poder público. A lei trouxe em, seu texto, diversos novos atores, que entraram em cena a partir da sua validade.

O primeiro a entrar em cena foi o órgão que fiscaliza o cumprimento da lei; na verdade, houve uma pequena inversão nesse ato, já que o órgão deveria ter sido criado antes de a lei entrar em vigor, mas, em se tratando de Brasil, ele ainda está sendo constituído durante o ano de 2020, pelo menos tendo seus diretores já sido nomeados. (TEPEDINO, 2020)

Assim, foi criada a ANPD (Autoridade Nacional de Proteção de Dados), ficando incumbida de fiscalizar o cumprimento da lei, zelar pela proteção de dados pessoais, elaborar as diretrizes, aplicar as sanções em caso de descumprimento da norma, promover para a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança:

> Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.
> § 1º 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.
> 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.

> Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente.

Como podemos observar na letra da lei 13.709/18, a composição da ANPD é bem complexa, sendo de 04 anos o mandato do Conselho Diretor.

Caberá ainda ao órgão promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade, e promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade.

A ANPD se faz muito importante, como a própria vigência da lei. Recentemente, a OCDE - Organização para a Cooperação e Desenvolvimento Econômico-, entidade a qual o Brasil está tentando ser membro, emitiu um relatório[2] sobre a economia digital no país, sugerindo que o país deveria reavaliar as condições estabelecidas no Artigo 55-A da Lei 13.709, para garantir total independência da ANPD, fixando regras mais claras, e que as regras para a indicação do Conselho Diretor da ANPD e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP) sejam imparciais e baseadas em conhecimento técnico. (TEPEDINO, 2020)

A figura central da nova lei é o titular dos dados, que consiste na pessoa natural a quem se referem os dados pessoais que são objetos da coleta, tratamento e o correto descarte. Lembrando que dados pessoais são as informações relacionadas à pessoa natural identificada ou identificável, como seu CPF e seu endereço residencial. Os dados pessoais são também categorizados como “dados pessoais sensíveis”, que, de acordo com a lei, são aqueles dados que falam sobre sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político. Também é um dado sensível aquele que fala sobre seu estado de saúde ou vida sexual, dado genético ou biométrico, tudo isso atrelado a uma pessoa natural.

Segundo o artigo 11º da Lei, o tratamento desses dados pessoais sensíveis só poderá ser tratado quando o titular ou seu responsável legal consentir de forma explícita e destacada. Porém o referido artigo enumera algumas hipóteses em que esses dados poderão ser usados sem o consentimento do titular:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;

> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
> § 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica.
> § 2º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei.
> § 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.
> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir:
> I - a portabilidade de dados quando solicitada pelo titular; ou
> II - as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo
> § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Segundo o professor Gustavo Tepedino, em seu livro Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro, os dados são considerados sensíveis pois eles estão presentes em todos os conjuntos de informações da pessoa humana, se relacionando com sua intimidade e segredo. No mesmo sentido, Danilo Doneda coloca que:

> Deve-se ter em conta que o próprio conceito de dados sensíveis atende a uma necessidade de delimitar uma área na qual a probabilidade de utilização discriminatória da informação é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal consequência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes se preste a fins legítimos e lícitos.(DONENDA, 2010.p.27).

Podemos perceber que LGPD tornou os dados sensíveis, o "*core*" da privacidade no Brasil, tentando evitar o uso indevido desses dados de forma discriminatória, abusiva e até mesmo ilícita na manipulação dos dados do titular.

3.2.2. Principais pilares no tratamento de dados pessoais

A LGPD prevê 03 pilares para o tratamento de dados pessoais. Com a lei, surgiu a figura do Controlador, que é a pessoa natural ou jurídica de direito público ou privado que fica encarregada de tomar as decisões do tratamento dos dados pessoais.

O segundo pilar é o Operador, que, como o Controlador, também é uma pessoa natural ou jurídica de direito público ou privado, que fará o tratamento de dados pessoais em nome do Controlador. Por ele, passarão todos os dados dos usuários, sendo uma figura de extrema importância, por ter que receber, armazenar, dar a devida destinação e eliminar de maneira correta esses dados quando não forem mais necessários. (TEPEDINO, 2020).

O último pilar é o Encarregado, que é a pessoa nomeada pelo Controlador ou pelo Operador, atuando como ponte de comunicação entre o Controlador, os titulares dos dados e a ANPD. Surgiu assim a figura do DPO (*Data Protection Officer*), uma nova profissão no mercado de trabalho. Um profissional que deve[evitar repetição] ter conhecimentos tanto na área da tecnologia da informação como da área do direito. (TEPEDINO, 2020)

Em seu artigo Panorama Geral Da Lei Geral De Proteção De Dados Pessoais No Brasil e a Inspiração no Regulamento Geral De Proteção de Dados Pessoais Europeu, a professora Regina Linden Ruaro, definiu bem o papel do DPO:

> A legislação brasileira foi muito mais genérica que a europeia, inclusive nesta, há menção expressa que o DPO é uma obrigação específica para empresas com mais de 250 funcionários. Tal limitação pode vir a ser indicada pela Autoridade Nacional de Proteção de Dados no Brasil, porém até o momento toda e qualquer empresa que trate dados pessoais de forma online ou offline deverá ter um DPO, assim como cumprir todas as normas previstas na lei 13.709.(RUARO,2019, pg.352)

Sobre as figuras acima discutidas, a LGPD fala em seu texto, *in verbis:*

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.
> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.
> Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.
> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

Falamos muito até aqui de tratamento de dados, mas em que ele consiste? Trata-se de conceito muito amplo. Podemos dizer, então, que tratamento de dados é toda e qualquer forma de manipulação feita com as informações pessoais, que vão desde a coleta, a reprodução, o acesso, o armazenamento, a distribuição e o descarte desses dados. Será aplicada alei brasileira quando essas etapas no tratamento de dados pessoais forem feitas dentro do território brasileiro ou quando haja finalidade em oferecer bens ou serviços a pessoas localizadas no Brasil. Uma dúvida muito frequente que ocorre é: esses dados somente podem ser coletados pela internet? A resposta é não. Esses dados podem ser coletados tanto online, como offline. Tanto por meios físicos ou por meios digitais. (TEPEDINO, 2020).

Para ficar bem claro, a coleta online ocorre quando se usam ferramentas informatizadas ou automatizadas para obter esses dados. Por exemplo, ao acessar um wi-fi de um determinado local, a pessoa faz um pequeno cadastro utilizando seus dados, para ter acesso à internet. Já a coleta offline ocorre quando os dados são coletados de maneira não informatizada. Um bom exemplo para ilustrar essa coleta ocorre quando uma pessoa vai assistir a uma palestra e faz seu cadastro preenchendo em papel seus dados.

O professor Marcio Cots definiu muito bem esse tema:

> A pergunta que pode surgir é qual será a legislação aplicável no tratamento dos dados pessoais via internet, tendo em vista que a LGPD é mais ampla do que o Marco Civil da Internet e seu regulamento quanto a este tema específico.
> Por outro lado, por tratar de tema específico, com é o tratamento de dados pessoais, ao contrário do Marco Civil da Internet, poder-se-ia entender que a LGPD é lei específica , sendo o segundo apenas lei geral.(COTS,2019, p.62)

> 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:
> I - a operação de tratamento seja realizada no território nacional;
> 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; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.
> O caput do artigo deixa claro que a LGPD é aplicável “independemente do meio”, ou seja, ao contrário do Marco Civl da Internet e Decreto 8.771/16, que disciplinam o tratamento de dados por meio da Internet, a LGPD abrangerá o tratamento de dados offline também.

Como podemos notar, a maior parte das obrigações referentes ao tratamento dos dados são de responsabilidade do controlador, por se relacionar diretamente com o titular dos dados, ficando o operador com as obrigações acessórias.

Como o operador é indicado pelo controlador, deve-se deixar bem claro a sua responsabilidade para se evitar que o controlador receba alguma sanção por eventual falha do operador. Tanto o controlador como o operador deve manter registro de todas as suas ações nas operações de tratamento de dados.

3.2.3. Casos em que não se aplica a LGPD.

A lei deixou bem clara as regras que determinam quando não se deve aplicar a LGPD. Quando uma pessoa física colhe dados para fins particulares e não comerciais. Também quando jornalistas no exercício de sua profissão recolhem esses dados para uso específico, artístico ou acadêmico. Ainda, não se aplica ao poder público, no caso de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais.

Vale a pena ressaltar que na Câmara dos Deputados [3] já há uma proposta de Anteprojeto sobre o uso de dados na segurança pública, que consiste em versão da LGPD para as polícias, para fiscalização, para investigações. Pois nesses setores são aplicados outros trâmites de uso de dados e seu compartilhamento entre os órgãos de segurança pública, não podendo assim esses entes seguir à risca a atual Lei.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Gustavo Tepedino explanou de maneira precisa as razões pela não incidência da LGPD:

> Premissa básica do constitucionalismo moderno, informa que os direitos não absolutos. Por essa razão, a privacidade não se sobrepõe, aprioristicamente e em abstrato, aos demais direitos e valores constitucionalmente positivados. No Brasil, ao tempo em que o texto constitucional acolhe a privacidade(art.5º,X), também prevê, promove e garante a liberdade de expressão, a liberdade de imprensa, o direito à informação e a segurança (art. 5º, IV,IX, e XIV; art.220). No âmbito da segurança, destaca a segurança pública que se estabelece como um direito social no art.6º, e como responsabilidade de todos no art.144. (TEPEDINO, 2020 pg. 166)

Fica bem claro que a aplicação da LGPD não atingirá a todos. Incidirá praticamente nas pessoas jurídicas que usam os dados pessoais como forma de sustentar suas atividades comerciais ou que, devido à sua atividade, tratem de maneira volumosa esses dados. Assim, pessoas físicas não serão atingidas pela lei de proteção de dados.

3.2.4. Do Consentimento.

Um dos princípios da LGPD é o consentimento do titular, como vemos no artigo 5º: *Art. 5º Para os fins desta Lei, considera-se: XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;*. O consentimento consiste na livre manifestação, informada e inequívoca, pela qual o titular dos dados dá seu aval para que seus dados pessoais sejam coletados para aquela finalidade específica, devendo estes serem bem claros e destacados.

Cada vez mais comum, logo depois da entrada em vigor da lei, são os avisos em sites ou aplicativos, informando e pedindo a permissão do usuário para coletar seus dados. O consentimento é uma das partes centrais da LGPD, e é com ele que se inicia a aplicação da lei por parte dos atores envolvidos. Nesse sentido, Gustavo Tepedino, pontua que:

> A base legal do consentimento para o tratamento de dados do titular representa instrumento de autodeterminação e livre construção da esfera privada. Permite diferente escolhas e configurações em ferramentas tecnológicas, o que pode ter reflexos diretos na personalidade do indivíduo. Ainda que represente figura de grande relevância nas leis de dados, o consentimento não é a única hipótese para o tratamento de dados pessoais nem é hierarquicamente superior às demais bases legais dispostas na Lei 13.709/18. (TEPEDINO, 2020 pg. 292)

3.2.5. Das penalidades.

Apesar de a Lei ter começado a vigorar em setembro de 2020, as penalidades e multas só valerão a partir de agosto de 2021.

Ficará a cargo da ANPD – Agência Nacional de Proteção de Dados, toda a fiscalização e aplicação das sanções e multas. Essas penalidades passarão por uma avaliação da ANPD, indo desde uma advertência, até obrigar a publicação e divulgação da infração cometida. Ela poderá também determinar o bloqueio ou a eliminação dos dados que sofreram as possíveis violações. (TEPEDINO, 2020)

O valor estipulado das multas vai até 2% do faturamento, sendo fixado um teto de R$ 50.000.000,00(cinquenta milhões de reais) por infração. Além disso, poderá ter a suspensão das atividades de coleta e tratamento dos dados, sem prejuízo da indenização pelos danos que causarem aos titulares dos dados. Nesse sentido, Fábio Medina Osório nos ensina que:

> Sanção (administrativa retributiva) é um mal, um castigo, e, portanto, implica um juízo de privação de direitos, imposição de deveres, restrição de liberdades, condicionamentos, ligados, em seu nascedouro e existência, ao cometimento de um ilícito administrativo.[...] consequência de conduta ilegal, tipificada em norma proibitiva, com uma finalidade repressora ou disciplinar, no âmbito de aplicação formal e material do Direito Administrativo. (OSÓRIO, 2011,p.276)

> 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:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
> § 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:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
> § 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.
> § 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.
> § 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.
> § 5º [.....]
> § 6º As sanções previstas nos incisos X, XI e XII do **caput** deste artigo serão aplicadas:
> I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do **caput** deste artigo para o mesmo caso concreto; e
> II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.
> § 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo.

Como podemos ver no texto da lei, as sanções previstas para quem descumprir as normas legais são bem pesadas.

Não são aplicadas imediatamente. Somente após a fiscalização da ANPD, sendo constatada alguma irregularidade, primeiro se aplicará uma advertência, e só depois aplicar-se-á a multa, caso a empresa não esteja em conformidade ou não tenha iniciado o processo de adequação às normas. A previsão de 2% sobre o faturamento bruto anterior, por infração, limitado a 50 milhões de reais, é bastante pesada para qualquer empresa.

Para muitos doutrinadores, pior que a multa pecuniária, será a obrigação da publicização por parte da empresa quando ocorrer algum grave incidente com os dados pessoais, já que essa publicização acarretará, sem dúvida nenhuma, a negativação da imagem para a marca das empresas e sua credibilidade perante o seu consumidor. Medidas como uma boa Política de Segurança da Informação (PSI) e política de Compliance e Governança deverão estar cada vez mais no cotidiano daqueles que operam dados pessoais. O texto da lei trás um rol de sanções autoexplicativas, iniciando pela multa simples que se diferencia da multa diária. Para Márcio Cots e Ricardo Oliveira há uma interpretação sistemática e teleológica, que não deve ser aplicada de maneira sistemática, item a item, da lei, e sim ao caso concreto como um todo. (COTS, 2019)

3.2.6. O Legítimo Interesse.

O legítimo interesse certamente é um dos pontos mais controversos da LGPD, pela maneira bem subjetiva como foi abordado pela lei. Porém, esse tema é de extrema importância, pois sem ele empreendedores digitais e inovadores correriam sérios riscos de deixarem de existir com o advento da nova lei, em virtude do grande volume de dados já tratados antes da norma. Esses dados se tornariam inúteis por não se encaixarem na base legal, e não seria possível sua posterior regularização. Assim, foi criada a hipótese de tratamento de dados pessoais sem o enquadramento em qualquer base legal inclusive o consentimento. (COTS, 2020).

Com a possibilidade de se tratar os dados pessoais sem o consentimento expresso, podemos observar o primeiro grande ponto de controvérsia. Esse tema foi abordado em três ocasiões na lei: no art. 7º, sendo colocado como base jurídica no tratamento dos dados; no art.10º, estabelecendo seus requisitos de utilização da base jurídica; e no art.37º, colocando como obrigação o registro de todas as operações com tratamento de dados pessoais por parte do controlador e do operador.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:[...]
> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.
> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

A LGPD é bem clara: a partir de sua entrada em vigor, nenhuma empresa poderá mais tratar dados pessoais sem a devida autorização, sem o consentimento do usuário.

Surgiu então um grande questionamento: o que fazer com o infindável volume de dados pessoais de posse das empresas obtidos sem o consentimento do usuário? Teriam que ser descartados ou deletados? Se fosse dessa maneira, muitas empresas iriam à falência, ou até mesmo deixariam de existir. Pensando nisso, o legislador previu na Lei o Legítimo Interesse, que nada mais são do que exceções em que as empresas poderão dispor dos dados pessoais

sem o devido consentimento do usuário. Os incisos do artigo 10ºdeixam bem claras as exceções do uso dos dados pessoais.

Assim, esse dispositivo garantiu que o exercício do legítimo interesse deve satisfazer alguns requisitos, como somente ser usado em situações concretas os dos dados essências e necessários para a sobrevivência das empresas, possibilitando assim o caráter inovador destas, bem como o exercício da livre iniciativa. (OLIVEIRA, 2018)

3.2.7. A Administração Pública e Compartilhamento de Dados Pessoais.

Mas no que consiste o compartilhamento de dados pessoais? A lei deixa bem claro que o compartilhamento de dados consiste em toda e qualquer comunicação, difusão, transferência internacional, interconexão de dados pessoais ou o seu tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no estrito cumprimento de suas atribuições legais, ou também entre esses órgãos e entidades privadas. Esse compartilhamento só ocorre com o expresso e específico consentimento do titular dos dados. Em seu livro Proteção de Dados Pessoais – Comentários à Lei 13.709/2018, a doutora Patrícia Peck Pinheiro fundamentou bem esse tema:

> Outro ponto fa LGPD que demonstra a influência do GDPR na criação do documento brasileiro diz respeito aos requisitos aplicados ao tratamento de dados pessoais. A LGPD destaca que o tratamento de dados pessoais deve observar a boa-fé e possuir finalidades, limites, prestação de contas, garantir a segurança por meio de técnicas e medidas de segurança, assim como a transparência e a possibilidade de consulta aos titulares. (PECK, 2018. pg.84)

A Administração Pública está obrigada a seguir todas as regras da LGPD? A resposta é que sim. Mas, como bem sabemos, o poder público sempre recebe tratamento diferenciado pelo nosso ordenamento jurídico. Com a LGPD não foi diferente, como podemos observar em seus dispositivos.

O primeiro ponto que podemos destacar é que a Administração Pública pode tratar os dados pessoais sem o devido consentimento do usuário, desde que esses dados sejam para execução de políticas públicas. Também poderão tratar dessas informações nos casos em que envolverem segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, sendo que, nesse caso específico, como foi falado anteriormente, haverá uma legislação específica. Sobre a Administração Pública, não podemos deixar de citar Hely Lopes Meireles:

> Os princípios básicos da administração pública estão consubstancialmente em doze regras de observância permanente e obrigatória para o bom administrador: legalidade, moralidade, impessoabilidade ou finalidade, publicidade, eficiência, razoabilidade, proporcionalidade, ampla defesa, contraditório, segurança pública, motivação e supremacia do interesse público. Os cinco primeiros estão expressamente previstos no art.37, caput da CF de 1988; e os demais, embora não mencionados decorrem do nosso regime político, tanto que, ao daqueles, foram textualmente enumerados pelo art. 2º da Lei Federal 9.784, de 29.01.19. (MEIRELLES, 2000, p.91)
>
> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
>
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
>
> II - (VETADO);
>
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e
>
> IV - (VETADO).
>
> § 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.
>
> § 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
>
> § 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
>
> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
>
> § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

O professor Marcio Cots, muito bem destacou um ponto importante a ser comentado, se referindo a uma previsão no texto da lei original que vedava o compartilhamento de dados na esfera do poder público e com pessoas jurídicas de direito privado, com base na Lei de Acesso a informação - Lei 12.527/2011. Essa previsão geraria grande insegurança jurídica. Atento a isso o legislador vetou essa proibição através da Lei 13.859/2019, por não fazer o menor sentido, pois a troca dessas informações é crucial para o regular exercício das diversas atividades e políticas públicas:

> Por estar atrelado à lei, o Poder Público precisa das permissões legais adequadas para sua atuação, o que incluía possibilidade de tratamento de dados de pessoas naturais, com prevê a LGPD.
> Dessa forma, essencial as disposições da LGPD dedicadas a normatizar o tratamento de dados por entes públicos, a fim não apenas de garantir o atendimento do interesse público, mas também para possibilitar maior transparência aos titulares do que, efetivamente, é feito com seus dados. (COTS, 2020,p 143)

Como bem sabemos o Poder Público sempre precisa de normas mais adequadas à sua finalidade e à sua realidade, que o difere dos demais atores do cenário jurídico. Nunca poderá ser tratado de maneira igual ao setor privado, por cuidar dos interesses da sociedade, do seu bem estar, da sua segurança e da sua saúde.

O artigo 23 e seus incisos trataram de adequar essa especificidade do poder público, como não poderia deixar de ser. Podemos destacar como ponto central do artigo 23 a não necessidade do consentimento, do usuário proprietário dos dados pessoais, para a manipulação desses dados quando o poder público achar necessário. Desse modo, ficam bem definidos na lei os papéis tanto das entidades privadas como do poder público no tratamento dos dados pessoais e suas consequências.

4. Considerações Finais

Um dos mais notáveis matemáticos de nossa época, o londrino Clive Humby, cunhou uma frase que mostra a real importância da necessidade de os países adotarem leis de proteção de dados: "*data is the a new oil",* que em uma tradução livre significa que os dados são o novo petróleo. Além da proteção da individualidade, resguarda-se a personalidade física e digital, bem como garantias fundamentais. Existe um comércio gigantesco de venda de dados pessoais, eis que bancos de dados de empresas valem muito dinheiro. A lei vem com o objetivo de tentar regular também essa prática, que põe em risco a privacidade das pessoas.

Assim, a LGPD foi criada, tendo como molde a lei europeia, a GDPR, tem por intuito oferecer ao cidadão brasileiro um maior controle sobre os seus dados pessoais, stabelecendo de maneira assertiva princípios, criando regras claras e bem definidas que devem ser seguidas pelas organizações privadas e públicas.

Neste artigo, tentamos apresentar os principais pontos da Lei Geral de Proteção de Dados, e seus impactos futuros nas relações que envolvam o tratamento de dados pessoais e todos aqueles que coletam e usam de alguma forma esses dados. A lei foi muito bem redigida, com alguns pontos controversos, nada mais do que o normal. O impacto inicial com a entrada em vigor da lei foi um maior cuidado com os dados pessoais por aqueles que coletam e tratam esses dados.

A partir de sua vigência, as empresas ou entes públicos não poderão mais tratar com descaso a gestão desses dados. Vimos também o surgimento de uma nova profissão no mercado de trabalho, o DPO (*Data Protection Officer*), um profissional que deverá possuir conhecimentos tanto jurídicos como técnicos de informática.

O tema, por ser muito novo, até o presente momento não apresenta nenhum julgado em nossos tribunais. Mesmo neófito na seara jurídica, podemos encontrar bons autores que atuam nessa área do Direito Digital já há algum tempo, como a Dra. Patrícia Peck Pinheiro, a professora Viviane Nóbrega Maldonado, o professor Danilo Doneda e o advogado Renato Ópice Blum. Suas obras foram muito importantes para a construção deste artigo. Suas teorias são bem convergentes nessa temática, não havendo quase nenhuma discordância doutrinária. Tendo como um ponto em comum, que o direito está sofrendo uma profunda transformação, saindo do mundo analógico e se tornando digital, e todos os operadores do direito terão que estar preparados para essa nova realidade.

REFERÊNCIAS

BRASIL. Câmara dos Deputados. **Medida Provisória 869. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências.** Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Mpv/mpv869.htm>. Acesso em: 15 setembro 2020.

BLEONARDI, Marcel. **Fundamentos do Direito Digital**. 3ª ed. São Paulo – SP. Revista dos Tribunais, 2019.

COTS, Márcio. OLIVEIRA, Ricardo**. O Legítimo Interesse e a LGPDP**. 1ª ed. São Paulo. Revista dos Tribunais, 2020.

COTS, Márcio. OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. 3ª ed. São Paulo. Revista dos Tribunais, 2020.

FARIAS,Cristiano Chaves. ROSENVALD,Nelson. BRAGA NETTO, Felipe Peixoto. **Curso de Direito Civil. Vol.3**. 6ª ed. São Paulo. Editora Jus Podivm, 2018

FERNANDES MACIEL, Rafael. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais**. 1ª ed. Goiânia-GO, 2019.

MEIRELLES, Hely Lopes. **Direito Administrativo Brasileiro**. 25ª ed. São Paulo-SP. Malheiros, 2000.

LUCON, Paulo Henrique dos Santos. WOLKART, Erik Navarro. LAUX, Francisco de Mesquita. RAVGNANI, Giovani dos Santos. **Direito, Processo e Tecnologia**. 1ª ed. São Paulo-SP. Thomson Reuters Brasil, 2020.

NOBREGA MALDONADO, Viviane. **LGPD – Lei Geral de Proteção de Dados Pessoais. Manual de Implementação**. 3º ed. São Paulo-SP. Revista dos Tribunais, 2020

NOBREGA MALDONADO, Viviane. OPICE BLUM, Renato. Comentários ao GDPR-Regulamento Geral de Proteção de Dados da União Europeia.4ª ed. São Paulo-SP. Revista dos Tribunais, 2019

OLIVEIRA, Ricardo, **Lei Geral de Proteção de Dados e seus impactos no ordenamento jurídico**. Revista dos Tribunais, v 107. N. 988, fev. 2018.

OSÓRIO, Fábio Medina, **Direito Administrativo Sancionador**. Revista dos Tribunais, 6ªed. São Paulo – SP, 2011

PINHEIRO, Patrícia Peck, **Proteção de dados Pessoais. Comentários à Lei nº 13.709/2018(LGPD)**. 2ª ed. São Paulo-SP:Saraiva Educação, 2020.

RUARO, Regina Liden. GLITZ, Gabriela Pandolfo Coelho. **Panorama Geral Da Lei Geral De Proteção De Dados Pessoais No Brasil e a Inspiração No Regulamento Geral De Proteção De Dados Pessoais Europeu**. REPATS, Brasília, V.6, nº 2, p 340-356, Jul-Dez, 2019.

SARTORI, Ellen Carina Mattias. **Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na internet**. Revista de Direito Civil Contemporâneo, São Paulo, v. 9, ano 3, p. 49-104, out.-dez. 2016.

TEPEDINO, Gustavo. FRAZÃO, ANA. OLIVA, Milena Donato. **Lei Geral de Proteção de Dados e suas repercussões no Direito Brasileiro**. Revista dos Tribunais, 2ªed. São Paulo – SP, 2020.

_____. Constituição da República Federativa do Brasil de 1988. **DOU de 5.10.1988**. Brasília, DF: Casa Civil da Presidência da República, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 2 out. 2020.

_____. Constituição Política do Império do Brazil (de 25 de março de 1824). Elaborada por um Conselho de estado e outorgada pelo Imperador D. Pedro I, em 25.03.1824. **Coleção de Leis do Império do Brasil - 1824, p. 7, v. 1**. Rio de Janeiro: Secretaria de Estado dos Negócios do Império do Brazil a fls. 17 do Liv. 4º de Leis, Alvarás e Cartas Imperiais, 1824. Disponível em: <http://www.planalto.gov. br/ccivil_03/Constituição/Constituicao24.htm>. Acesso em: 15 out. 2020.

_____. Lei 13.709/2018. Lei Geral de Proteção de Dados. **DOU de 15.08.2018**. Brasília, DF: Casa Civil da Presidência da República, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 17 oago. 2020.

_____. Novo Código Civil Brasileiro. **DOU de 11.01.2002**. Brasília, DF: Casa Civil da Presidência da República, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 10 out. 2020.

3._____.https://www.camara.leg.br/noticias/694562-anteprojeto-sobre-uso-de-dados-na-seguranca-publica-deve-ficar-pronto-em-novembro/

2._____https://www.oecd.org/education/a-caminho-da-era-digital-no-brasil-45a84b29-pt.htm

_____. https://www.lgpdbrasil.com.br/resolucao-do-bacen-equipara-risco-cibernetico-a-risco-operacional/

_____.https://www.privacy-regulation.eu/pt/28.htm