PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

TRATAMENTO DE DADOS PESSOAIS

POR QUE PRECISAMOS SABER COMO OS NOSSOS DADOS PESSOAIS SÃO TRATADOS?

ORIENTANDA: ISABELLA TEIXEIRA MARTINS

ORIENTADORA: PROFA. DRA. MARINA RÚBIA MENDONÇA LOBO

GOIÂNIA
2020

ISABELLA TEIXEIRA MARTINS

TRATAMENTO DE DADOS PESSOAIS

POR QUE PRECISAMOS SABER COMO OS NOSSOS DADOS PESSOAIS SÃO TRATADOS?

Monografia Jurídica apresentada à disciplina Trabalho de Curso II , da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Profa. Orientadora: Dra. Marina Rúbia Mendonça Lobo.

GOIÂNIA
2020

ISABELLA TEIXEIRA MARTINS

TRATAMENTO DE DADOS PESSOAIS

POR QUE PRECISAMOS SABER COMO OS NOSSOS DADOS PESSOAIS SÃO TRATADOS?

Data da Defesa: ____ de _____ de 2020

BANCA EXAMINADORA

_____

Orientadora: Profa. Dra Marina Rúbia Mendonça Lobo Nota

_____

Examinador: Prof. Me Luiz Paulo Barbosa da Conceição Nota

SUMÁRIO

RESUMO 5

INTRODUÇÃO..... 6

1 DIREITO DIGITAL 8

1.1 CONCEITO DE DIREITO DIGITAL 8

1.2 EVOLUÇÃO HISTÓRICA DO DIREITO DIGITAL E SURGIMENTO DA LEI 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS 9

2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI Nº 13.709/2018 14

2.1 INTRODUÇÃO AOS DADOS PESSOAIS 14

2.2 ENTENDENDO A LEI Nº 13.709/2018 15

2.2.1 Conceito e vigência 16

2.2.2 Terminologia 17

2.2.3 Princípios 18

2.2.4 Territorialidade 19

2.2.5 Direito à privacidade e à informação 20

2.3 TRATAMENTO DE DADOS PESSOAIS 22

2.3.1 Bases legais da Lei 23

2.3.2 Tratamento de Dados Pessoais pelo Poder Público 26

2.4 DIREITOS DO TITULAR 27

2.4.1 Direito ao esquecimento e exclusão dos dados pessoais 28

3 RESPONSABILIDADE CIVIL, SEGURANÇA E BOAS PRÁTICAS 30

3.1 BOAS PRÁTICAS, GOVERNANÇA E COMPLIANCE 32
3.2 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS – ANPD 33
3.2.1 SANÇÕES ADMINISTRATIVAS 35

CONCLUSÃO 37

REFERÊNCIAS BIBLIOGRÁFICAS 40

RESUMO

MARTINS, Isabella Teixeira. **Tratamento de Dados Pessoais: Por que precisamos saber o porquê nossos dados pessoais são tratados?** 2020. 42 f. Monografia (Graduação em Direito) – Pontifícia Universidade Católica de Goiás, 2020.

A priori, a referida monografia busca apresentar a Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018 e explicar como o tratamento de dados pessoais deve acontecer. Dessa forma, é apresentado como a lei surgiu, o conceito de dados pessoais, as formas de tratamento destes dados, o direito à privacidade e à informação, direito ao esquecimento e à exclusão de dados pessoais e a responsabilidade civil, segurança e boas práticas.

Palavras-Chave: Direito Digital – Dados Pessoais – Privacidade – Proteção de Dados Pessoais – Responsabilidade Civil

INTRODUÇÃO

A priori, o objetivo deste trabalho de conclusão de curso é analisar e estudar a aplicabilidade da Lei 13.709/2018, no que se refere ao Tratamento de Dados Pessoais. Além disso, busca entender a trajetória do Direito Digital na história, bem como evidenciar conceitos e princípios importantes. Nesse sentido, será analisado o posicionamento doutrinário majoritário no que tange ao direito à privacidade e ao dever de informação.

Explica-se a escolha do referente tema em decorrência da evolução do Direito e da necessidade de um estudo mais aprofundado dessa questão. O comportamento humano mudou ao longo dos anos e hoje, praticamente tudo que as pessoas fazem, é postado na internet e esse comportamento precisa ser pautado pelo Direito, que rege as regras do bom convívio social.

É notório saber que a lei específica que hoje, aborda sobre o tratamento de dados pessoais, não está ligada à cidadania ou a nacionalidade dos dados pessoais, mas sim como os dados deverão ser armazenados e protegidos em território brasileiro. Atualmente, para se ter acesso a certos serviços, produtos ou conveniências, é necessária uma troca de informações, um cadastro dos dados pessoais.

Sendo assim, essas empresas e até órgãos públicos deverão desenvolver meios de proteger esses dados, a fim de evitar a violação de dados por meio de exposição, perda (quando não há backup), uso não adequado ou uso ilícito.

Portanto, serão abordados durante o trabalho alguns tópicos conexos, no intuito de explicar e entender as garantias dessa legislação específica.

O trabalho foi dividido em três capítulos e o seu teor foi elaborado com base em materiais coletados em pesquisas, e-books sobre o tema, legislações e, também, em doutrinas.

No primeiro capítulo desse trabalho será abordado o conceito de Direito Digital, bem como sua evolução histórica no Brasil e no mundo, sendo necessário entender o porquê a Lei Geral de Proteção de Dados Pessoais existe.

Ato contínuo, o segundo capítulo tratará sobre a Lei Geral de Proteção de Dados, o tratamento de dados pessoais, seu conceito, princípios e direitos do usuário. Também será esclarecido como as empresas e órgãos públicos devem agir e a penalidade aplicada, caso descumpram a regra.

Por fim, o terceiro capítulo tratará sobre a responsabilidade civil perante o tratamento de dados e as consequências tanto para o usuário tanto para quem controla o banco de dados, bem como as boas práticas, *compliance* e segurança.

1 DIREITO DIGITAL

1.1 CONCEITO DE DIREITO DIGITAL

Antes de começar efetivamente este trabalho, é preciso entender o conceito de Direito Digital. Para isso, Patrícia Peck explica que:

> O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.). (PECK, 2016, p. 77)

A tecnologia evolui a cada dia e o Direito precisa acompanhar essa mudança para que os direitos fundamentais, individuais, sociais, trabalhistas, dentre outros sejam respeitados em sua totalidade. Isso significa que os responsáveis por garantir o direito de imagem, da propriedade intelectual e industrial, segurança da informação, autoral, dentre tantos outros, são os novos profissionais do Direito que estão atuando no Direito Digital.

Com o passar dos anos, a tecnologia foi integrada e hoje todos são capazes de acessar tudo que quiser pelo celular, computador, tablet ou qualquer outro aparelho que possibilite postar uma foto nas redes sociais, fazer uma ligação, chamada de vídeo, tudo a uma distância de um clique.

Por causa dessa integração, o mundo todo está conectado. As empresas transformaram seu negócio e se adaptaram para conquistar uma maior visibilidade com a internet. Porém, com esse aumento, houve o crescimento de *hackers*, plágios, vazamento de dados pessoais, dentre outros problemas. Isso fez com que as infrações ao Código de Defesa do Consumidor, por exemplo, e o desrespeito a marcas e patentes também aumentassem. Por isso, quando há uma manifestação em massa, essas condutas precisam ser abordadas e estudadas pelo Direito, a fim de garantir uma segurança jurídica.

O Direito Digital traz consigo a possibilidade de utilizar uma série de princípios e soluções que já são utilizados no ordenamento jurídico brasileiro e internacional, podendo assim preencher as lacunas e alcançar resultados satisfatórios. Logo, o Direito Digital estabelece um relacionamento entre o Direito Codificado e o Direito Costumeiro, utilizando – se dos seguintes elementos para ampará-lo: generalidade,

uniformidade, continuidade, durabilidade e a publicidade.

> O Direito é responsável pelo equilíbrio da relação comportamento-poder, que só pode ser feita com a adequada interpretação da realidade social, criando normas que garantam a segurança das expectativas mediante sua eficácia e aceitabilidade, que compreendem e incorporem a mudança por meio de uma estrutura flexível que possa sustenta-la no tempo. Esta transformação nos leva ao Direito Digital. (PECK, 2016, p. 57)

Sabe-se que o Direito Digital parte da premissa de que toda relação que envolve textos e multimídias, através da ação humana ou de máquinas, gera direitos, deveres, obrigações e responsabilidades. Por isso o Direito Digital se vale de vários mecanismos, dentre eles, a analogia, costumes, princípios gerais de direito etc. que possibilite a regulamentação dessas relações, entre seres humanos e máquinas, a fim de intermediar os conflitos gerados por elas.

Deve-se lembrar que a internet não é o principal objeto de estudo do Direito Digital, mas sim um mecanismo que precisa ser juridicamente atendido, assim como todas as inovações tecnológicas.

Patrícia Peck elucida as principais características do Direito Digital. Senão vejamos:

> As características do Direito Digital, portanto, são as seguintes: celeridade, dinamismo, auto-regulamentação, poucas leis, base legal na prática costumeira, o uso da analogia e solução por arbitragem. Esses elementos o tornam muito semelhante à *Lex Mercatoria* (significa "conjunto de regras, princípios e costumes oriundos da prática comercial, sem vinculação a qualquer direito nacional"), uma vez que ela não está especificamente disposta em um único ordenamento, tem alcance global e se adapta às leis internas de cada país de acordo com as regras gerais que regem as relações comerciais e com os princípios universais do Direito como boa-fé, *suum cuique tribuere* (significa "dar a cada um o que é seu")*, neminem laedere* (significa "a ninguém lesar") *e honeste vivere* (significa "viver honestamente"). (PECK, 2016, p. 82)

Como já dito, o Direito Digital se vale dos costumes, e o Direito Costumeiro, ou *Common* Law, é um Direito que utiliza o histórico de decisões de casos concretos com base legal para uma ação judicial, ou seja, ele cria um banco de dados de memória futura, tendo como referência os costumes da sociedade.

A prática costumeira é importante e deve ser levada em consideração, pois no Direito Digital, é necessário ter dinamismo para dar soluções rápidas aos conflitos, tendo em vista que a tecnologia de hoje, pode se tornar obsoleta daqui um dia, mês ou ano. Deve-se levar em consideração que o Direito é um conjunto de comportamentos e linguagens. Hoje podemos ver isso mais claramente.

1.2 SURGIMENTO DA LEI 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Percebe-se que a sociedade vive em constante mudança. A prova disso é a evolução de mecanismos que usamos no dia a dia, como por exemplo: do Código Morse passamos a utilizar a localização por GPS (*Global Positioning System*), da carta ao e-mail, do telegrama ao *WhatsApp*, do rádio ao *Spotify* e assim sucessivamente. As informações, hoje, circulam de uma maneira cada vez mais rápida, logo, os meios pelos quais essas informações circulam também estão em constante crescimento.

Por isso, Patrícia Peck (2016, p. 51) traz alguns apontamentos sobre as Três Ondas e sua evolução histórica: Alvin Toffler era um escritor e futurista norte-americano, conhecido por escrever sobre a revolução digital e que abordou um tema bastante relevante: as três ondas. A Primeira Onda ele caracteriza como a Era Agrícola, pois foi o momento em que os humanos deixaram o nomadismo e passaram a cultivar a terra e usá-la como instrumento de poder e riqueza. A Segunda Onda teve início com a Revolução Industrial, em que a riqueza passa a ser uma combinação de propriedade, trabalho e capital e com seu ápice na Segunda Guerra Mundial.

E por fim, a Terceira Onda, conhecida como a Era da Informação ou Era Digital e que teve início no auge da Segunda Onda, com a criação dos grandes veículos de comunicação, como por exemplo o telefone, rádio, televisão, rádio, dentre outros, num período de cinquenta anos entre o final do século XIX e início do século XX. A característica principal da Terceira Onda é o grande tráfego de informações, que cresciam constantemente. (PECK, 2016, p. 52)

A Terceira Onda foi consolidada quando houve a criação da tecnologia digital, bem como o surgimento da Internet, pois ela conseguiu incluir dois elementos importantes: velocidade na transmissão de informações e a descentralização destas. (PECK, 2016, p.52)

> Na Era Digital, o instrumento de poder é a informação, não só recebida mas refletida. A liberdade individual e a soberania do Estado são hoje medidas pela capacidade de acesso à informação. Em vez de empresas, temos organizações moleculares, baseadas no Indivíduo. A mudança é constante e os avanços tecnológicos afetam diretamente as relações sociais. Sendo assim, o Direito Digital é, necessariamente, pragmático e costumeiro, baseado em estratégia jurídica e dinamismo. (PECK, 2019, p. 74)

Então, a partir desse momento e com o desenvolvimento da tecnologia digital, a privacidade passou a ser algo muito importante e para entender o momento que se tornou um direito fundamental, passível de proteção pela jurisdição, é necessário entendermos a evolução histórica do Direito Digital no Brasil até o surgimento da Lei 13.709/2018, que trata sobre a proteção de dados pessoais.

> Essa investigação histórica nos ajuda a confirmar o fato de ser a privacidade um valor desejado hoje, ainda que alguns, há pouco tempo, tenham sustentado que em troca dos benefícios proporcionados pela miríade de serviços gratuitos na Internet, as pessoas renunciariam, ou não se importariam, com a violação a esse direito. (MACIEL, 2019, online).

Em 1824, com a Constituição do Império que reconheceu o direito à privacidade ao proteger o “segredo da carta” e a “inviolabilidade da casa”. Nessa época, a privacidade estava ligada a ideia de propriedade, protegendo o meio físico e não o conteúdo em si.

O Brasil teve influências internacionais no que se refere a legislações sobre proteção de dados e privacidade. É importante saber que a primeira lei mundial de proteção aos dados pessoais, surgiu em 1970, no Estado Alemão de Hesse, que reconheceu que os “dados pessoais constituem uma projeção da personalidade do indivíduo e que, portanto, merecem uma tutela forte” (SCHERTEL, 2011, online).

No Brasil, a partir de 1990 surgiram legislações que deram à proteção de dados pessoais uma nova visibilidade, surgindo então a Lei nº 8.078/90, conhecida como Código de Defesa do Consumidor, que, dentre outras abordagens, passou a regular sobre os dados dos consumidores, dando a eles o direito a “informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivado sobre ele”. A partir de então, outras leis surgiram, a fim de regulamentar e proteger a privacidade.

> O Código de Defesa do Consumidor disciplinou, em seu art. 43, os bancos de dados e cadastros de consumidores. Note-se a amplitude do dispositivo em questão, que alcança todo e qualquer dado pessoal do consumidor, indo muito além, portanto, dos bancos de dados de informações negativas para fins de concessão de crédito. A racional do legislador foi alcançar todo e qualquer banco de dados que atinja o livre desenvolvimento da personalidade do consumidor. (BIONI, 2020, online)

A privacidade foi ganhando relevância ao longo do tempo, e em 2002 o Código Civil Brasileiro, trouxe um capítulo sobre os Direitos da Personalidade, incluindo a vida privada, e fornecendo instrumentos para coibir a violação deste direito. É importante ressaltar que o teor do Código Civil Brasileiro, traz a proteção à privacidade como um direito subjetivo, evoluindo o conceito de proteção dado em 1824.

A privacidade ganhou grande destaque quando, no início de setembro de 2013, Edward Snowden revelou que Dilma Rousseff, a então Presidente da República na época, e seus principais assessores haviam sido alvos diretos de espionagem de uma agência americana (G1, 2013, online). Isso fez com que o governo brasileiro tomasse medidas, e uma delas foi a tramitação do PL 2126/11 (Marco Civil da Internet).

Através da Lei 12.965 de 2014 – Marco Civil da Internet, a palavra “privacidade”

passou a constar no nosso ordenamento jurídico brasileiro e ao entrar em vigor em 2014, a internet no Brasil começou a ser melhor disciplinada, prevendo como princípios a proteção da privacidade e dos dados pessoais, na forma da lei, em seu Artigo 3º, incisos II e III, bem como direitos e garantias aos usuários em seu Artigo 7º e seguintes.

> A Lei 12.965/2014, conhecida como Marco Civil da Internet/MCI, inaugurou uma normativa específica para os direitos e garantias do cidadão nas relações travadas na Internet. O MCI foi, aliás, uma reação da sociedade civil contra um movimento legislativo que pretendia regulamentar a Internet no Brasil por meio de leis penais. Nesse sentido, o MCI procurou, de forma principiológica, assegurar os direitos e garantias do cidadão no ambiente eletrônico, sendo o seu traço marcante a distância de uma técnica normativa prescritiva e restritiva das liberdades individuais, própria do âmbito criminal, que poderia ter efeitos inibitórios para a inovação e a dinamicidade da Internet. (BIONI, 2020, online)

Em 2016, na Europa, o *General Data Protection Regulation* – GDPR foi aprovado e em 2018 ele entrou em vigor. Com isso, o Brasil se viu pressionado a “agilizar a votação de um projeto de lei de dados pessoais, caso contrário as empresas brasileiras teriam enorme dificuldade em realizar negócios com europeus” (MACIEL, 2019, online).

Para fins de contextualização, antes da criação da GDPR, foi criada em meados da década de 90, mais precisamente em 1995, a Diretiva nº 46 da União Europeia, visando a proteção de dados pessoais e por mais que não tivesse força legal perante os países membros, serviu como base para legislações nacionais e os seus princípios mais relevantes foram mantidos no GDPR.

Por fim, após inúmeras leis criadas com o intuito de proteger a privacidade humana, e diante da necessidade de regulamentar a proteção dos dados pessoais, visto que os demais países do mundo já haviam se posicionado e regulamentado esse assunto em suas legislações, o Brasil sancionou em 2018 a Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018, influenciada diretamente pelo GDPR – *General Data Protection Regulation*.

> Em 2018 então, o Brasil passou a entrar no rol de países com uma legislação voltada à proteção de dados pessoais, claramente inspirada no regulamento europeu. Com vigência inicialmente prevista para o dia 16 de fevereiro de 2020, com a edição da Medida Provisória nº 869/18, tal prazo foi estendido por seis meses, passando para agosto do mesmo ano. (MACIEL, 2019, online).

Por muito tempo não se via o assunto “proteção aos dados pessoais” como algo que deveria ter muita relevância, pois existe um mercado de dados pessoais no Brasil e no mundo. Muitas empresas ganharam relevância no mercado porque passaram a

conhecer melhor o seu cliente, seus gostos musicais, os filmes que mais assiste, as plataformas que mais acessa e com esse conhecimento acerca do público-alvo, foi possível elaborar estratégias de marketing mais direcionadas, como por exemplo campanhas personalizadas por idade, sexo e características do comportamento.

Como não havia uma legislação específica que garantia aos titulares, proteção de seus dados pessoais, ao longo dos anos estes passaram a ser fundamentais para as empresas compreenderem melhor os seus clientes e suas necessidades e assim oferecer-lhes os devidos serviços, bem como os anúncios direcionados.

> O mercado de dados pessoais é cada vez mais relevante na sociedade informacional e pode ser entendido como as interações econômicas voltadas à compra e venda das informações relativas a uma pessoa identificada ou identificável, direta ou indiretamente. O mercado de dados pessoais se baseia nas necessidades de informação das empresas, instituições públicas e usuários finais. (SILVEIRA, AVELINO, SOUZA, 2016, p.219)

Diante do exposto, percebe-se que a trajetória da proteção de dados pessoais no Brasil é extensa e com uma larga lista de leis específicas. Mas como já foi dito, o Direito Digital não possui um Código específico, pois ele é baseado em comportamentos e influenciado diretamente pelo Direito Internacional. Portanto, foi necessário estudar toda essa trajetória, para se perceber a importância da Lei Geral de Proteção de Dados Pessoais e estudá-la com maior clareza.

2 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LEI Nº 13.709/2018

A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais é aquela que regulamenta o uso de dados pessoais por empresas, Poder Público, ou mesmo por pessoas físicas que possuem interesse econômico. Ela tem a finalidade de proteger os direitos fundamentais.

> A LGPD surge com o intuito de proteger direitos fundamentais como privacidade, intimidade, honra direito de imagem e dignidade. Pode-se pontuar também que a necessidade de leis específicas para a proteção dos dados pessoais aumentou com o rápido desenvolvimento e expansão da tecnologia no mundo, como resultado dos desdobramentos da globalização, que trouxe como uma de suas consequências o aumento da importância da informação. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder. (PECK, 2020, p. 70)

Sendo assim, com a evolução constante das tecnologias, a Lei Geral de Proteção de Dados Pessoais demonstra a importância de o titular dos dados pessoais entender que ele é o verdadeiro dono destes. Esse assunto é tão importante, que o documentário *The Social Dilemma*, da Netflix, trouxe a seguinte frase:

> *There are only two industries that call their customers 'users': ilegal drugs and software. - Edward Tufte*
>
> Existem apenas duas indústrias que chamam seus clientes de usuários: a de drogas e a de software. - Edward Tufte

A informação sempre deu poder para aqueles que a possuem e por isso que a regulamentação de como, quando e onde os dados pessoais estão sendo usados é tão importante. As pessoas precisam saber como essa indústria funciona, porque:

> "*Personal data is the new oil of the Internet and the new currency of the digital world*" - Meglena Kuneva, European Consumer Commisioner, March, 2009
>
> Dado Pessoal é o novo óleo da Internet e a nova moeda do mundo digital. - Meglena Kuneva, Comissária do Consumidor Europeu, Março, 2009

2.1 INTRODUÇÃO AOS DADOS PESSOAIS

Para se falar de dados pessoais, é preciso falar um pouco sobre personalidade. Entende-se por personalidade, as particularidades ou o conjunto de particularidades que diferenciam uma pessoa da outra.

Os direitos da personalidade, ao longo da história, passaram por diversas mudanças até se tornarem juridicamente tutelados. Orlando de Carvalho, ensina:

> A noção-chave da disciplina civilista é, a dos direitos da pessoa, a dos direitos subjetivos em função da realização dos mencionados direitos da pessoa, isto

> é, o poder dos homens de espontaneamente estabelecerem a disciplina da sua quotidiana convivência. (CARVALHO, 1981, p.30)

O ser humano se desenvolve em comunidade, se conecta com pessoas que possuem o mesmo estilo de vida, o mesmo gosto musical, ou seja, o indivíduo se desenvolve intelectualmente, fisicamente, emocionalmente e espiritualmente com aqueles que se identifica. Isso tudo forma a base da personalidade do indivíduo, pois define quem ele é e, portanto necessitam de tutela jurisdicional perante o ordenamento jurídico brasileiro, e entre eles, o ordenamento civilista.

Os direitos da personalidade possibilitam o desenvolvimento do ser humano em comunidade e possuem tutela jurisdicional perante o Código Civil, em seu rol *numerus apertus*, ou seja, um rol aberto. Por não serem direitos que se exaurem naquelas espécies elencadas nos artigos 11 ao 21 do Código Civil, isso gerou a possibilidade de reconhecimento da proteção dos dados pessoais como um novo direito da personalidade.

> A função dos direitos da personalidade é promover e assegurar o valor-fonte do ordenamento jurídico, a pessoa humana que se encontra respaldada por um sistema ou uma cláusula geral de proteção. Essa orientação é energizada pela concepção de um direito privado despatrimonializado ou repersonalizdo. (BIONI, 2020, online)

A intenção deste trabalho não é aprofundar em direitos da personalidade, mas demonstrar que o ordenamento jurídico brasileiro está aberto a novas maneiras de garantir a proteção do ser humano, pois como já dito, a sociedade está em constante evolução, sempre com novas tecnologias e o Direito precisa acompanhar os novos desafios que surgem.

A quantidade de características que particularizam o indivíduo é imensa, como por exemplo, nome, endereço, CPF, RG, e-mail, fotos, gostos musicais, dentre tantos outros. Essas particularidades podem ser consideradas dados pessoais, ou seja, toda e qualquer informação que seja capaz de identificar ou tornar identificável, uma pessoa. Portanto, os dados pessoais precisam ser protegidos pela jurisdição brasileira, a fim de garantir segurança ao titular dos dados.

Até pouco tempo, o ordenamento jurídico brasileiro não contava com uma lei que disciplinasse sobre o que são dados pessoais, e como eles devem ser tratados, de maneira clara e específica.

2.2 ENTENDENDO A LEI Nº 13.709/2018

2.2.1 Conceito e vigência

Visando proteger esses dados pessoais, foi criada a Lei nº 13.709/2018, chamada de Lei Geral de Proteção de Dados Pessoais – LGPD, a fim de tratar a deficiência existente no ordenamento jurídico brasileiro. A Lei Geral de Proteção de Dados Pessoais foi totalmente influenciada pelo *General Data Protection Regulation* (GDPR), o regulamento da União Europeia sobre o tema.

> A LGPD decorre de uma imperatividade contemporânea, eis que a mudança do centro de consumo e das interações sociais do plano exclusivamente "analógico" para o ambiente digital interconectado pela rede mundial de computadores forçou a adaptação de regras jurídicas para esta nova realidade; garantindo assim, o império da lei tanto à luz da constatação de que a informação, conceitualmente considerada, é hoje um ativo com um autêntica atribuição mercantil e exploração "monetizável". (TEIXEIRA, MAGRO, 2020, p. 35)

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, de acordo com o Artigo 1º da Lei nº 13.709 de 14 de agosto de 2018.

A referida lei foi publicada em 14 de agosto de 2018 e o legislador determinou que a *vacatio legis* seria de 18 meses. Após, a vigência da Lei 13.853/2019, esse prazo foi alterado para 24 meses, ficando determinado que a LGPD entraria em vigor em 16 de agosto de 2020.

Durante o ano de 2020, a LGPD foi objeto de vários projetos de lei. Em 30 de março de 2020, foi criado o PL 1.179/2020, com o objetivo de prorrogar a vigência da LGPD para 1º de janeiro de 2020 e as sanções aplicáveis para 1º de agosto de 2020.

Em 29 de abril de 2020 foi publicada a MP 959/2020 que, em seu artigo 4º prorrogava a vigência da Lei nº 13.709/2018 para 3 de maio de 2021.

Em 14 de maio de 2020, a Câmara dos Deputados aprovou o texto do PL 1.179/2020 quanto as sanções, para que estas sejam aplicáveis a partir de agosto de 2021. No que se refere à vigência, aguardou-se a apreciação da MP 959/2020. Em 19 de maio de 2020, o Senado Federal manteve a redação da Câmara dos Deputados quanto as sanções. Quanto a vigência, votou pelo texto original da LGPD, ou seja, agosto de 2020.

Em 10 de junho de 2020 foi sancionada a Lei nº 14.010/2020 que altera a Lei nº 13.709/2018 (LGPD), determinando que as sanções previstas na lei sejam aplicáveis

a partir de 1º de agosto de 2021.

Em 25 de agosto de 2020, a Câmara dos Deputados votou a MP 959/2020, estabelecendo que a vigência da LGPD fosse para o dia 31 de dezembro de 2020.

Mas, no dia 26 de agosto de 2020, o Senado Federal votou e aprovou a MP 959/2020, porém sem o artigo de adiamento da vigência, alegando que a matéria já havia sido votada anteriormente. Por fim, em 18 de setembro de 2020 a Lei Geral de Proteção de Dados Pessoais entrou em vigor, com o sancionamento pelo Presidente da República da lei 14.058 de 17 de setembro de 2020.

2.2.2 Terminologia

A LGPD é uma lei principiológica e possui três pilares importantes: uso legítimo, segurança e governança.

Por uso legítimo, entende-se o uso correto dos dados pessoais, obedecendo as regras impostas pela LGPD, respeitando a vontade do titular. Por segurança, entende-se que as instituições públicas e privadas, e em alguns casos pessoas físicas, precisam procurar medidas que garantam a proteção dos dados pessoais confiados a elas. Por fim, entende-se que governança é uma estrutura criada pelas instituições privadas e públicas juntamente com sua equipe para lidar com os dados pessoais e enfrentar os novos desafios que irão surgir. (MARQUES, online, 2020).

O Artigo 5º da LGPD traz 19 (dezenove) conceitos de termos usados ao longo de seu texto. Porém, para facilitar a interpretação deste trabalho, abaixo estão alguns termos que mais serão mencionados. Veja:

a) **Dados pessoais:** é toda informação relevante sobre uma pessoa, ou seja, informação que faça com que aquela pessoa seja identificada ou identificável. Tem-se como exemplos: nome, sobrenome, e-mail, endereço etc.

b) **Dados pessoais sensíveis:** é toda informação que esteja relacionada a personalidade do indivíduo e suas escolhas pessoais. Tem-se como exemplos: opinião política, dados sobre saúde ou vida sexual, dados genéticos ou biométricos, religião, dentre outros.

c) **Dados anonimizado:** não são dados pessoais. São dados referentes a um indivíduo que não pode ser identificado, levando em consideração os meios disponíveis no momento de seu tratamento.

d) **Titular:** é o indivíduo, dono dos dados pessoais. É aquele que possui as

informações prestadas para tratamento de dados.

e) **Tratamento de dados pessoais:** é toda operação realizada com os dados pessoais.
f) **Agentes de tratamento:** são aqueles que tratam os dados pessoais, por meio de alguma operação. A lei traz dois agentes: o controlador e o operador. Controlador é aquele que recepciona os dados pessoais dos titulares por meio de consentimento ou das bases legais de exceção. O operador é aquele que realiza o tratamento de dados pessoais, seja por obrigação legal ou por contrato. Um ponto importante a ser falado aqui, é que o controlador deverá indicar o encarregado pelo tratamento dos dados pessoais, nos termos do Artigo 41 da lei.
g) **Consentimento:** é a manifestação de vontade do titular de permitir ou não o tratamento dos dados. Esse tópico será abordado com mais profundidade mais a frente, mas vale ressaltar que não é a única forma que autoriza o tratamento de dados.

> A especificação dos termos utilizados no contexto dos dados pessoais é particularmente importante e visa resolver os problemas de conceituação e até mesmo categorização que as informações coletadas sofriam. A partir da LGPD, passa a ficar claro e apontável o que é ou não dado pessoal, assim como todos os processos, as técnicas ou os procedimentos relativos ao tratamento de dados. (PECK, 2020, p.80)

2.2.3 Princípios

O artigo 6º da LGPD (Lei nº 13.709/2018) traz um rol com 10 (dez) princípios que devem ser seguidos quando os dados pessoais são tratados, bem como a boa-fé. Entretanto, entende-se que os principais princípios que regem a LGPD são: princípio da transparência, princípio da necessidade e princípio da finalidade.

Conforme artigo 6º, inciso I da Lei nº 13.709 de 14 de agosto de 2018, por princípio da finalidade entende-se ser a:

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

Conforme artigo 6º, III da Lei nº 13.709 de 14 de agosto de 2018, por princípio da necessidade entende-se ser a:

> III - 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.

Conforme artigo 6º, inciso VI da Lei nº 13.709 de 14 de agosto de 2018, por princípio da transparência, entende-se ser a:

> VI - 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.

Portanto, ao realizar o tratamento de dados pessoais, o agente de tratamento precisa levar em consideração todos os princípios expostos no artigo supramencionado, entretanto deve dar ênfase a esses três: finalidade, necessidade e transparência.

A Lei Geral de Proteção de Dados Pessoais foi criada para o titular, mas se comunica o tempo todo com os agentes de tratamento. Isso ocorre porque ao longo dos anos foi desenvolvido um pensamento de que as empresas privadas ou públicas são proprietárias dos dados pessoais dos usuários, entretanto a LGPD veio para desmistificar esse pensamento e deixar claro para todos que o único proprietário dos dados pessoais, é o próprio titular.

Pode parecer que seguir à risca esses princípios, prejudique o desenvolvimento econômico do país. Mas não se deve seguir essa linha de raciocínio. Quando as instituições privadas e públicas explicam para o titular o que está sendo feito com os dados pessoais dele, como e porque serão tratados, deixando claro sua finalidade e solicitando apenas os dados necessários, por consequência, o relacionamento entre o agente de tratamento e o usuário irá se solidificar.

Isso significa que em uma relação de consumo, por exemplo, o usuário-consumidor, quando sabe o que a empresa está oferecendo e porque ela precisa daqueles dados pessoais, a tendência é que aquele consumidor se torne um cliente fiel. Então, o que parece ser algo preocupante e prejudicial, na verdade, a longo prazo será de grande valia para todos. A ideia da legislação é fazer com que a sociedade se torne mais consciente.

2.2.4 Territorialidade

O critério de aplicação da LGPD é territorial e não possui ligação com nacionalidade. Isso significa que não é porque o usuário é brasileiro que os seus dados pessoais serão tratados conforme a LGPD determina. O que deve ser analisado é se os dados pessoais daquele usuário passaram pelo território brasileiro ou estão

em solo brasileiro.

Conforme o Artigo 3º da LGPD, deve ser verificado as seguintes situações:

A) Os dados pessoais podem ter sido tratados dentro do território brasileiro;

B) O tratamento de dados pode ter começado no Brasil e ter sido destinado para outro país (território);

C) O tratamento de dados pode ter começado em outro território e ter sido destinado para o território brasileiro.

Portanto, o artigo supramencionado nos esclarece mais uma característica da lei, não importando a nacionalidade da pessoa física ou a sede da pessoa jurídica. Se de alguma maneira os dados pessoais foram tratados em território brasileiro, a eles se aplicam a LGPD.

2.2.5 Direito à privacidade e à informação

Quando se trata do direito à privacidade, sabe-se que é um direito fundamental previsto no artigo 5º, X da Constituição Federal, que prevê a inviolabilidade da "intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente da sua violação".

A vida privada também é protegida pelo Código Civil, em seu artigo 21, que dispõe: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

No mesmo sentido, a proteção da privacidade também é considerada um princípio da "disciplina do uso da internet no Brasil" pelo Marco Civil na Internet (Lei nº 12.965/2014) em seu artigo 3º, II.

Com o surgimento da LGPD esse posicionamento não poderia ser diferente. Em seu artigo 2º, disciplina os fundamentos da proteção de dados e logo no inciso I vem "o respeito à privacidade". Portanto, é visível a importância da proteção à privacidade no ordenamento jurídico brasileiro.

Os termos vida privada, privacidade e intimidade não devem ser usados como sinônimos, é necessária uma atenção quanto a isso. Por vida privada entende-se como a esfera que as pessoas possuem mais acesso à informação, acontecimentos de vida, vontades e afazeres do indivíduo, que opta por dividir com seus conhecidos e familiares distantes. (CONSALTER, 2017, p.127)

Por privacidade entende-se que é algo mais confidencial, mais íntimo, ou seja, são assuntos que o indivíduo divide apenas com amigos e familiares próximos. Por fim, a intimidade, é aquela que diz respeito a valores mais secretos e intrínsecos do indivíduo, aquilo que ele não divide com ninguém. (CONSALTER, 2017, p.127)

Tarcísio Teixeira e José Afonso da Silva, consideram que esses termos possuem o mesmo significado, pois consideram que o direito à privacidade inclui "todas as manifestações da esfera íntima, privada e da personalidade que o art. 5º, inc. X, da Constituição Federal consagrou: direito à intimidade, à vida provada, à honra e à imagem das pessoas". (SILVA, 1997, p. 202 apud TEIXEIRA, 2014, p. 71)

Sendo assim, cada indivíduo tem o direito de escolher quais dados pessoais podem ou não ser divulgados, de maneira que "todos indistintamente têm o dever de se abster de qualquer ato, público ou privado, que importe na divulgação não desejada da informação". (LUCCA, SIMÃO FILHO, LIMA, 2015, p. 507)

No que se refere ao mundo digital, a privacidade tem uma importância tremenda em razão da "maior quantidade de informações disponíveis, a enorme facilidade e a maior escala de intercâmbio de informações, os efeitos potencializados das informações errôneas e a duração perpétua dos registros". (MARTINS, 2014, p. 265)

Quando se trata do direito à informação, sabe-se que também é um direito fundamental previsto no artigo 5º, XIV e XXXII da Constituição Federal, que reconhece a possibilidade de o indivíduo obter informações a seu respeito, armazenadas em cadastros públicos e retificá-las quando for o caso.

> O dever-direito de informação é o primeiro instrumento para desencadear a referida perspectiva solidária das relações obrigacionais. Isso porque apenas com uma informação adequada o cidadão estará capacitado para controlar seus dados. O fluxo dos seus dados precisa tomar uma forma (ser informado), sendo pressuposto para que haja qualquer tipo de processo de tomada de decisão por parte do titular dos dados. (BIONI, 2020, online)

Esse direito está ligado ao Estado Democrático de Direito, tendo em vista que é o que norteia o direito de informar e de ser informado, a liberdade de expressão, o acesso à informação, e, inclusive, a proibição da censura, conforme prevê o artigo 220 da Constituição Federal. Viviane Nóbrega Maldonado explica que:

> [...] aos cidadãos em geral, é garantida a liberdade de informação sob a acepção de que podem, ativa e livremente, fornecer informações sob os limites da lei, anotando-se aqui a existência de circunstâncias especiais sobre as quais o sigilo é imperioso. E, de outra parte, a esses mesmos cidadãos é assegurado o direito de buscar e de acessar informações relevantes para o pleno exercício de seus direitos. (MALDONADO, 2017, p.69)

Assim como o direito à privacidade, a liberdade de expressão é garantida como

princípio do uso da internet no Brasil pelo Marco Civil da Internet em artigo 8º, I e na LGPD, está prevista no artigo 2º, III, o artigo que disciplina os fundamentos da proteção de dados.

> A Sociedade Digital já não uma sociedade de bens. É uma sociedade de serviços em que a posse da informação prevalece sobre a posse dos bens de produção. Essa característica faz com que a produção do Direito à Informação seja um dos princípios basilares do Direito Digital, assim como a proteção de seu contradireito, ou seja, do Direito à não informação. (PECK, 2016, p. 89)

É necessário entender que o direito de informar é um direito ativo, o direito de ser informado, é um direito passivo e o direito de não receber informação é um direito ativo e passivo. A questão da não informação protege a privacidade do indivíduo e deve se equilibrar essas relações para que a intervenção do Estado seja mínima, não necessitando de uma imposição de limites, a fim de não ferir o direito de liberdade de pensamento.

> Por todo o exposto, podemos afirmar que na era da Informação, o poder está nas mãos do indivíduo, mas precisa ser utilizado de modo ético e legal, sob pena de, no exercício de alguns direitos, estar-se infringindo outros, e isso não é tolerável em um ordenamento jurídico equilibrado. (PECK, 2016, p. 94)

2.3 TRATAMENTO DE DADOS PESSOAIS

É necessário pontuar que dados pessoais, dados pessoais sensíveis e dados anonimizado possuem conceitos diferentes e são tratados em capítulos diferentes na LGPD. Vale ressaltar que dado anonimizado não é dado pessoal, nem dado pessoal sensível, tendo em vista que este dado é incapaz de identificar alguém. O presente trabalho visa aprofundar apenas no que se refere a dados pessoais.

O tratamento dos dados pessoais está previsto no Artigo 7º da Lei n 13.709/2018, ou seja, a lei traz a forma que o agente (controlador e operador) pode tratar os dados pessoais.

O tratamento dos dados pessoais das crianças e dos adolescentes deverão ser realizados a fim de garantir seu melhor interesse, levando em consideração a Lei Geral de Proteção de Dados e a legislação pertinente (artigo 14), qual seja, o Estatuto da Criança e do Adolescente. Entretanto, não é o objetivo deste trabalho trazer de forma aprofundada os direitos e garantias da criança e do adolescente perante a Lei Geral de Proteção de Dados, tendo em vista ser um assunto com dimensões para um outro estudo.

2.3.1 Bases legais da Lei

Para que os dados pessoais sejam tratados de forma correta, a LGPD traz 10 (dez) hipóteses de bases legais que autorizam o tratamento, nos incisos do Artigo 7º:

A) Mediante o fornecimento do consentimento do titular;

B) Para o cumprimento de obrigação legal ou regulatória pelo controlador;

C) Pela Administração Pública para execução de políticas públicas;

D) Realização de estudos por órgãos de pesquisas;

E) Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja a parte o titular;

F) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

G) Proteção da vida ou da incolumidade física do titular ou de terceiros;

H) Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

I) Necessário par atender aos interesses legítimos do controlador ou terceiros;

J) Para proteção do crédito;

O artigo 7º é taxativo e exaustivo, e as bases legais deixam claro sua utilização. Vale ressaltar que as bases legais podem ser cumuladas e elas modulam o tempo, ou seja, o tratamento de dados pode começar com uma base, se manter com outra e finalizar com uma terceira. É necessária uma análise cautelosa.

Mesmo o rol do artigo 7º ser de fácil compreensão, existem duas bases legais que merecem um estudo mais aprofundado e maior atenção, tendo em vista os seus requisitos.

A primeira base, é a do consentimento (Artigo 7º, I da referida Lei), uma vez que este valida a própria vontade dos titulares dos dados, contanto que preencha os seguintes requisitos, de maneira concomitante: ser prévio, livre, informado, inequívoco e revogável. Vale ressaltar que se os dados tornarem manifestadamente públicos pelo titular (artigo 7º, § 4º), a exigência do consentimento é dispensada, resguardos seus direitos e os princípios da LGPD.

> O titular dos dados pessoais alçou papel de protagonista a partir da segunda geração de leis de proteção de dados pessoais. Naquele momento, optou-se por uma estratégia regulatória que nele depositava a responsabilidade de auto proteger as suas informações pessoais. essa diretriz normativa foi fundada a partir do direito de o indivíduo controlar os seus dados pessoais, socorrendo-se, por isso, à técnica legislativa de exigir o consentimento do

> titular dos dados pessoais para que eles fossem coletados, utilizados, compartilhados, enfim, para toda e qualquer etapa de tratamento de tais informações. (BIONI, 2020, online)

O agente de tratamento de dados pessoais tem que deixar claro quais são as finalidades daquele tratamento, pois o consentimento será vinculado àquela(s) finalidade(s) exposta(s).

Não há um conceito claro do que seja consentimento “livre, informado e inequívoco”, porém como já foi mencionado neste trabalho, a LGPD foi totalmente influenciada pela GDPR – *General Data Protection Regulation* e essa discussão foi abordada em uma de suas diretrizes, a *Guideline 05/2020* que, dentre outros assuntos, aborda sobre o consentimento e o desiquilíbrio de poder em dois aspectos: nas relações de emprego e no tratamento de dados realizado pelo Poder Público.

Desequilíbrio de poder é a posição hierarquicamente superior do controlador de dados pessoais perante o titular. Nesse caso, seria pertinente a busca de outras hipóteses para justificar o tratamento de dados, a fim de mitigar os possíveis riscos.

Sendo assim, como há uma certa omissão da legislação na definição de “livre, informado e inequívoco”, o juiz decidirá de acordo com as fontes do direito, jurisprudências, doutrinas, legislações em âmbito internacional e o que mais o ordenamento jurídico brasileiro lhe oferecer.

Se o consentimento (Artigo 7º, I) for obtido por escrito, o artigo 8º, § 1º nos esclarece que é necessária uma cláusula destacada das demais cláusulas contratuais, tratando sobre esse consentimento que será dado, seguindo todas as regras exigidas pela Lei Geral de Proteção de Dados Pessoais.

> [...] Nesse sentido, garantir que as pessoas/usuários tenham ciência de que devem consentir o uso dos dados, assim como tenham direito de saber a finalidade da coleta e acesso ao seu conteúdo em qualquer momento, é primordial para assegurar a liberdade e a privacidade. (PECK, 2020, p. 85)

Isso possui uma conexão com o parágrafo seguinte (Artigo 8º, § 2º), pois este determina a inversão do ônus da prova. Para a LGPD, é o controlador que tem o ônus de provar que requereu o consentimento do titular, nos exatos termos da referida lei.

> É vedado o tratamento de dados pessoais mediante vício de consentimento. O consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência de forma clara e inequívoca. (CAVALCANTE, 2018, p. 68)

Como já mencionado aqui, a LGPD tem o objetivo de desmistificar a ideia de que os dados pessoais são das empresas. Os dados pessoais foram e são do titular.

Enfim, o consentimento pode ser revogado a qualquer tempo mediante manifestação expressa do titular, e o procedimento deve ser gratuito e facilitado.

A segunda base legal a ser pontuada é a do interesse legítimo (Artigo 7º, IX). Essa é uma das bases legais que não necessita de consentimento e ao ler o inciso IX, parece ser um tratamento de dados mais simples.

Nesta base legal, o legislador também não conceituou o que seria “interesse legítimo”, deixando um conceito aberto capaz de se adequar as mais diversas hipóteses.

Mas isso não significa que o uso dessa base legal pode ser feito de qualquer maneira. Ela possui os seguintes requisitos: legitimidade do interesse, necessidade, balanceamento e precauções. Esses requisitos são cumulativos e devem estar necessariamente presentes para utilização dessa base legal.

Entende-se por legitimidade do interesse (artigo 10, *caput* e I da LGPD), aquela que é especificada, devidamente informada e faz sentido para o titular de dados. Deve-se analisar também se o uso dos dados possui alguma finalidade econômica para o controlador, bem como se há uma “situação em concreto”. Quanto mais bem descrita a situação, mais fácil será analisar se há legítimo interesse.

Feito isso, deve ser verificado se os dados coletados são minimamente necessários para a realização da finalidade pretendida. É uma base de exclusão, ou seja, deve ser usada quando as demais hipóteses do artigo 7º não forem possíveis.

> O fio condutor de toda essa avaliação é “balancear” os direitos em jogo. De um lado, do titular dos dados e, de outro lado, de quem faz uso das suas informações. Tão importante quanto aferir se há um interesse legítimo é verificar se as legítimas expectativas e os direitos e liberdades fundamentais do cidadão serão respeitados. (BIONI, 2020, online)

O terceiro passo e o principal é o balanceamento (artigo 10, II). Já verificados os dois passos supracitados, deve-se verificar se o novo uso atribuído ao dado está de acordo com as expectativas legítimas do titular de dados, ou seja, o uso adicional dos dados deve ser compatível com o uso primário, sempre levando em conta o princípio da finalidade. Ato contínuo, é necessário demonstrar de que forma os titulares serão impactados, especialmente os efeitos negativos que podem surgir, no sentido de descriminação e sobre a sua autonomia. Caso, mas não obrigatoriamente, o tratamento de dados também os beneficie, há o equilíbrio. (BIONI, 2020, online)

O desafio para justificar o uso dessa base legal fica em entender o que poderia ser legítimo interesse, dada a subjetividade deixada pelo legislador e a desnecessidade

do consentimento do titular. Desta forma, como uma forma de marcar sua utilização, além dos requisitos cumulativos e necessários, deve-se levar em consideração a razoabilidade e a proporcionalidade.

Por fim, as precauções tomadas devem ser a transparência e a minimização dos riscos ao titular do dado (artigo 10, §§ 2º e 3º), sendo a transparência em primeiro lugar, o poder de decisão par se opor ou "sair" de tal atividade de tratamento de dados (*opt-out)*, como segundo; e ações que amenizem os riscos adotadas pelo controlador, como terceira.

> Ao mesmo tempo, as empresas devem ter a liberdade de utilizar os dados de maneira transparente e ética em troca de um serviço ou acesso, tendo em vista que o desenvolvimento econômico também deve ser garantido a esses sujeitos. Importante destacar que cabe à instituição que realiza o tratamento a capacidade de demonstrar que estava legítima (detinha o registro do consentimento ou se enquadrava nas hipóteses de exceção). (PECK, 2020, p.85/86)

2.3.2 TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Assim como as instituições privadas precisam se adequar à Lei Geral de Proteção de Dados, a pessoa jurídica de direito público também precisa, devendo levar em consideração a finalidade e o interesse público.

> O interesse público pode ser compreendido como produto das forças de uma dada sociedade (jurídicas, políticas, econômicas, religiosas, dentre outras) concretizadas em certo momento e espaço que exprime o melhor valor de desenvolvimento de um maior número possível de pessoas dessa mesma sociedade. Então, alcançar esse produto, considerando as forças de uma sociedade, é o dever primordial do Estado, conforme o art. 3.º da CF.
> [...]
> Assim definido, urge raciocinar que a atuação estatal – em destaque, da Administração Pública – precisa estar intimamente conectada com a realização e a promoção de um interesse público concreto, ou concretizável. (FRANÇA, 2016)

A partir do Artigo 23, inicia-se o capítulo referente ao tratamento de dados pessoais pelo Poder Público. A lei especifica como pessoas jurídicas de direito públicos aquelas descritas no Artigo 1º da Lei nº 12.527 de 2011, conhecida como Lei de Acesso à Informação.

> Trazendo o exposto para a redação do art. 1º da Lei de Acesso à Informação, verifica-se que Administração Pública direta é composta por todos os órgãos dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, o Judiciário e o Ministério Público. Da mesma maneira, a referida Lei estabelece que a Administração Pública indireta será composta pelas autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.
> Assim, infere-se que o Poder Público pode ser encontrado nos poderes da União, Distrito Federal, Estados e Municípios, por meio dos serviços e das

> atividades desempenhadas, a partir das competências designadas pela estrutura administrativa. (TEIXEIRA, MAGRO, 2020, p. 122.)

Entretanto, as instituições públicas poderão seguir procedimentos e prazos apontados por leis específicas (artigo 23, § 3º da referida lei).

O Conselho Nacional de Justiça, já se posicionou e publicou a Recomendação nº 73 de 20 de agosto de 2020, para orientar o Judiciário a instituir um padrão nacional de proteção dos dados pessoais existentes nas suas bases. Também publicou a Resolução 331/2020 que trata sobre a Base Nacional de Dados do Poder Judiciário – DATAJUD, progredindo a ideia de criação de um banco de dados público, resguardados o sigilo e a confidencialidade das informações.

Foi publicado ainda a Resolução 332/2020 que dispõe sobre ética, transparência e a governança na produção e no uso de Inteligência Artificial no Poder Judiciário e dá outras providências.

Portanto, a Lei Geral de Proteção de Dados traz de maneira clara, que tanto as instituições privadas quanto as públicas, precisam informar a finalidade do tratamento de dados pessoais, bem como respeitar os direitos e garantias do titular, salvo as exceções previstas em lei.

2.4 DIREITOS DO TITULAR

> “O direito dos titulares dos dados de livre acesso às informações relativas ao tratamento é reiterado de maneira enumerativa no art. 18, cuja preocupação é garantir que o titular possa assegurar que os seus dados estão sendo tratados de forma segura, verídica e cumprindo a sua finalidade.” (PECK, 2020, p. 101)

Deve ficar claro que os dados pessoais fornecidos pelo titular não devem se confundir com o banco de dados que as empresas possuem. A LGPD foi assertiva ao deixar claro os limites do sigilo comercial e industrial, mas reservado ao titular a escolha do que fazer com os seus dados pessoais. É importante entender essa diferenciação, porque nem sempre vai ser possível se desfazer das combinações de dados pessoais existentes. Essa ideia seria quase utópica.

> Qual a importância disso? É que determina toda uma dinâmica que irá impactar o ciclo de vida da informação quando os dados pessoais passarem a integrar uma base de dados e esta, por sua vez, vir a integrar outras. Em um dado momento é praticamente impossível desfazer todas as combinações e composições que já tiveram os dados pessoais coletados originalmente, de forma legítima. (PECK, 2016, p. 486)

O artigo 20 esclarece que o titular tem o direito de solicitar a revisão de decisões

tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinas a definir o seu perfil pessoal, profissional, consumerista e de crédito ou os aspectos de sua personalidade.

Por fim, o artigo 21 e 22 reforçam o que já foi mencionado neste trabalho: o titular, ao exercer os seus direitos, não deve ser prejudicado, bem como deve ter assegurado o seu direito de acesso à justiça e defesa de seus direitos, conforme preceitua o Artigo 5º, XXXIV da Constituição Federal.

2.4.1 DIREITO AO ESQUECIMENTO E EXCLUSÃO DOS DADOS PESSOAIS

No que se refere ao direito ao esquecimento, Tarcísio Teixeira e Américo Ribeiro Magro, ensina que:

> O instituto do direito ao esquecimento, também conhecido como direito de ser deixado em paz, direito de estar só, direito ao apagamento e direito de apagar, garante ao indivíduo que informações relacionadas à sua pessoa não se perpetuem indeterminadamente em domínio público, de forma que possa viver “sem máculas do passado, sob a invocação do princípio da dignidade humanam de tal modo, permite que haja a remoção de dados pretéritos que já não possuam interesse público. (TEIXEIRA, MAGRO, 2020, p.102)

O direito ao esquecimento foi devidamente reconhecido pela VI Jornada de Direito Civil, em seu Enunciado 531 que determina: “A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento”.

A finalidade do Enunciado 531 é remediar qualquer dano provocado pelas novas tecnologias que popularizam a informação, com o intuito de dar segurança do direito de ressocialização sem qualquer ligação com os fatos ocorridos no passado. Com isso, o direito à privacidade e o direito à informação serão protegidos e aplicados de maneira ponderada.

Portanto, para que o direito ao esquecimento seja aplicado, é necessária uma decisão judicial determinando que as informações acerca daquela pessoa sejam retiradas do meio público, da Internet. A retirada dessas informações da Internet não é algo simples de ser feito, pois envolve armazenamento de dados em servidores do mundo todos e em alguns países, e em alguns lugares o entendimento acerca de política de privacidade são divergentes do entendimento do Brasil. Entretanto, não se deve confundir direito ao esquecimento com eliminação de dados pessoais.

A eliminação dos dados pessoais está prevista no artigo 15 da Lei Geral de Proteção de Dados Pessoais e se enquadra como uma das formas de tratamento, nos

termos do Artigo 5º da referida Lei. A eliminação ocorre nas seguintes hipóteses:

> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - fim do período de tratamento;
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Portanto, o direito ao esquecimento é garantido a qualquer pessoa que deseja ter suas informações excluídas do meio público, em razão de algum fato vexaminoso ligado à sua vida e que afetou sua reputação de alguma forma, a fim de ser esquecida pela população após um lapso de tempo. A eliminação de dados pessoais é um direito garantido ao titular dos dados e existe desde a vigência do Marco Civil da Internet.

> O excesso de informações disponíveis e a facilidade ao seu acesso, principalmente em meio virtual, pode vir a acarretar prejuízos aos indivíduos titulares de dados pessoais, que muitas vezes são rejeitados em vagas de empregos, excluídos socialmente ou expostos em situações íntimas. Como uma tentativa de solução para esta problemática, a Lei nº 13.709/2018 determina aos controladores e operadores de dados pessoais que promovam a eliminação de dados pessoais na ocorrência do término de seu tratamento, salvaguardando algumas hipóteses de exceção. (TEIXEIRA, MAGRO, 2020, p.109)

O artigo 19 do Marco Civil da Internet – Lei nº 12.965 de 2014 garante ao usuário da internet, por meio de ordem judicial, a indisponibilidade do conteúdo apontado como infringente, ou seja, o direito ao esquecimento destas informações.

Já a Lei Geral de Proteção de Dados garante ao titular dos dados pessoais, após o término do tratamento, a exclusão dos dados tratados, mediante requerimento ao agente de tratamento, nos termos do Artigo 16 da referida Lei, ou seja, direito a exclusão.

Em julgado recente do Superior Tribunal de Justiça, a Terceira Turma julgou o REsp 1660168/RJ, esclarecendo que:

> [...] 4. Há, todavia, circunstâncias excepcionalíssimas em que é necessária a intervenção pontual do Poder Judiciário para fazer cessar o vínculo criado, nos bancos de dados dos provedores de busca, entre dados pessoais e resultados da busca, que não guardam relevância para interesse público à informação, seja pelo conteúdo eminentemente privado, seja pelo decurso do tempo. 5. Nessas situações excepcionais, o direito à intimidade e ao esquecimento, bem como a proteção aos dados pessoais deverá preponderar, a fim de permitir que as pessoas envolvidas sigam suas vidas com razoável anonimato, não sendo o fato desabonador corriqueiramente rememorado e perenizado por sistemas automatizados de busca. [...]. 9. Recursos especiais parcialmente providos.
> (REsp 1660168/RJ, Rel. Ministra NANCY ANDRIGHI, Rel. p/ Acórdão Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em

08/05/2018, DJe 05/06/2018)

Conclui-se que, o direito ao esquecimento vem sendo permitido a depender do caso concreto, do lapso temporal e outros fatores que podem influenciar a decisão judicial para se obter esse direito. E no que se refere ao direito de exclusão previsto pela Lei Geral de Proteção de Dados, com certeza haverá bastante discussão acerca deste direito e todos os campos que ele pode influenciar.

3 RESPONSABILIDADE CIVIL, SEGURANÇA E BOAS PRÁTICAS

Durante todo este trabalho, foi apontado os pontos importantes da Lei Geral de Proteção de Dados Pessoais, possibilitando o entendimento da importância da referida lei na Era da Informação, que é a que o Brasil e o mundo estão vivendo. Assim como os direitos do titular foram explicitados, os deveres e a responsabilidade dos agentes de tratamento também. Porém, ainda há um caminho longo a se percorrer, principalmente acerca de educação digital.

Assim como o Marco Civil da Internet trouxe a responsabilidade civil aos provedores de conexão à internet, a Lei Geral de Proteção de Dados Pessoais trouxe a responsabilidade civil para os agentes de tratamento nos artigos 42 ao 45.

> Condutas humanas trazem consigo a problemática da responsabilidade. Afinal, condutas humanas são hábeis a ocasionar danos e danos tem aptidão de impor dever de reparação. Nessa toada, a compreensão e o estudo da responsabilidade são essenciais a todo e qualquer operador do direito, quem, em última análise, busca responsabilizar ou afastar a responsabilidade. (FIGUEIREDO, FIGUEIREDO, 2020, p. 550)

O Código Civil Brasileiro, em seu Artigo 1º dispõe que toda pessoa é titular de direitos e deveres na ordem jurídica. Dentre esses deveres, existe o dever de não causar dano a outrem, bem como o dever de reparar o dano, já que aquele que causar o dano a outra pessoa fica obrigado a repará-lo (CC, art. 927).

Patrícia Peck (2016, p. 514) explica que, quando se trata de Responsabilidade Civil no Direito o Digital, a teoria do risco tem maior aplicabilidade, pois nasceu na era da industrialização e quando se trata de reparação de danos em que a culpa é dispensável, é a teoria que melhor se enquadra quando há responsabilidades mesmo que sem culpa, a depender do caso concreto.

> No Direito Digital, a responsabilidade civil tem relação direta com o grau de conhecimento requerido de cada prestador de serviço e do consumidor-usuário também. Nenhuma das partes pode alegar sua própria torpeza para se eximir de culpa concorrente. (PECK, 2016, p. 514)

A Lei Geral de Proteção de Dados Pessoais esclarece que o controlador ou operador que causa dano patrimonial, moral, individual ou coletivo, deve repará-lo. O artigo 42 da referida Lei preceitua que:

> O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

A legislação deixa claro a responsabilidade solidária do operador e controlador, quando descumprir as obrigações impostas pela lei. Assim, o Artigo 42, §1º prevê:

> § 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.

Uma observação importante a se fazer, é que o legislador não traz responsabilidade ao encarregado pelos danos provocados pelos controladores ou operadores aos titulares, mas o Artigo 42, § 4º preceitua que “aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.”

> [...] O objetivo da lei é dar maior efetividade nas indenizações aos titulares e, portanto, caberá aos agentes um cuidado redobrado na celebração dos contratos e definição das obrigações de cada parte, com mecanismos de controle e gerenciamento de forma a mitigar potenciais danos. (MACIEL, 2019, online)

Tendo em vista a importância de estar sempre em busca de mitigar os danos, o legislador trouxe apenas três hipóteses em que os agentes de tratamento não serão responsabilizados. Para que eles não tenham essa responsabilidade, é necessário que comprovem (artigo 43):

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

Vale ressaltar que no que se refere ao tratamento de dados feito pelo Poder Público, o legislador também traz formas de responsabilizar os agentes, caso haja alguma violação no tratamento de dados pessoais, conforme os artigos 31 e 32 da referida Lei. As instituições públicas têm a necessidade de prever o impacto de privacidade no âmbito da administração pública, pois a Lei Geral de Proteção de Dados Pessoais terá

grande impacto e exigirá muitas implementações.

> Os órgãos públicos estão sujeitos às medidas administrativas específica; em virtude disso, cabe à autoridade nacional garantir que as medidas cabíveis e proporcionais sejam adotadas quando da violação do tratamento de dados pessoais nos órgãos públicos. (PECK, 2020, p. 110)

Quando se tratar de relação consumerista, a Lei Geral de Proteção de Dados Pessoais determina que se houver violação dos direitos do titular, às regras de responsabilidade previstas no Código de Defesa do Consumidor e/ou Código Civil Brasileiro serão aplicadas (Artigo 45 da referida Lei).

Sendo assim, quando os direitos do titular forem violados, a responsabilidade e ressarcimento de danos é a medida trazida pelo legislador, evidenciando o direito fundamental à indenização pelo dano sofrido seja ressarcido, conforme prevê o Artigo 5º, incisos V e X da Constituição Federal.

Se houver dano, ele precisa ser reparado, para que não haja insegurança jurídica e para que a responsabilidade civil cumpra o seu papel de restabelecer o estado jurídico no qual o titular se encontrava antes de sofrer o dano. (FIGUEIREDO, FIGUEIREDO, 2020, p. 551 e 555).

3.1 BOAS PRÁTICAS, GOVERNANÇA E COMPLIANCE

A fim de evitar ou mitigar danos aos titulares, a Lei Geral de Proteção de Dados Pessoais, estabelece um capítulo VII intitulado “da segurança e das boas práticas”, composto de duas seções: “da segurança e do sigilo de dados” (artigos 46 ao 49) e “das boas práticas e governança” (artigos 50 e 51). É importante ressaltar que o legislador não deixou especificado, o termo “governança”.

> A governança de TI é uma parte da governança corporativa que cuida especificamente da tecnologia da informação, ou melhor, cuida dos resultados obtidos pela tecnologia da informação. Assim, a governança de TI garante instrumentos e ferramentas para que as diretrizes estabelecidas pela governança corporativa sejam cumpridas. (TEIXEIRA, MAGRO, 2020, p. 176)
> No âmbito da promoção da segurança da informação, os processos e procedimentos devem assegurar a disponibilidade, integralidade e confidencialidade de todas as formas de informação, ao longo de todo o ciclo de vida do dado. (PECK, 2020, p. 124)

As empresas precisam estar em busca de maneiras de garantir a segurança dos dados pessoais e demonstrar para o titular como isso é feito. Uma prática muito comum entre as empresas, é o uso da política de privacidade e termos de uso como forma de publicitar como é feito o tratamento de dados pessoais e a condições de uso

daquele site ou aplicativo, respectivamente.

O artigo 46 da legislação mencionada, preceitua que:

> Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Com a criação da Lei Geral de Proteção de Dados Pessoais e sua vigência, muito se tem falado em política de privacidade, pois existe a necessidade de adequação à legislação e também a interpretação errônea de que se adequar seria apenas mudar tal política com os requisitos exigidos por lei. Para esclarecer esse apontamento, necessário se faz lembrar do conceito de *compliance*.

> Destarte, ser c*ompliance* é conhecer as normas da organização, bem como seguir os procedimentos recomendados, agindo em conformidade e sentir quanto é fundamental a ética e a idoneidade em todas as nossas atitudes. Igualmente, estar em *compliance* é estar em conformidade com leis e regulamentos internos e externos. (TEIXEIRA, MAGRO, 2020, p. 188)

As empresas precisam estar em *compliance* com a legislação, ficando claro que a política de privacidade é apenas um dos documentos a ser providenciados durante a adequação à Lei Geral de Proteção de Dados Pessoais.

> Por isso, a proteção contratual do consumidor no âmbito das políticas de privacidade deve ser vista como o mecanismo ideal para a proteção dos dados pessoais. deve ser encarada como uma ação paliativa se a causa regulatória primária falhar, qual seja, o empoderamento *ex ante* do cidadão para exercer um controle genuíno sobre seus dados pessoais. (BIONI, 2020, online)

Dessa forma, para que as medidas de segurança, técnica e administrativas, mencionadas no Artigo 46 e seguintes da lei supramencionada sejam eficazes, é necessário que as empresas e seus agentes de tratamento de dados pessoais, estejam totalmente envolvidos com a proteção de privacidade, sempre viabilizando ao titular o uso fácil e tranquilo das tecnologias, a fim de cativar no usuário uma real capacidade de administrar seus dados pessoais.

> Isto posto, é preciso que as empresas adotem tanto procedimentos de governança, bem como estejam em *compliance* com a legislação, pois da mesma forma que a utilização da tecnologia e a manipulação dos dados pessoais podem trazer benefícios às empresas, inclusive para o aperfeiçoamento da gestão, há também os riscos e vulnerabilidades trazidos pela tecnologia apontada, com sanções que chegam até a R$ 50.000.000,00 (cinquenta milhões) de reais, conforme art. 52 da LGPD. (TEIXEIRA, MAGRO, 2020, p. 194)

3.2 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS – ANPD

A Autoridade Nacional de Proteção de Dados Pessoais – ANPD é o órgão da administração pública federal, integrante da Presidência da República, conforme disposição do Artigo 55-A da Lei Geral de Proteção de Dados Pessoais.

> A criação de uma autoridade de proteção de dados é, inclusive, um dos requisitos para considerar um país adequado para tratar dados sob o enfoque da legislação europeia, que prevê além da existência de um sistema jurídico protetivo, também a existência de autoridades de controle. (MACIEL, 2019, online)

O Decreto nº 10.474 de 26 de agosto de 2020, aprova a estrutura da Autoridade Nacional de Proteção de Dados Pessoais – ANPD.

O Artigo 1º do referido Decreto, dispõe que:

> Art. 1º A Autoridade Nacional de Proteção de Dados - ANPD, órgão integrante da Presidência da República, dotada de autonomia técnica e decisória, com jurisdição no território nacional e com sede e foro no Distrito Federal, tem o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, orientada pelo disposto na Lei nº 13.709, de 14 de agosto de 2018.

Um ponto muito importante trazido pela Lei Geral de Proteção de Dados Pessoais e reforçado no decreto que estruturou a Autoridade Nacional de Proteção de Dados Pessoais, é a preservação do segredo empresarial e do sigilo das informações (artigo 1º, § 5º do Decreto e Artigo 55-J, II da Lei).

A Autoridade Nacional de Proteção de Dados Pessoais – ANPD, possui 24 (vinte e quatro) competências, conforme dispõe o artigo 2º do Decreto nº 10.474/2020. Segue abaixo algumas:

> 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 da Lei nº 13.709, de 2018;
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
> XIV - consultar os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e seu planejamento;
> 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, empresas de pequeno porte e iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem **startups** ou empresas de inovação possam adequar-se ao disposto na Lei nº 13.709, de 2018;
> XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos da Lei nº 13.709, de 2018, e da Lei nº 10.741, de 1º de outubro de 2003 - Estatuto

> do Idoso;

Dessa forma, a estruturação da Autoridade Nacional de Proteção de Dados Pessoais demonstra ser um passo na segurança dos dados pessoais como o direito da personalidade, tendo em vista que ter um órgão fiscalizador, incluirá o Brasil no contexto de informação e economia global, principalmente no que se refere a transferência de dados pessoais para a União Europeia. E é uma maneira de solucionar conflitos de maneira mais ágil, quando comparada à apreciação pelo Poder Judiciário. (TEIXEIRA, MAGRO, 2020, p. 224)

3.2.1 SANÇÕES ADMINISTRATIVAS

Quando se fala em Lei Geral de Proteção de Dados Pessoais, quase sempre se fala primeiro das sanções previstas por ela. Esse tópico da legislação, tem sido fato gerador que obriga as instituições a se adequarem a lei. Entretanto, deve-se lembrar que apesar das sanções com valor aquisitivo elevado, a adequação feita irá garantir à empresa uma confiança de seus consumidores, gerando oportunidade de mercado. A verdadeira intenção é se adequar para se valorizar perante o mercado consumidor. (MACIEL, 2019, online)

Além da responsabilidade civil pelo tratamento inadequado realizado pelos agentes, a legislação também prevê sanções administrativas. O artigo 52 preceitua que as sanções são:

> 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;
> VII – VETADO
> VIII – VETADO
> IX – VETADO
> 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; (Incluído pela Lei nº 13.853, de 2019)
> 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; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a

> tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

Após o procedimento administrativo e oportunizada a ampla defesa, as sanções poderão ser aplicadas de forma gradativa, isolada ou cumulativa, conforme o caso concreto, seguindo os seguintes parâmetros e critérios (artigo 52, § 1º):

> 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.

Portanto, as medidas de boas práticas e governança aplicadas, a adoção de mecanismos e procedimentos internos que mitiguem o dano, podem ser fatores que irão contribuir para a redução da sanção.

> Observando o princípio constitucional da proporcionalidade, a imputação das sanções deve sempre observar a proporcionalidade como um critério para prevenir e inibir possíveis abusos do poder estatal no momento do exercício de suas funções. (PECK, 2020, p. 132)

E no que se refere ao poder público, a ele poderão ser aplicadas as mesmas sanções (artigo 52, § 3º), exceto as pecuniárias, porém sem prejuízo ao que está disposto na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), na Lei nº 8.429, de 2 de junho de 1992 (Lei de Improbidade Administrativa), e na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Por fim, o artigo 54 da lei prevê que, em caso de multa diária, na intimação feita deve contar no mínimo a descrição da obrigação imposta e prazo razoável e estipulado para o seu cumprimento.

Diante do exposto, percebe-se a importância de estar sempre atento a todos os princípios e requisitos trazidos pela Lei Geral de Proteção de Dados Pessoais, bem como a adequação do tratamento de dados pessoais às bases legais previstas, para evitar o desvio de finalidade no tratamento, para mitigar danos aos titulares e também não ocasionar sanções administrativas.

CONCLUSÃO

Todo o estudo abordado neste trabalho teve como objetivo a conscientização do titular dos dados pessoais. Por ser uma lei nova e que trouxe a autodeterminação informativa, ou seja, o titular é o dono dos dados pessoais e tem que saber o que está sendo feito com eles, essas questões precisam ser levantadas, e levadas até o titular. O Direito não pode e nem deve ser complexo. Ele deve ser simples e facilitar ao máximo ao titular, a compreensão e aplicação.

Sabe-se que há muitos anos, o acesso a informação era limitado, caro e privilegiado. Com o desenvolvimento da tecnologia e da evolução do ser humano, houve uma quebra de paradigmas. Hoje, o acesso a informação está a uma distância de um clique. Qualquer pessoa que possua acesso a internet, pode ter acesso a qualquer conteúdo e informação que deseja, em qualquer lugar do mundo, a qualquer hora.

Atualmente, por causa desse avanço, as empresas que trabalham com tecnologia ou que oferecem serviços que necessitam de dados pessoais, passaram a realizar uma constante coleta de dados pessoais do usuário/titular. Os dados pessoais possuem grande valor financeiro, pois eles definem as tendências do momento.

Um ditado popular diz que “conhecimento é poder” e quando se trata de dados pessoais, o conhecimento é sinônimo de muito poder financeiro. Portanto, houve a necessidade de regulamentação do uso desses dados, a fim de evitar a violação aos direitos fundamentais dos usuários, dentre eles, a privacidade e a intimidade.

Diante disso, no capítulo 1 (um) deste trabalho, fora feita uma introdução ao Direito Digital, trazendo um pouco do seu conceito e como ele vem sendo utilizado atualmente. Isso foi importante para entender a importância da criação da Lei Geral de Proteção de Dados Pessoais e como se deu esta criação. O Direito Digital veio, não para ser mais um ramo do Direito, mas sim para interdisciplinar os ramos que já existem e assim trazer uma solução mais completa para uma possível lide.

Viu-se também que a Lei Geral de Proteção de Dados Pessoais, teve uma influência direta da *General Data Protection Regulation* – GDPR, ou seja, uma lei nova, de multidisciplinariedade, inclusive o Direito Internacional. Percebeu-se que as tecnologias estão evoluindo e o Direito precisa acompanhar essa demanda, mas de maneira mais eficaz e rápida. É necessário desenvolver uma cultura preventiva.

O segundo capítulo traz uma introdução aos dados pessoais, a fim de possibilitar uma melhor compreensão do conceito. Em seguida foi feita uma abrangência da lei, apresentando seu conceito, vigência, as terminologias usadas, princípios, territorialidade da lei, direito à privacidade e à informação.

O tópico 2.3 trouxe uma profundidade no que se refere ao tratamento de dados pessoais pelas empresas e pelo Poder Público. Reitera-se que este trabalho não se aprofundou em dados pessoais sensíveis e nem em dados anonimizado. Fora explicado as bases legais trazidas pela legislação para que o tratamento de dados pessoais possa ser realizado, enfatizando duas bases legais: a do consentimento e a do interesse legítimo, pois ambas possuem mais detalhes, caso sejam escolhidas para a realização do tratamento.

Deixou-se claro também, os direitos do titular, bem como a diferença do direito ao esquecimento e o direito a exclusão dos dados pessoais.

Por fim, o terceiro capítulo abordou o tema da responsabilidade civil, segurança e boas práticas. As sanções administrativas previstas na lei, só poderão ser aplicadas em 01 de agosto de 2021, pela Autoridade Nacional de Proteção de Dados Pessoais. Mas isso não impede que as empresas ou o Poder Público sejam responsabilizados pelo mau uso dos dados pessoais dos titulares. Vale lembrar que a pessoa física que trata dados pessoais com finalidade econômica, também deve se adequar a Lei Geral de Proteção de Dados Pessoais, a fim de evitar a responsabilidade civil e a aplicação de sanções administrativas.

É sabido que os “dados são o novo petróleo”, em razão deles serem a matéria prima da informação das empresas e que por consequência gera o conhecimento necessário. Esse conhecimento capacita as empresas de prestar um serviço ou oferecer um produto personalizado para seus clientes.

A matéria prima que gera a informação, que gera o conhecimento, é a que faz as empresas crescerem, é a que faz as empresas faturarem. Entende-se a importância dos dados para o crescimento da economia e assim por diante. Então, por que é preciso saber o que são feitos com os dados pessoais?

O problema não está no tratamento dos dados pessoais, mas o que é feito com eles. Quando a informação é monopolizada, existe maiores chance de ocorrer abusividades. Os dados estão em praticamente tudo que se usa no dia a dia e quanto mais tecnologia, mais praticidade, mais consumo de dados pessoais.

A Lei Geral de Proteção de Dados Pessoais veio para devolver a autodeterminação

informativa para o titular e para mitigar a abusividade praticada durante o tratamento dos dados pessoais. Portanto, é necessário que os agentes de tratamento busquem diversas maneiras de proteger os dados pessoais, mas também informar o titular, levar a informação do que está acontecendo de maneira clara e precisa, gerando uma cultura de proteção de dados. No futuro, que não está muito distante, a transparência e zelo com o consumidor serão requisitos essenciais para a contratação de um serviço ou para a compra de um produto.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Constituição (1998). **Constituição da República Federativa do Brasil**. Brasília, DF: senado, 1988.

BRASIL, Código de Defesa do Consumidor (1990). **Lei nº 8.078 de 11 de setembro de 1990. Código de Defesa do Consumidor**. Brasília, DF: senado, 1990.

BRASIL. Código Civil (2002). **Lei nº 10.406 de 10 de janeiro de 2002. Código Civil**. Brasília, DF: senado, 2002.

BRASIL, Supremo Tribunal de Justiça. **REsp 1660168/RJ**. Brasília, DF: 2018. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/595923405/recurso-especial-resp-1660168-rj-2014-0291777-1/inteiro-teor-595923409. Acessado em 25 de setembro de 2020.

BRASIL. Marco Civil da Internet (2014). **Lei nº 12.965 de 23 de abril de 2014.** Brasília, DF: senado, 2014.

BRASIL. Decreto nº 10.474 de 26 de agosto de 2020. **Dispõe sobre a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança da Autoridade Nacional de Proteção de Dados – ANPD.** Brasília, DF: Poder Executivo, 2020.

CARVALHO, Orlando de. **A teoria geral da relação jurídica: seu sentido e limites.** Coimbra: Centelha – SARL, 1981.

CONSALTER, Zilda Mar. **Direito ao esquecimento: proteção da intimidade e ambiente virtual**. Curitiba: Juruá, 2017.

CONSELHO DA JUSTIÇA FEDERAL. **Enunciado nº 531 da VI Jornada de Direito Civil.** Disponível em: https://www.cjf.jus.br/enunciados/enunciado/142. Acessado em 08/09/2020.

DIREITO, Dizer o. **Lei 13.709/2018: Lei Geral de Proteção de Dados Pessoais**. Disponível em: encurtador.com.br/oqszY. Acessado em 01 de junho de 2020.

ESCOLA, Brasil. **Direito Digital – o direito à privacidade e a vedação ao anonimato na era digital**. Disponível em: encurtador.com.br/gqszP. Acessado em 01 de junho de 2020.

FIGUEIREDO, Luciano. FIGUEIREDO, Roberto. **Manual de Direito Civil**. Volume único. Salvador: Editora JusPodivm, 2020.

FRANÇA, Philip Gil. **Interesse público, um conhecido conceito "não determinado"**. Direito do Estado, n. 249, 2016. Disponível em: http://www.direitodoestado.com.br/colunistas/phillip-gil-franca/interesse-publico-um-conhecido-conceito-nao-indeterminado. Acessado em 24 de setembro de 2020.

GUIDELINES, European Union. **https://bityli.com/l3uwN**. Acessado em 08/09/2020. G1, São Paulo. http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html. Acessado em 19/06/2020.

LONGHI, João Victor Rozatti; JÚNIOR, José Luiz de Moura Faleiros. **Estudos essenciais de direito digital.** Uberlândia: LAECC, 2019. E-book, online.
LUCCA, Newton de. SIMÃO FILHO, Adalberto. LIMA, Cíntia Rosa Pereira de. **Direito e Internet III – Tomo I: Marco Civil da Internet (Lei n. 12.965/2014).** São Paulo: Quartier Latin, 2015.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. 1ª ed. Goiânia/GO: RM Digital Education, 2019. ISBN: 9781093409420. E-book, online.

MALDONADO, Viviane Nóbrega. **Direito ao Esquecimento**. São Paulo: Novo Século, 2017.

MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na Internet.** 2 ed. São Paulo: Revista dos Tribunais, 2014.

MARQUES, Rodrigo. **Direito Digital e Tecnologia – LGPD – Lei Geral de Proteção de Dados Aplicada ao Mercado**. Aula 1.4 – LGPD. – Prof. Rodrigo Marques. Disponível em: https://www.cers.com.br/curso/direito-digital-e-tecnologia-juridica. Acessado em 24 de setembro de 2020.

NOGUEIRA, Jose Helano Matos, Silvani Matos. **Direito Digital e Cibernético: Legislação Específica.** 1ª ed. Joinville/SC: Clube de Autores, 2019. E-book, online.

PINHEIRO, Patrícia Peck. **Direito Digital.** 6 ed., ver., atual e ampl. São Paulo: Saraiva, 2016.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** 2. Ed. São Paulo: Saraiva Educação, 2020.

SILVEIRA, Sergio Amadeu da Silveira. AVELINO, Rodolfo. SOUZA, Joyce. **A privacidade e o mercado de dados pessoais**. 2016. Artigo. Liinc em Revista, Rio de Janeiro, v.12, n.2, p. 217-230, novembro 2016, http://www.lblct.br/liinc; http://dx.dol.org/10.18617/liinc.v12i2.902

SILVA, José Afonso da. **Curso de direito constitucional positivo.** 13 ed. São Paulo: Malheiros, 1997.

SCHERTEL MENDES, Laura. **O Direito Fundamental à proteção de dados pessoais.** Revista de Direito do consumidor, vol. 79/2011. Editora RT.

TEIXEIRA, Tarcísio. **Curso de direito e processo eletrônico: doutrina, jurisprudência e prática.** 2 ed. São Paulo: Saraiva, 2014.

WIRECARD. **A importância dos Termos de Uso e Política de Privacidade no e-commerce**. Disponível em: encurtador.com.br/kxU28. Acessado em 25 de setembro de 2020.

ZANATTA, Leonardo. **O direito digital e as implicações cíveis decorrentes das relações virtuais.** Disponível em: encurtador.com.br/tyBR6. Acessado em 01 de junho de 2020.

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRÓ-REITORIA DE DESENVOLVIMENTO INSTITUCIONAL
Av. Universitária, 1069 I Setor Universitário
Caixa Postal 86 I CEP 74605-010
Goiânia I Goiás I Brasil
Fone: (62) 3946.3081 ou 3089 I Fax: (62) 3946.3080
www.pucgoias.edu.br I prodin@pucgoias.edu.br

RESOLUÇÃO n˚038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

A estudante Isabella Teixeira Martins do Curso de Direito ,matrícula 2016.1.0001.0625-6, telefone: 62 98620-9989, e-mail isabellatjur@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado **Tratamento de Dados Pessoais: Por que precisamos saber como nossos dados são tratados?**, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 25 de novembro de 2020.

Assinatura do(s) autor(es): Isabella Teixeira Martins

Nome completo do autor: Isabella Teixeira Martins

Assinatura do professor-orientador: _____

Nome completo do professor-orientador: Marina Rúbia M Lôbo de Carvalho