Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito

CAMILA ALMEIDA GARCIA

COMPLIANCE E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: a importância da Matriz de Risco no tratamento dos dados pessoais

BRASÍLIA
2021

CAMILA ALMEIDA GARCIA

COMPLIANCE E A LEI GERAL DE PROTEÇÃP DE DADOS PESSOAIS: a importância da Matriz de Risco no tratamento dos dados pessoais

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Ricardo Victor Ferreira Bastos

BRASÍLIA
2021

CAMILA ALMEIDA GARCIA

COMPLIANCE E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: a importância da Matriz de Risco no tratamento dos dados pessoais

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador: Professor Ricardo Victor Ferreira Bastos

BRASÍLIA, 1º DE MARÇO DE 2021

BANCA AVALIADORA

_____

Professor Orientador

_____

Professor Avaliador

Compliance e a Lei Geral de Proteção de Dados

Camila Almeida Garcia

Resumo: O presente artigo tem como objetivo a análise das exigências trazidas pela Lei Geral de Proteção de Dados Pessoais – Lei nº. 13.709 de 14 de agosto de 2018 –, tomando-se em conta o conceito de "dados" e de "informação" para tal estudo, bem como a abrangência da aplicação da Lei, conforme exposto em seu artigo 3º. Ante tamanho alcance das diretrizes da Lei nº. 13.709/2018 (LGPD), o problema explorado será quanto aos meios e às possibilidades que as empresas terão a seu dispor para acompanhar tais comandos legais. A fim de recortar o tema, para melhora trabalhá-lo, o método eleito para ser exposto no presente artigo é chamado de *compliance* ou "programa de integridade". Diante do atual cenário nacional, este estudo traz ao debate a possibilidade que o *compliance* representa como ferramenta eficaz de conformação à referida Lei. O método utilizado para tanto é de revisão bibliográfica, a fim de demonstrar a relevância do tema abordado e trazer como solução ao problema de conformidade a política interna de integridade.

Palavras-chave: Lei Geral de Proteção de Dados. Direitos da personalidade. Privacidade. Práticas de *compliance*. Matriz de risco. Transparência.

Abstract: The purpose of this articles is to analyze the requirements of Personal Data Protective Law, knowing the concept of "data" and "information", as well as the coverage of its application, according to its 3º article. Based on the scope of the Law nº. 13.709/2018, the situation addressed in this article is about the companies's possibilities to comply its legal commands. In order to specify theses studies, the method that will be exposed on this article is called Compliance, or internal controls. Given the current national situation, these studies bring to light the discussion of Compliance's possibility to represent effective means to comply that Law. The method used is a bibliographic review, in order to show that topic's relevance and expose Compliance as a solituion to the complying problem.

Key words: General Data Protection Law. Personality rights. Privacy. *Compliance*. Risks matrix. Transparency.

Sumário:

INTRDUÇÃO

A proteção de dados pessoais tem sido cada vez mais objeto de estudos e de tutela no campo jurídico. O movimento mundial em direção à regulamentação e à proteção de dados pessoais tem sido cada vez mais expressivo, em atenção aos avanços tecnológicos.

O direito é um meio onde diversas mudanças têm ocorrido, a fim de tutelar o que tem sido chamado de "personificação virtual", que é a expressividade da pessoa no meio digital. Tal preocupação demonstra-se legítima, já que incidentes recentes têm envolvido manipulação de informações, compra e venda de dados pessoais no âmbito do marketing digital, elaboração de "score social"[1] – *big data* – e ainda influência sobre resultados eleitorais[2].

Um marco nas legislações de proteção de dados pessoais é a Lei nº. 2016/679 (UE). Tamanha importância na proteção das informações pessoais que circulam no mundo virtual dá-se em razão do alto potencial de risco que estas informações carregam. Considerando que os dados pessoais são uma espécie de "personificação virtual" do titular, o direito que os resguarda deve ser interpretado como personalíssimo.

Para maiores esclarecimentos a respeito do objeto da Lei nº. 13.709/2018, cumpre determo-nos nos conceitos de dados e informações, a fim de que as futuras análises se deem sobre alicerces sólidos.

Bruno Ricardo Bioni[3], com exatidão, destaca que a diferença entre dado e informação consiste no "estado". O dado seria "o estado primitivo da informação", de forma que por si só não acrescenta conhecimento. O autor destaca que são "fatos brutos".

Já informação é o processamento, a organização daqueles, de modo a estar convertido em algo inteligível, do qual se extrai conhecimento, ou seja, liga-se à finalidade que será dada a tal combinação de fatos.

> A dinâmica de um banco de dados envolve entrada (input) e processamento de dados e a saída (output) de uma informação. É imprescindível, portanto, o gerenciamento, manual ou automatizado, de um banco de dados, para que dele seja extraído algum conhecimento.[4]

É claro, portanto, que a simples captação de dados não representa qualquer utilidade ao mercado. Ou seja, tudo o que é recolhido – com ou sem consentimento do titular – é tratado,

---

[1] QIAN. Sun. **China's social credit system was due by 2020 but is far from ready**. Disponível em: https://algorithmwatch.org/en/story/chinas-social-credit-system-overdue/. Acesso em 21 fev. 2021.
[2] BBC. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 12 jan. 2021.
[3] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p 31.
[4] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p 32.

lapidado. Neste sentido, a Lei Geral de Proteção de Dados pretende que os dados sensíveis sejam tutelados com maior rigor.

A União Europeia[5] indica como "dados pessoais" toda e qualquer "informação relativa a uma pessoa viva, identificada ou identificável" e ainda o conjunto de informações distintas que podem gerar a identificação de um indivíduo. Isto porque da identificação do titular podem advir diversos danos ou violações aos seus direitos.

Neste sentido, o artigo 5º, da Lei nº. 13.709/2018[6], define, em seus incisos, os conceitos de dados pessoais como informação que identifica – ou que possibilita identificar – o titular e ainda, como dado pessoal sensível:

> […] dado pessoal sobre origem racial ou étnica convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Importa notar que, diante de tal realidade, a proteção aos dados pessoais que a LGPD traz é de suma importância para as relações que têm se estabelecido na atualidade. É cada vez mais comum que sejam celebrados contratos virtuais: compra e venda, prestação de serviços, marketing, são apenas alguns exemplos.

Nestas transações muitos dados são compartilhados. Mas não apenas nesses casos. Devemos notar que, sob o prisma de Bioni[7], dados são fatos. Todo conteúdo curtido, comentado, compartilhado, áudios e vídeos enviados e/ou recebidos por aplicativos de comunicação são também dados capazes de gerar informações. Dados que, na realidade, geram informações. Sendo, portanto, necessário entender a natureza da proteção dos dados pessoais que a Lei Geral de Proteção de Dados busca trazer. Bem como os mecanismos que precisam, desde já, ser adotados para uma maior observância à Lei Geral de Proteção de Dados.

Neste trabalho será apresentado o "programa de integridade" como uma das soluções possíveis para a prevenção de danos aos titulares e também como mecanismo eficaz e necessário para as empresas, no sentido de prevenção de riscos.

---

[5]UNIÃO EUROPEIA. **Collaboration in Research and Methodology for Official Statistics**. Disponível em: https://ec.europa.eu/eurostat/cros/content/personal-data_en . Acesso em: 22 mar. 2021.
[6] BRASIL. **Lei Geral de Proteção de Dados** (Lei no 13.709, de 14 de agosto de 2018). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 fev. 2021.
[7] BIONI, Bruno Ricardo**. Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p 58.

O *compliance* – ou "programa de integridade" –, para além de propor o mero cumprimento rigoroso de preceitos legais, busca reafirmar e disseminar a "ética nas atividades empresariais, por meio de instrumentos, no âmbito da pessoa jurídica, que visam à **detecção**, à **prevenção** e à **remediação** de atos ilícitos"[8].

Uma vez que a Lei Geral de Proteção de Dados tem aplicabilidade tanto interna quanto externamente, a depender da atividade desenvolvida pelo empresário, a adoção de medidas preventivas é essencial para o bom funcionamento de seus trabalhos. A expressividade da Lei nº. 13.709/2018 está determina em seu artigo 3º, com poucas exceções.

Justamente por este motivo, o *compliance* parece ser o melhor método de alinhar as condutas empresariais ao dispositivo legal. Porque compreende diversas estratégias de organização, cujo objetivo não se limita à obediência legal, mas exige a criação de um código de ética interno. É pressuposto, para tanto, o envolvimento efetivo e verdadeiro da diretoria.

Mais importante é verificar que a elaboração deste programa de integridade deve ser sempre personalizada segundo a necessidade de cada pessoa (física ou jurídica). Deve-se considerar, desta forma, um código de ética, a elaboração da matriz de riscos, o "suporte da alta administração, treinamento periódicos, cultura corporativa, monitoramento dos controles e processos"[9], bem como canais de apuração e de condutas ilícitas.

O presente artigo, portanto, se desenvolve a fim de analisar as exigências da Lei Geral de Proteção de Dados Pessoais fazendo um paralelo com o programa de integridade.

1 PROTEÇÃO DOS DADOS PESSOAIS COMO FORMA DE GARANTIR OS DIREITOS DA PERSONALIDADE

Um dos objetivos fundamentais da ciência do Direito é garantir o mínimo de resguardo jurídico à personalidade. Não é possível, sob esta ótica, ignorar a importância da proteção à intimidade (ou privacidade), à autonomia e à informação, que são facetas daquele e

[8] LIMA, Ana Júlia Andrade Vaz. **Programa de Integridade na Lei nº. 12.846/2013**. 2018. 318 p. Tese (Mestrado em Direito) – Pontifícia Universidade Católica de São Paulo PUC-SP, São Paulo, 2018.
[9] KOEPSEL, Alice de Medeiros. **Adoção e Efeitos do Programe de Compliance à Luz da Lei Geral de Proteção de Dados Pessoais**. 2020. 71 p. Trabalho de Conclusão de Curso (Monografia) – Universidade do Sul de Santa Catarina, 2020.

devem ser protegidas em conformidade com as necessidades apresentadas pelos diversos momentos históricos.

O direito à intimidade, autonomia e informação encontra hoje desafios no aspecto digital, pois cada vez mais a humanidade tem caminhado para a "virtualização" das relações. Negócios, ensino, trabalho, amizade, namoro e muitas outras formas de relacionamento desenvolvem-se cada vez mais na realidade da informática, por meio do ambiente virtual.

Não somente as relações mais formais, mas também as situações mais cotidianas têm se instalado no ambiente virtual. Mensagens no *Whatsapp*, postagens no *Instagram* e no *Facebook* são ferramentas usadas corriqueiramente. É inegável que a humanidade tem caminhado cada vez mais para a virtualização das realidades.

Tal virtualização não pode ser ignorada pelo Direito, pois a partir dela surgem situações de abuso e de mau uso da liberdade na abrangente realidade da Internet. A informação disponível nas redes pode – e muitas vezes o são – ser informações pessoais. Doneda[10] comenta que os dados pessoais representam a própria pessoa no espaço virtual.

Em atenção à proteção da pessoa humana, tem havido um movimento mundial em direção à criação de leis e normas que visam assegurar boas práticas no ambiente virtual.

Os dados são produzidos pelo titular, conforme suas escolhas, sua conduta, seus hábitos, seus relacionamentos. Não são fatos sobre os quais a pessoa humana tem poderes, mas são fatos expressos pela própria individualidade do titular. São reflexos da realidade de determinada vida humana, laços criados e relações estabelecidas, de modo que é impossível ignorar que se trata de uma "representação virtual da pessoa"[11]

As informações geradas a partir dos dados produzidos pelos titulares estão intimamente ligadas à pessoa, porque são capazes de identificá-la e individualizá-la. Uma vez que isto ocorra, os danos daí advindos serão sofridos pessoalmente pelo titular. Se, por exemplo, em razão da comercialização de dados entre empresas, um cliente tiver menor acessibilidade a determinados produtos ou benefícios, ou ainda se tiver sua escolha influenciada por uma

---

[10] DONEDA, Danilo. **A proteção dos Dados Pessoais como um Direito Fundamental**. Disponível em: file:///C:/Users/caalm/AppData/Local/Temp/Dialnet-AProtecaoDosDadosPessoaisComoUmDireitoFundamental-4555153.pdf. Acesso em 22 mar. 2021.

[11] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 123

propaganda previamente direcionada, o dano sofrido não se dará apenas na esfera patrimonial, mas na esfera moral.

Neste mesmo sentido, Bioni entende que personalidade é o "conjunto de características que distingue uma pessoa da outra"[12], de modo que:

> Os direitos da personalidade seriam os caracteres incorpóreos e corpóreos que conformam a projeção da pessoa humana. Nome, honra, integridade física e psíquica seriam apenas alguns dentre uma série de outros atributos que dão forma a esse prolongamento.

Desta definição, fica ainda mais nítido que a proteção garantida pela LGPD é de natureza personalíssima, uma vez que os próprios dados refletem a pessoa que os gerou. Sendo, na verdade, uma proteção aos elementos que têm valor por si só e de maneira anterior ao ordenamento jurídico – que apenas faz reconhecê-los, mas não os criar.

1.1 **Os Princípios Protetivos da Lei Geral de Proteção de Dados Pessoais e a Importância do Consentimento do Titular**

Dada a grande importância que os dados pessoais têm para o indivíduo, é natural que a LGPD venha no sentido de tutelá-los rigorosamente. E o faz à luz dos princípios constitucionais.

Uma vez que representa proteção tão ampla, é importante frisarmos algumas formas desta proteção. Isso porque ao mesmo tempo que tutela o direito à privacidade, resguarda o direito de informação, ambos previstos na Constituição Federal da República Federativa do Brasil de 1988 (CF/88), em seu artigo 5º, incisos X e XIV[13]. Vejamos:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: […]
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; […]
> XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; […].

Laura Mendes, interpretando o dispositivo constitucional salienta que não haveria razão para retirar a proteção à intimidade justamente em situações em que a pessoa mais se

---

[12] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p 55

[13] BRASIL. **Constituição Federal da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 jun. 2020.

encontra vulnerável. Salienta tal vulnerabilidade por entender que os bancos de dados representam risco "constante e diário para todos os cidadãos"[14].

A Lei Geral de Proteção de Dados Pessoais, em seus artigos 1º e 2º, indica seu objetivo e seus fundamentos[15]:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

O reconhecimento deste direito fundamental, portanto, representa um avanço significativo para os titulares de dados. Além de terem seus direitos reconhecidos nas relações estabelecidas pessoalmente, terão ainda resguardo mais significativo nas suas relações virtuais.

Isto porque, conforme frisa Koepsel[16], a "inviolabilidade da intimidade, da honra e imagem é um desdobramento da proteção à privacidade" (página 18). Sendo, portanto, direitos vinculados à personalidade.

Como já destacado, os dados podem ser uma forma de apresentação virtual da pessoa, ou seja, qualquer forma de exposição daqueles pode configurar um dano à personalidade

---

[14] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 171.
[15] BRASIL. **Lei Geral de Proteção de Dados** (Lei no 13.709, de 14 de agosto de 2018). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jun. 2020.
[16] KOEPSEL, Alice de Medeiros. **Adoção e Efeitos do Programe de Compliance à Luz da Lei Geral de Proteção de Dados Pessoais**. 2020. 71 p. Trabalho de Conclusão de Curso (Monografia). Universidade do Sul de Santa Catarina, Tubarão. 2020

do seu titular. Em razão de tais riscos Laura Mendes[17] entende que a proteção aos dados pessoais se dá de duas formas:

> Assim, entendemos que o direito básico do consumidor à proteção de dados pessoais envolve uma dupla dimensão: (i) a tutela da personalidade do consumidor contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais; e (ii) a atribuição ao consumidor da garantia de controlar o fluxo de seus dados na sociedade.

Seriam, respetivamente, o aspecto objetivo e subjetivo de tal tutela. De modo que o titular teria, com a vigência da LGPD, a possibilidade de controlar o fluxo de seus dados por meio de uma decisão verdadeiramente informada e livre. Este é exatamente o escopo da Lei Geral de Proteção da Dados.

O artigo 7º, inciso I, desta Lei[18] indica como primeiro requisito para o tratamento dos dados o consentimento do titular. Vê-se, desde logo, a importância atribuída à concordância do titular dos dados.

Zanatta[19], neste ponto, frisa que o consentimento deverá ser autodeterminado, para que seja válido. De modo que, em certo sentido, a proteção de dados apenas poderá dar-se efetivamente quando for possível pressupor que o titular tem controle sobre suas informações. O autor entende que a privacidade é, na verdade, a "cabeça" dos direitos da personalidade e das liberdades fundamentais.

Neste mesmo sentido o artigo 11, I, da LGPD, exige o consentimento do titular para o tratamento de dados sensíveis. Bem como o artigo 14, §1º, do mesmo diploma legal, estipula que, em se tratando de crianças e adolescentes, os pais ou o responsável legal deverão consentir no tratamento dos dados.

---

[17] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. p. 203

[18] BRASIL. **Lei Geral de Proteção de Dados (Lei no 13.709, de 14 de agosto de 2018)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jun. 2020. Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular (…).

[19] ZANATTA, Rafael Augusto Ferreira. **Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica?**. 2017. Rede de Pesquisa em Governança da Internet, 2017. Disponível em: http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf. Acesso em: 22 mar. 2021.

Neste sentido, impossível discordar de Zanatta quanto à necessidade de que o titular tenha efetivo controle sobre seus dados. Para tanto é imprescindível uma política de honestidade e transparência no tratamento dos dados.

Daí se pode extrair que, apesar de o consentimento não ser a regra, não se pode ignorar que o objetivo da Lei é empoderar o titular, atribuindo-lhe controle sobre suas informações e autonomia de vontade. Devendo-se, no entanto, ressaltar que há casos em que não haverá necessidade de o titular manifestar concordância com o tratamento; o legislador entendeu que os controladores precisarão também de certa liberalidade para que suas atividades possam ser desenvolvidas.

Ainda assim, é importante frisar que o consentimento consciente de que a autora Laura Mendes[20] fala na obra supracitada é justamente baseado em que se conheça todas as condições envolvidas no tratamento, sendo-lhe possível saber quem é o responsável pelo tratamento, quais as finalidades, como se dará e como serão usados seus dados, por exemplo. Tais indicativos encontram-se explícitos no artigo 6º da LGPD[21]:

> 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

[20] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 204.
[21] BRASIL. **Lei Geral de Proteção de Dados** (Lei nº 13.709, de 14 de agosto de 2018). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jun. 2020.

> 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.

O referido artigo aponta os parâmetros a serem observados quando do tratamento de dados pessoais. Sendo todos pautados na boa-fé quanto à finalidade do tratamento, à adequação dos meios, à necessidade e à abrangência, bem como ao livre acesso do titular aos dados, à qualidade do tratamento (garantindo clareza e exatidão aos titulares), à transparência, à segurança e à proteção, à não discriminação e, por fim, quanto à responsabilização e à prestação de contas ante a qualquer erro ou tratamento indevido.

Sendo livre e consciente o consentimento, o titular terá mais controle sobre a finalidade do tratamento, quais dados seus estão sendo tratados e ainda por quanto tempo poderão sê-lo – vide artigo 15, III, Lei nº. 13.709/2018[22].

Toda a relação entre o titular e o agente responsável por tratar os dados deverá, claramente, ser pautada pelo princípio da vulnerabilidade. Não apenas no sentido da diferença de poder econômico entre as partes, mas também ante a projeção social do dano em face ao conhecimento e capacidade técnica para diminuir ou controlar tais consequências.

É nítido que a pessoa física estará sempre em disparidade, em condição vulnerável em relação à pessoa jurídica, neste sentido. É exatamente por esta razão que a Lei Geral de Proteção de Dados indica as diretrizes e bases em que se devem dar as relações que envolvam a troca dos dados.

Neste sentido, Laura Mendes indica três passos[23] consecutivos – três níveis – a fim de assegurar maior garantia ao titular de dados:

> O modelo proposto pode ser sumariamente apresentado da seguinte forma: qualquer tratamento de dados pessoais somente pode ser iniciado se atendidas as condições para a sua legitimidade (condições de legitimidade);
> (a) qualquer tratamento de dados pessoais somente pode ser iniciado se

[22] BRASIL. **Lei Geral de Proteção de Dados (Lei no 13.709, de 14 de agosto de 2018).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 fev. 2021. Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: (…) 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.

[23] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 204.

> atendidas as condições para a sua legitimidade (condições de legitimidade);
> (b) atendidas as condições de legitimidade, todo o tratamento de dados deve cumprir determinados procedimentos, essenciais para a garantia do direito básico (procedimentos para a garantia do direito);
> (c) em caso de violação a esse direito, são aplicáveis sanções administrativas, civis e penais (sanções e reparação).

No primeiro nível deve-se analisar justamente os termos em que se deu o consentimento. Enquanto que no segundo, o objetivo é garantir o direito básico de proteção dos dados, numa relação de equidade entre as partes, quanto à informação. Por fim, deve-se falar das consequências do descumprimento de qualquer uma das etapas anteriores.

Neste sentido, a Lei Geral de Proteção de Dados Pessoais trouxe um rol de diretrizes quanto à Agência Nacional de Proteção de Dados, cujos objetivos estão previstos no artigo 55-J, da Lei, incluído pela Lei nº. 13.853/2019[24].

Alguns destes objetivos deixam claro o viés protetivo da Lei, como por exemplo: fiscalizar e aplicar sanções quando do tratamento indevido, elaboração de políticas de proteção de dados, promoção de cooperação com autoridades internacionais de proteção de dados, realização de auditorias quanto à fiscalização, implementação de mecanismos de reclamação quanto ao tratamento de dados.

2 A NECESSIDADE DE IMPLEMENTAÇÃO DE DIRETRIZES INTERNAS PARA CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Desde 1999 a Organização para Cooperação e Desenvolvimento Econômico (OECD), em demonstração clara de interesse quanto ao uso da internet, emprega e explica a expressão da orientação normativa conhecida como *"Fair Information Practice Pinciples/FIPPS"*[25].

Esta expressão origina-se de um código canadense de proteção de informações pessoais, denominado de "*CSA Model Code*", desenvolvido em 1996. Este modelo aponta dez princípios, cuja finalidade é assegurar verdadeira proteção à privacidade e à liberdade[26], que

[24] BRASIL. **Lei Geral de Proteção de Dados (Lei no 13.709, de 14 de agosto de 2018)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso: 21 fev. 2021.
[25] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Forum:** Challenges and Opportunities of Advertising Today. Disponível em: https://marcomm.mccarthy.ca/pubs/share4.htm. Acesso em: 23 fev. 2021
[26] CANADA. Government of Canada. **Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96.** Disponível em: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-11.html. Acesso em: 23 fev. 2021.

foram mais aprimorados em conformidade com as necessidades supervenientes. São eles[27], em tradução livre:

a) Prestação de contas: uma vez que a empresa é responsável pelos dados que se encontram sob seu controle, deve apontar quem será, internamente, designado para controlar os dados segundo o programa de integridade da empresa;

b) Propósitos específicos: a motivação da coleta dos dados pessoais deverá estar clara para o titular, antes da coleta.

c) Consentimento: o conhecimento e o consentimento são necessários para a coleta dos dados (para eventual uso ou divulgação também), dadas exceções previstas na Lei.

d) Limite de coleta dos dados: a coleta de dados pessoais deve ser estritamente coletada com base nas diretrizes da Lei, pautada por princípios de transparência e honestidade.

e) Limites ao uso, à divulgação e à retenção de dados: os dados não devem ser usados de modo diverso das finalidades apontadas quando da coleta, a não ser que haja consentimento do titular.

f) Veracidade: os dados devem ser verdadeiros, completos e atualizados de acordo com as necessidades da finalidade da coleta.

g) Segurança: os dados devem ser protegidos apropriadamente conforme a sensibilidade do dado.

h) Transparência: a empresa tem a obrigação de disponibilizar imediatamente informações sobre a sua política de tratamento de dados, quando solicitado.

i) Acesso: uma vez solicitado pelo titular dos dados, este deverá ter acesso aos seus dados, bem como direito de confrontar as informações a ele relativas, para que sejam retificadas.

j) *Compliance*: o indivíduo deve ter conhecimento os princípios adotados pela empresa, no que tange ao tratamento e segurança dos seus dados.

[27] CANADA. **Ten Privacy Principles.** Disponível em: https://www.legalaid.on.ca/privacy-policy/ten-privacy-principles/. Acesso em: 26 fev. 2021

Não restam dúvidas que o efeito é elevar o titular dos dados ao papel de protagonista, já que o tratamento somente será justo e lícito conforme houver consentimento – e quanto mais informado e livre for, mais válido será. O cidadão passará a ter controle sobre seus dados, de modo a ser possível então falar de autodeterminação informativa, como indica Bioni[28].

O artigo 18 da Lei Geral de Proteção de Dados traz uma série de direitos que o titular tem sobre seus dados, bem como lhe atribui poderes para consultar, manifestar-se sobre a veracidade deles, requerer anonimização, eliminação e ainda de revogar seu consentimento a qualquer momento. Um direito garantido neste rol que merece atenção é o que dispõe o inciso VIII[29], quanto a possibilidade de o titular conhecer os efeitos da sua negativa ao tratamento.

Ora, um dos problemas enfrentados hoje é que diversas plataformas e sites de relacionamento ou de compra e venda, no momento do cadastro, exigem, como requisito para acesso ao produto ou serviço, a sinalização de que o titular concorda com os termos a ele impostos.

Com a vigência da Lei Geral de Proteção de Dados, tal conduta não poderá ser admitida. Tanto em razão da validade do consentimento quanto em função do referido inciso. Isso porque ele dá ao titular poder de negociar.

De outro lado, os controladores deverão aperfeiçoar suas estratégias regulatórias, não coletando dados em excessividade, especificando as finalidades da coleta, de forma que o tratamento dos dados será centrado no titular e no controlador. O que estaria justamente encaixado nos princípios apontados, em especial, pelas letras “a”, “g”, “h” e “j”, anteriormente expostos.

Para tanto, é nítida a necessidade de que as informações prestadas ao titular de dados sejam inteligíveis, acessíveis e claras. Fica, portanto, nítida a necessidade urgente que as

---

[28] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019. p 115.

[29] BRASIL. **Lei Geral de Proteção de Dados (Lei no 13.709, de 14 de agosto de 2018).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 fev. 2021. Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: (...) VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa (...).

empresas têm de adequar suas políticas internas para melhor conformidade com as diretrizes e exigências da Lei nº. 13.709/2018.

Nesse sentido, o *compliance*, que surge com a finalidade de criar mecanismos internos de controle e monitoramento de operações – com a preocupação crescente em aplicar um código interno de ética –[30], parece ser um mecanismo eficaz no sentido de adequação das empresas à referida Lei.

2.1 O Conceito de *Compliance*

Antes de adentrar mais profundamente nas práticas envolvidas pelo *compliance*, convém frisar o seu conceito, segundo Bertoccelli[31]:

> […] o compliance integra um sistema complexo e organizado de procedimentos de controle de riscos e preservação de valores intangíveis que deve ser coerente com a estrutura societária, o compromisso efetivo da sua liderança e a estratégia da empresa, como elemento, cuja adoção resulta na criação de um ambiente de segurança jurídica e confiança indispensável para a boa tomada de decisão.

Notável, portanto, que tais práticas não se limitam ao combate à corrupção ou uma conduta de observância das leis. Gustavo Artese[32] entende que o *Compliance* se dá mais ainda no sentido estratégico, a fim de que, além de serem cumpridas as diretrizes legais a que a empresa ou instituição está sujeita, esta também elabore políticas próprias de natureza procedimental, ética.

Em razão desta definição, estas práticas foram escolhidas para o presente estudo no que tange à necessidade que as empresas (S/As, limitadas, individuais), associações, entidades, entre outras apresentarão ante a vigência da LGPD.

Dentre as diversas relações jurídicas que o titular de dados participa, no meio virtual, a mais corriqueira é que a se dá na relação de consumo. Ainda mais em se considerando o momento de pandemia e quarentena a que estamos sujeitos desde março de 2020, em que tais relações passaram a ocorrer muito mais por meios digitais.

---

[30] SANTOS, Viviane Bezerra de Menezes. **Lei Geral de Proteção de Dados: Fundamentos do Compliance**. 2019. Trabalho de Conclusão de Curso (Monografia). Universidade Federal do Ceará, Fortaleza, 2019.
[31] BERTOCCELLI, Rodrigo de Pinho. Compliance. *In*: CARVALHO, André Costa. **Manual de Compliance**. 2ª ed. Rio de Janeiro. 2020. p. 39.
[32] ARTESE, Gustavo. Compliance digital e privacidade. In: CARVALHO, André Castro. **Manual de Compliance**. 2ª ed. Rio de Janeiro. 2020. p. 455.

2.2 Finalidade e Necessidade de Elaboração de uma Matriz de Riscos

Para as pessoas jurídicas que atuam diretamente no âmbito consumerista, a necessidade de alinhar-se às diretrizes da LGPD é gritante, em razão da presunção trazida Código de Defesa do Consumidor (CDC)[33] quanto à vulnerabilidade do consumidor, reforçado ainda pelos princípios da Lei nº. 13.709/2018, conforme exposto acima no presente estudo.

Os dados recolhidos pelos fornecedores devem ser resguardados com extrema diligência, bem como com o resguardo necessário para que não haja qualquer violação à privacidade e intimidade do titular. Especialmente quando se fala na comercialização dos dados, dentro do marketing digital.

A matéria tratada nesta Lei é essencial para o desenvolvimento dos negócios baseados no processamento e fluxo de dados pessoais. Isto porque afeta diretamente a liberdade, o acesso à informação e a privacidade dos consumidores. Ou seja, as empresas que lidam com tais dados – direta ou indiretamente – precisam ser capazes de proteger a individualidade e intimidade do titular, de modo a anonimizar as informações geradas e tratadas.

A fim de garantir tais direitos personalíssimos, vem o *compliance*. Uma vez que o indivíduo deve ter possibilidade de "escolher livremente as formas de coleta, uso e revelação de seus dados pessoais"[34], surge a necessidade de que as empresas atuem eticamente no tratamento dos dados.

Artese entende que a interpretação da LGPD pode dar-se em dois sentidos estritamente contrários: por um lado supervalorizar o consentimento do titular, por outro trazer maiores exigências para os controladores de dados. Neste sentido, o *compliance* teria um papel fundamental, especialmente no segundo viés.

Uma vez que sua obra é voltada para as práticas de Compliance digital, é compreensível que o autor adote tal entendimento. Em que pese não seja o mesmo aderido neste trabalho – pois entendemos pela necessidade de dar força ao titular exatamente por meio do

---

[33] BRASIL. **Código de Defesa do Consumidor (Lei nº. 8.078, de 11 de setembro de 1990)**. Disponível em: hhttp://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 26 fev. 2021. Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo.

[34] ARTESE, Gustavo. Compliance digital e privacidade. In: CARVALHO, André Castro. **Manual de Compliance**. 2ª ed. Rio de Janeiro. 2020. p. 465

consentimento livre e informado. No entanto, entendemos que a abordagem do autor é relevante para o tema, devendo, portanto, ser exposta.

Artese indica cinco elementos essenciais no conceito de "organização responsável", cujo compromisso com a responsabilidade é cristalino. Tais elementos articulam condições, requisitos para sua implementação. São eles[35]:

a) O compromisso com a responsabilidade e a adoção de políticas internas compatíveis com os critérios externos (legislações, regulamentos, decretos): é típico do *Compliance* que as práticas envolvam toda a hierarquia da empresa. Não seria diferente neste caso, que exige a criação de política interna capaz de monitorar o tratamento dos dados. É essencial que tanto o corpo quanto a cabeça da empresa estejam intimamente envolvidos no propósito de dar segurança o titular.

b) Mecanismos para revisões internas de supervisão e segurança internas e verificação externa: neste passo está inclusa a elaboração da matriz de riscos. É o momento de avaliar as circunstâncias em que a empresa está inserida, de modo que é necessário ter mecanismos adequados de gerenciamento de informações, uma vez que se trata de dados sensíveis – tanto dos titulares, quanto de parceiros e inclusive os próprios.

c) Transparência e mecanismos de participação individual: o controlador de dados deve promover práticas e medidas pautadas na transparência para com o titular. Novamente, ressalta-se a necessidade de que estejam envolvidos o corpo e a cabeça da empresa.

d) Meios para remediação e execução externa: por fim, a empresa deve apresentar possibilidades sancionatórias, em caso de falha das práticas internas.

Dentre estas condições, a segunda é aquela que passará a ser explorada mais detidamente. É a etapa que envolve a elaboração dos riscos – internos e/ou externos – a que a empresa está sujeita. É também aquela que envolve tratamento e discriminação dos dados aos quais a empresa tem acesso.

3 TRANSPARÊNCIA E HONESTIDADE NA ELABORAÇÃO DA MATRIZ DE RISCOS

[35] ARTESE, Gustavo. Compliance digital e privacidade. In: CARVALHO, André Castro. **Manual de Compliance**. 2ª ed. Rio de Janeiro. 2020. p. 472.

Como já ressaltado, a elaboração da matriz de risco representa um momento em que se faz necessária a análise e a discriminação de determinados dados. É comum haver certos abusos no tratamento dos dados, a fim de que a empresa possa ter mais controle sobre os riscos aos quais está sujeita.

E, em certa medida, a discriminação "positiva" é necessária. Ou seja, aquela que se dá não com a finalidade de estratificar os consumidores e separá-los em categorias, mas aquela que se dá unicamente em função da saúde da empresa, sem que haja identificação de indivíduos ou troca de informações a respeito de determinado nicho mercadológico.

A finalidade positiva do tratamento de dados, do ponto de visto do *compliance*, deve ser sempre a saúde da empresa e deve estar pautado na honestidade e transparência para com o titular dos dados. De modo que, condutas contrárias aos princípios enumerados pela Lei nº. 13/709/2018, em seu artigo 6º, são corretamente consideradas ilícitas.

Neste sentido, o controle de abusividade é um grande passo em direção à boa-fé nas relações que envolvem tratamento de dados. Laura Schertel[36] comenta que o tratamento de dados pautado num consentimento válido deverá observar minimamente: a declaração expressa do titular dos dados para o tratamento, as condições em que este se dará, a finalidade do tratamento, quais dados serão tratados, bem como, ainda, a possibilidade de revogar seu consentimento.

Sendo feito em termos diversos destes, o tratamento poderá ser considerado abusivo e, portanto, ilícito. Isto porque em se tratando de um contrato, é essencial que as partes envolvidas tenham conhecimentos mínimos a respeito dos seus termos. Sem que se ignore a situação de vulnerabilidade do titular frente aos controladores, operadores e encarregados do tratamento dos dados.

A Lei Geral de Proteção de Dados, neste sentido, traz diversas diretrizes e determinações quanto ao comportamento de quem será responsável pelo tratamento dos dados. Exigindo medidas protetivas e de controle sobre os dados, a fim de que torne possível o "rastreamento" do responsável.

---

[36] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014. p. 205-207.

O controle de abusividade vem, portanto, no sentido de resguardar os direitos do titular e cobrar dos tratadores uma conduta honesta e franca, como deve ser.

A adoção das práticas de *Compliance* para conformidade com a legislação é sempre "personalizada" para as necessidades específicas de cada empresa e mudam conforme as necessidades de cada contexto. No entanto, existem algumas delas que são basilares, ou seja, estarão presentes genericamente em todos os casos. No que tange à elaboração da matriz de risco, as consequências serão diretas.

A matriz de risco abarca informações sensíveis à empresa que está aplicando o *Compliance*, tanto dados internos e próprios, quanto aqueles advindos de parcerias, dados sensíveis do seu nicho de atuação e ainda dados sensíveis dos consumidores.

Como já ressaltado, a elaboração da matriz de risco é uma etapa basilar na prática de *Compliance*, o que significa dizer que estará presente em todos os modelos. É, portanto, uma etapa necessária à saúde da empresa.

Exige, para tanto, certo tratamento e discriminação de dados. Afinal este é o próprio teor da matriz de riscos: filtrar e estratificar as informações a fim de que, a partir delas, seja possível traçar metas e planos de atuação.

Na medida em que for elaborada com métodos pouco honestos ou transparentes, deve mesmo ser limitada e inclusive estar sujeita a punição. Como já frisado, os dados pessoais são direito da personalidade e as consequências de sua manipulação indevida são sempre drásticas para o titular.

De modo que, inclusive no que tange à aplicação das práticas de *compliance*, a elaboração da matriz de risco deverá ser pautada numa política interna ética de transparência e honestidade para com o titular. A fim de que cada vez menos os direitos de personalidade sejam feridos em razão de motivações pouco justas.

O *compliance*, como ferramenta capaz de criar novos padrões cultuarias no ambiente de trabalho, parece ser o meio mais completo para instaurar uma mentalidade respeitosa nas negociações, quanto à privacidade e à não "objetificação" das pessoas.

CONSIDERAÇÕES FINAIS

O mundo tem caminhado aceleradamente para a “virtualização” das relações pessoais, de trabalho e, por fim, jurídicas. A realidade mundial da pandemia do COVID-19 mostra diariamente como a tecnologia é necessária para a manutenção das realidades materiais, pois possibilita a determinadas parcelas da população que realizem seus trabalhos e estudos de suas casas, que comprem e vendam por meio de *sites*, que tenham relacionamentos via internet.

A proteção de todos os dados que circulam diariamente pela realidade digital é de extremas urgência e importância. As negociações, a compra e venda, as contratações, as divulgações de informações pessoais não ficarão paralisadas aguardando a adaptação de empresas, entidades e associações. Tudo ocorrerá como já ocorre: minuto a minuto.

A necessidade, antes latente, de criar e implantar políticas éticas no tratamento dos dados pessoais, agora é pungente.

O *compliance*, por ser um compilado de práticas de “boa conduta”, tem intrinsecamente o condão de ser personalizado e adaptável às circunstâncias de cada pessoa jurídica. Em razão desta maleabilidade, entendemos que se trata do método mais acertado para garantir a efetividade das tutelas trazidas pela Lei nº. 13.709/2018.

A elaboração de um código de ética que auxilie e embase a criação da matriz de riscos – abrangendo riscos internos e externos –, com o devido envolvimento de toda a hierarquia da empresa é o primeiro passo essencial para a concretização de grandes ideias: o respeito à liberdade e ao direito de informação e a transparência nas condutas empresariais.

REFERÊNCIAS

ARTESE, Gustavo. Compliance digital e privacidade. In: CARVALHO, André Castro. **Manual de Compliance**. 2ª ed. Rio de Janeiro. 2020. p. 455 - 480.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019

BRASIL. **Código de Defesa do Consumidor (Lei nº. 8.078, de 11 de setembro de 1990)**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 25 jun. 2020

BRASIL. **Constituição Federal da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 jun. 2020.

BRASIL. **Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jun. 2020.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Costa. **Manual de Compliance.** 2ª ed. Rio de Janeiro. 2020. p. 39 - 58.

CANADA. Government of Canada. **Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96**. Disponível em: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-11.html. Acesso em: 23 fev. 2021.

DONEDA, Danilo. **A proteção dos Dados Pessoais como um Direito Fundamental**. Disponível em: file:///C:/Users/caalm/AppData/Local/Temp/Dialnet-AProtecaoDosDadosPessoaisComoUmDireitoFundamental-4555153.pdf. Acesso em 22 mar. 2021.

BBC. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 12 jan. 2021.

KOEPSEL, Alice de Medeiros. **Adoção e Efeitos do Programa de Compliance à Luz da Lei Geral de Proteção de Dados Pessoais**. 2020. 71 p. Trabalho de Conclusão de Curso (Monografia) – Universidade do Sul de Santa Catarina, Santa Catarina, 2020.

CANADA. **Ten Privacy Principles**. Disponível em: https://www.legalaid.on.ca/privacy-policy/ten-privacy-principles/. Acesso em: 26 fev. 2021.

LIMA, Ana Júlia Andrade Vaz. **Programa de Integridade na Lei nº. 12.846/2013. 2018**. Dissertação (Mestrado em Direito). Pontifícia Universidade Católica de São Paulo PUC-SP, São Paulo, 2018.

MAGALHAES, Mariana Cardoso. **LGPD e a vigência em tempos de coronavírus**. Disponível em: https://www.migalhas.com.br/depeso/329594/lgpd-e-a- vigencia-em-tempos-de-coronavirus. Acesso em: 25 jun. 2020.

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

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Forum:** Challenges and Opportunities of Advertising Today. Disponível em: https://marcomm.mccarthy.ca/pubs/share4.htm. Acesso em: 23 fev. 2021.

SANTOS, Viviane Bezerra de Menezes. **Lei Geral de Proteção de Dados: Fundamentos do Compliance**. 2019. Trabalho de Conclusão de Curso (Monografia). Universidade Federal do Ceará, Fortaleza, 2019.

QIAN. Sun. **China's social credit system was due by 2020 but is far from ready**. Disponível em: https://algorithmwatch.org/en/story/chinas-social-credit-system-overdue/. Acesso em 21 fev. 2021.

UNIÃO EUROPEIA. UNIÃO EUROPEIA. **Collaboration in Research and Methodology for Official Statistics**. Disponível em: https://ec.europa.eu/eurostat/cros/content/personal-data_en . Acesso em: 22 mar. 2021.

ZANATTA, Rafael Augusto Ferreira. **Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica?**. 2017. Rede de Pesquisa em Governança da Internet, 2017. Disponível em: http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf. Acesso em: 22 mar. 2021.

AGRADECIMENTOS

A Deus, pelas diversas oportunidades e desafios que recebi até hoje, mas principalmente por Seu Amor.
Aos meus pais, pelos exemplos que foram e são para mim, assim como aos meus irmãos, sem os quais eu não viveria com tanta alegria, como vivo hoje, nem teria aprendido a importância da fraternidade.
Aos amigos que puderam acompanhar esta trajetória até o final, ao meu lado, me ajudando a superar cada uma das dificuldades, me alegrando, me ensinando sobre as belezas mais diversas e profundas do dia a dia.
Ao meu namorado, que me viu passar por diversos momentos de euforia e de desânimo, por ter sentado ao meu lado enquanto eu escrevia o presente artigo, me mantendo firme nos meus propósitos.
Ao meu terapeuta, por ter sido um verdadeiro amigo, em muitos momentos, inclusive para a conclusão deste trabalho.
Ao meu orientador, que generosamente fez uma solicitação para me inserir nas vagas dos seus orientandos, por sua disponibilidade e bom humor tão necessários no final do curso.
Aos profissionais da área com quem convivo, que são exemplos de trabalhadores, de familiares e de amigos, por me ensinarem com paciência e zelo nos anos em que estive com eles.