UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
MESTRADO PROFISSIONAL

MICHELLE JOCIANE ALI ZINI

PROTEÇÃO DE DADOS PESSOAIS NO MUNDO EMPRESARIAL NO CENÁRIO DA LGPD NO BRASIL: uma proposta de *Framework*

Porto Alegre
2020

Michelle Jociane Ali Zini

Proteção de Dados Pessoais no Mundo Empresarial no Cenário da LGPD no Brasil: uma proposta de *Framework*

Dissertação apresentada como requisito parcial para obtenção do título de Mestre, pelo Programa de Pós-Graduação e Mestrado Profissional em Direito das Empresas e dos Negócios da Universidade do Rio dos Sinos – UNISINOS.

Orientador: Prof. Dr. Wilson Engelmann

Porto Alegre

2020

Z77p Zini, Michelle Jociane Ali
Proteção de dados pessoais no mundo empresarial no cenário da LGPD no Brasil: uma proposta de framework. / Michelle Jociane Ali Zini -- 2021.
122 f. : il.; color. ; 30cm.

Dissertação (Mestrado) -- Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação e Mestrado Profissional em Direito das Empresas e dos Negócios da, 2021.
Orientador: Prof. Dr. Wilson Engelmann.

1. Direito à privacidade. 2. Tratamento de dados pessoais. 3. Empresa brasileira - Adaptação - Lei Geral de Proteção de Dados. 4. Framework. I. Título. II. Engelmann, Wilson.

CDU 343.45

Catalogação na Publicação: Bibliotecário Eliete Mari Doncato Brasil - CRB 10/1184

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA EMPRESA E DOS NEGÓCIOS
NÍVEL MESTRADO PROFISSIONAL

O Trabalho de Conclusão de Curso intitulado: **"PROTEÇÃO DE DADOS PESSOAIS NO MUNDO EMPRESARIAL NO CENÁRIO DA LGPD NO BRASIL"**, elaborado pela mestranda **Michelle Jociane Ali Zini,** foi julgado adequado e aprovado por todos os membros da Banca Examinadora para a obtenção do título de MESTRE EM DIREITO DA EMPRESA E DOS NEGÓCIOS - Profissional.

Porto Alegre, 23 de setembro de 2020.

(Participação por webconferência)
Prof. Dr. **Wilson Engelmann**
Coordenador do Programa de Mestrado Profissional em Direito da Empresa e dos Negócios

Apresentada à Banca integrada pelos seguintes professores:

Orientador: Dr. Wilson Engelman	(Participação por webconferência)
Membro: Dr. Cristiano Colombo	(Participação por webconferência)
Membro: Dra. Raquel Von Hohendorff	(Participação por webconferência)
Membro Externo: Dra. Salete Oro Boff	(Participação por webconferência)

AGRADECIMENTOS

Agradeço a Deus por ser a minha essência de vida.

Ao meu marido, Josué Zini, por sempre estar ao meu lado, fazendo-me crer que sou bem melhor do que realmente sou.

A meus filhos, Davi Enrico e Natália Ali Zini, por alegrarem a minha vida mesmo nos dias de tribulação.

Agradeço à minha mãe, Celanira Ali, por suas orações diárias e seus cuidados incansáveis de avó.

Ao meu irmão, Marcelo Ali, por sempre me auxiliar nos estudos, desde o primário até aqui.

À minha sogra, Vera Zini, por ter dedicado longos dias cuidando da minha família e de mim para que esta pesquisa fosse concluída com êxito.

À minha grande amiga e colega de profissão, Drª. Dione Luiza Ferreira, pelas incansáveis horas disponibilizadas em meu favor para que esse estudo fosse concluído.

Agradeço ao meu brilhante Orientador, Prof. Dr. Wilson Engelmann, a quem tanto admiro, por muito ter me ajudado na caminhada até aqui, pois mostrou-me, mesmo quando eu tive dúvidas, que eu conseguiria terminar este trabalho e obteria o tão sonhado título de Mestre.

“Feliz é o homem que persevera na provação, porque depois de aprovado receberá a coroa da vida, que Deus prometeu aos que o amam”.

Tiago, 1:12

RESUMO

Esta dissertação se propõe a estruturar um *Framework* a partir de alguns elementos considerados fundamentais na lei Geral De Proteção de Dados (LGPD) para esclarecer às empresas como vai funcionar o uso de dados pessoais após a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), Lei13.709/2018. Para tanto, fez-se um levantamento bibliográfico nos principais portais de periódicos de pesquisa, como o da CAPES, para formar base de dados documental e com fontes em outras áreas do conhecimento para, assim, elaborar o *Framework*. Nesse sentido, cabe dizer que o *Framework* foi constituído utilizando-se como base a perspectiva de *Framework* de Latham (2014). Como resultado da pesquisa, constatou-se que o *Framework* favorece a adaptação inicial das empresas brasileiras à LGPD. Também constatou-se que, a partir de um passo a passo a ser aplicado tendo em vista a implementação do chamado tratamento de dados pessoais, é possível proporcionar o atendimento a princípios indispensáveis à proteção de dados pessoais e trazer propostas confiáveis para as empresas. Isso se dá a partir das principais etapas da aplicação do passo a passo inicial do Framework por um empresário para cumprir a LGPD relativa aos dados pessoais como alternativa à adequação das empresas e como forma de mitigar os riscos aos quais os agentes estão expostos. Por fim, constatou-se que, com o formato de framework, inspirado parcialmente no modelo de Latham(2014), pode-se aplicar uma estrutura do Framework clara, identificando os pontos principais da LGPD e suas implicações, exigências relacionadas à lei, bem como a explanação sobre a sua violação ou inobservância. A partir desse instrumento, as empresas terão uma alternativa de solução de problemas propostos que, no caso em tela, é a adequação das empresas à LGPD, a qual foi aplicada a partir do *Framework* o conteúdo do Capítulo II, Seção I, do Art. 7º ao 10º da LGPD.

Palavras-chave: Tratamento de dados pessoais. Adaptação das empresas brasileiras à LGPD. *Framework*. Privacidade de dados.

ABSTRACT

This dissertation proposes to structure a Framework based on some elements considered fundamental in the General Data Protection Law (GDPL) in order to make it possible for companies to know how the use of personal data will work, after the General Data Protection Law (GDPL) L.13.709/2018 comes into force. For the development of the research, bibliographic research was used through access to databases such as the CAPES periodicals portal, documentary research and sources in other areas of knowledge were sought for the development of the Framework; a Framework was built from some ideas inspired by the perspective of Jonh R. Latham's Framework (2014). As a result of the research it was observed that the Framework is able to allow the initial adaptation of Brazilian companies to GDPL, with a step-by-step to be applied to the implementation of the so-called personal data processing, provided the fulfillment of principles indispensable to the protection of personal data and brought reliable proposals, with the main steps that an entrepreneur should observe and as an initial step to comply with GDPL regarding personal data as an alternative in the adequacy of companies and ways to mitigate the risks that agents are exposed. In the end. It is noted that with the Framework companies will have an alternative solution to proposed problems which, in this case, is the adequacy of companies to GDPL, where the content of Chapter II, Section I, of Article 7 to 10 of GDPL was applied through the Framework.

Keywords: Personal data processing, adaptation of Brazilian companies to LGPD, Framework, privacy.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AEPD	Agência Espanhola de Proteção de Dados
ARPANET	Advanced Research Projects Agency Network
CDC	Código de Defesa do Consumidor
CEDIS	Centro de Direito, Internet e Sociedade
CF	Constituição Federal
CGU	Controladoria Geral da União
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
ECEUROPA	Comissão Europeia
EU	União Europeia
EUA	Estados Unidos da América
GDPR/RGPD	Regulamento Geral de Proteção de Dados
IBGE	Instituto Brasileiro de Geografia e Estatística
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da *Internet*
MP	Medida Provisória
NBR	Norma Técnica Brasileira
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
PLC	Projeto de Lei da Câmara
SGSI	Sistema de Gestão de Segurança da Informação
STJ	Superior Tribunal de Justiça
TJUE	Tribunal de Justiça da União Europeia
UNISINOS	Universidade do Vale do Rio dos Sinos

SUMÁRIO

1 INTRODUÇÃO

No atual mundo globalizado, onde quase estudo está ao alcance de todos a partir de um clique, o Direito precisa adequar-se às necessidades da sociedade. Essas necessidades estão, cada vez mais, inseridas no mundo digital. Por conta dessa inserção ao mundo digital, surge a necessidade de proteger, de forma adequada, os dados pessoais de cada cidadão.

Os dados pessoais, considerando a importância que apresentam na sociedade contemporânea e o poder que eles carregam consigo, mereceram, recentemente, proteção mais específica no contexto da União Europeia, a saber: a) Diretiva 2016/680: relativa à proteção dos dados destinados às autoridades policiais e judiciárias (EURO-LEX, 2020); b) Regulamento 45/2001, que se aplica ao tratamento de dados pessoais por órgãos ou agência da União (EURO-LEX, 2020); c) Diretiva 2000/31, trata do Comércio Eletrônico. (EURO-LEX, 2020).

Na sequência da proteção jurídica aos dados no âmbito da União Europeia, entrou em vigor em maio de 2018 e trouxe uma nova regulamentação o chamado, em português, Regulamento Geral de Proteção de Dados - RGPD (ECEUROPA, 2020). Para Lima (2018), a GDPR pretende ser a mais completa e melhor regra de privacidade e proteção dos dados pessoais e do seu livre movimento (LIMA, 2018).

A partir da inspiração na GDPR, o Poder Legislativo, no Brasil, aprovou a Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018. Essa Lei dispõe sobre a proteção, o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado no Brasil e altera a Lei 12.965, de 23 de abril de 2014, o Marco Civil da *Internet* (BRASIL, 2018). Para Cartaxo (2018), a LGPD tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Com a revogação, a LGPD passou a determinar que as empresas deveriam ter uma política de privacidade obrigatória, na qual seria indispensável exigir o prévio consentimento dos usuários no que concerne à entrega de seus dados pessoais. Passa a ser exigido um propósito específico e explícito nessa entrega de informações na *Internet*.

Em relação à Lei 12.965/14, cabe dizer que ela ficou conhecida pelo nome de Marco Civil da *Internet* (BRASIL, 2014), porque estabelecia princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil.

Com base nas premissas descritas e para cumprir com os objetivos propostos, a presente dissertação estrutura-se de forma a trazer, no primeiro capítulo, um compilado histórico da LGPD, com os marcos para o desenvolvimento da privacidade e do princípio do direito de personalidade, levando em conta apontamentos sobre princípios anexos, como o da intimidade e da vida privada. Por derradeiro, explana sobre a consequente evolução da proteção de dados no Brasil.

No segundo capítulo, apresentam-se os impactos nas operações de negócios com as inúmeras prorrogações para a entrada em vigor da Lei 13.709/2018, bem como a descrição do panorama da proteção de dados na LGPD e a GDPR como modelo para a legislação brasileira. Por fim, o capítulo também aborda o tratamento e os desafios do tratamento de dados.

No terceiro e último capítulo, aborda-se o *compliance* como forma de mitigação de riscos, os padrões de segurança que as empresas devem seguir, os termos de uso, as políticas de privacidade como melhores práticas a serem seguidas. Ao final, propõe-se um *Framework* como alternativa para as empresas se adequarem a LGPD.

Tomando em consideração esse panorama, esta pesquisa visa a estruturar um *Framework,* viabilizando a adaptação das empresas brasileiras à LGPD, definindo procedimentos e práticas à implementação do chamado “tratamento de dados pessoais”, a fim de mitigar os riscos envolvidos nesse aspecto da nova Lei aos possíveis impactos para as empresas no que tange ao armazenamento de dados.

1.1 Tema

O tratamento de dados pessoais à luz da LGPD.

1.2 Delimitação do tema

O impacto da LGPD na proteção e na privacidade dos dados pessoais no cenário empresarial, especialmente no que se refere aos procedimentos e às práticas para a implementação do chamado tratamento de dados. Trata-se também dos riscos envolvidos nesse aspecto com a não adequação à nova lei, as formas de mitigação e o tratamento de dados pessoais da LGPD, disponíveis do Art. 7º ao Art.10º. Leva-se em consideração o término desta pesquisa, que ocorreu no dia 2 de abril de 2020, antes da entrada em vigor da LGPD.

1.3 Problema de pesquisa

Com a chegada da LGPD, em 18 de setembro de 2020, as empresas tiveram que se adaptar a novas regras de proteção de dados. Essas novas regras afetaram todas as transações referentes ao processamento de informações de dados dos cidadãos brasileiros. Diante desse cenário, consideramos pertinente investigar quais elementos devem integrar um *Framework* que viabilize a adaptação das empresas brasileiras à LGPD. Assim, cabe também investigar quais procedimentos e práticas à implementação do chamado tratamento de dados pessoais podem ser utilizados a fim de mitigar os riscos envolvidos nas mudanças das novas regras trazidas pela LGPD.

1.4 Hipótese

Ao partirmos do pressuposto de que o tratamento dos dados pessoais se dará em todos os momentos, ou seja, em toda operação envolvendo dados pessoais, conforme dispõe Art. 5 da LGPD, podemos destacar:

> Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2018).

Além de ser capaz de atender e prever cada uma destas formas de tratamento dos dados, bem como do respectivo cuidado com cada forma, que envolve os requisitos descritos no capítulo II, seção I da LGPD, o *Framework* deverá viabilizar o atendimento de princípios, como: a transparência, a auditabilidade de cada uma das etapas de tratamento dos dados, a fim de dar conta do direito à explicação de alguma parte que tenha permitido o acesso aos seus dados pessoais.

1.5 Objetivos

1.5.1 Objetivo geral

Examinar os elementos que devem integrar um *Framework* a fim de mitigar os riscos envolvidos nesse aspecto da nova lei, além de viabilizar a adaptação das empresas brasileiras à LGPD, para definir procedimentos e práticas à implementação do chamado “tratamento de dados pessoais” (BRASIL, 2018).

1.5.2 Objetivos específicos

Analisar os Artigos de 7º a 10°, da LGPD, nos quais se estipulam especificamente os requisitos para o tratamento de dados pessoais;

Estudar as diversas interpretações doutrinárias sobre a operação “tratamento dos dados pessoais” a fim de propor um *Framework*, contendo os passos referentes ao tratamento de dados pessoais e as exigências para cada um deles a fim de orientar as empresas brasileiras.

1.6 Justificativa

O presente estudo merece destaque no âmbito acadêmico, social e empresarial devido ao objetivo de buscar elucidar, de forma analítica, a nova legislação de dados pessoais brasileira – LGPD, que entrou em vigor em meados do ano 2020, mas que já provoca uma série de alterações sistêmicas, cadastrais e culturais no mercado brasileiro.

O cuidado com o tratamento dos dados é um dos destaques da nova lei brasileira, dada a responsabilidade sobre o armazenamento e uso dos dados pessoais por quem quer que seja, trazendo uma série de consequências, tais como: multas, sanções, retratação pública e respeito às boas práticas em governanças coorporativas. A nova lei deve gerar uma conduta reputacional fundada no respeito à privacidade, na inviolabilidade da expressão, de informação, de comunicação, de opinião, da intimidade, da honra e da imagem da pessoa. Além disso, tem-se o favorecimento do livre desenvolvimento da personalidade, da dignidade e do exercício da cidadania das pessoas naturais.

Pretende-se, com o resultado do presente estudo, servir de apoio para as empresas melhor compreenderem a dinâmica, os termos e conceitos que a nova lei irá regulamentar. Para isso, ao final do presente estudo, propõe-se um *Framework*,

voltado para as empresas, sobre os desafios da implantação da LGPD no Brasil, especialmente pela ambiguidade da operação “tratamento de dados”.

Esta Dissertação pretende contribuir com o esclarecimento dessa operação, considerada uma das mais importantes da LGPD.

O tema desta Dissertação está em sintonia com os temas investigados na Linha de Pesquisa n. 1: “Direito da Empresa e Regulação”, do Mestrado Profissional em Direito da Empresa e dos Negócios da UNISINOS. Além disso, o tema também se encontra alinhado ao projeto de pesquisa do orientador, intitulado: “Direito, Novas Tecnologias e Inovação”, além dos trabalhos e investigações realizadas no âmbito do Grupo de Pesquisa Jusnano, credenciado junto ao CNPq.

1.7 Metodologia

1.7.1 Tipos de pesquisa

A metodologia consiste em uma série de parâmetros e padronizações por meio da qual os pesquisadores das mais diversas áreas do conhecimento podem efetuar suas pesquisas e trabalhos de maneira organizada, delimitada, criteriosa e rigorosamente científica. Isso é fundamental para garantir que o trabalho seja academicamente válido, trazendo problemas, hipóteses e objetivos factíveis, pertinentes e adequados ao estado em que se encontra o problema em questão.

A metodologia, segundo Siena (2017), pode ser entendida como a etapa na qual se explicitam as abordagens e os procedimentos que serão adotados na realização da pesquisa, de modo que outra pessoa possa reaplicá-la. No presente estudo, utiliza-se a metodologia de fundamentação teórica e estudo prático.

O passo inicial para se iniciar uma pesquisa é a definição do objetivo e da abordagem, que pode ser qualitativa, quantitativa ou uma combinação destas, sendo essa última a hipótese do presente estudo. Só após a definição do tipo de procedimentos metodológicos a serem adotados é que se iniciam a pesquisa e a aplicação do estudo.

O presente trabalho tem como metodologia a pesquisa bibliográfica e abrange a pesquisa científica, recorrendo-se metodologicamente ao estudo exploratório qualitativo, por meio de acesso a bases de dados, como o portal de periódicos da

CAPES, a pesquisa documental, além de fontes em outras áreas do conhecimento para a elaboração do *Framework*.

É importante ressaltar aqui que o material disponível em relação ao assunto específico da proteção de dados pessoais ainda é escasso, em especial porque a LGPD sequer entrou em vigência até o fechamento deste estudo, sendo essa a deficiência na literatura existente. (MACHADO, 2017).

2 EVOLUÇÃO HISTÓRICA

Neste capítulo, traça-se um compilado histórico da LGPD, com os marcos para o desenvolvimento da privacidade e o princípio como direito de personalidade, trazendo apontamentos sobre princípios anexos, como o da intimidade e da vida privada. Por derradeiro, disserta-se sobre a consequente evolução da proteção de dados no Brasil.

Nunca antes em sua história a humanidade passou por um período de tantas inovações e crescimento como o atual. Fenômenos como a globalização, a revolução tecnológica e a invenção da *Internet* fizeram o planeta dar um salto quantitativo em relação à modernidade. Na esteira de tais fenômenos, houve a consequente diminuição da privacidade e o aumento de abusos, tais como o acesso a dados privados de cidadãos sem autorização prévia.

Para Mendes (2014), a proteção à privacidade, em seus primórdios, vem com uma perspectiva totalmente individualista, com grande preocupação no direito de ser deixado só (*right to be alone).* Essa visão ganhou forças a partir das suas características de direito negativo com a não intervenção Estatal no que concerne às garantias da vida privada.

No decorrer do século XX, a transformação da função do Estado, aliada à revolução tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade. (MENDES, 2014).

Nas lições de Boff, Fortes e Freitas (2018), revela-se uma cultura que se preocupa com a circulação das informações, na metade do século XX, durante a guerra fria. Com a criação da ARPANET[1] que surge como uma rede de computadores autônomos e capazes de distribuir informações.

De acordo com Boff, Fortes e Freitas (2018), a partir da criação do computador e do surgimento da *Internet*, nos EUA, na Califórnia (Vale do Silício), nos anos 70, ocorreu uma revolução da informação. Para que isso ocorresse, contou-se com mão de obra especializada, conhecimentos de tecnologia e empresas, os quais também estão em constante atualização.

Diante dessa revolução da informação, o Estado passou a influenciar no modo de inovação tecnológica e começa a comandar a economia.

---

[1] ARPANET é a ideia de construção de uma rede de computadores que pudesse trocar informações.

> O grande progresso tecnológico que se deu no início dos anos 1970 pode, de certa forma, ser relacionado à cultura da liberdade, inovação individual e iniciativa empreendedora oriunda dos *campi* norte-americanos da década de 1960. (CASTELLS, 2018, p. 25, grifo do autor).

Para Castells (2018, p. 430), “[...] a Internet é a espinha dorsal da comunicação global mediada por computadores”.

O avanço tecnológico e o aquecimento da economia são fatores mundialmente relevantes e trazem a necessidade de proteção dos direitos fundamentais, tais como o da privacidade do indivíduo. Com isso, a análise de marcos internacionais, no que se refere ao desenvolvimento e à evolução do direito à privacidade, torna-se relevante.

2.1 Marcos internacionais para o desenvolvimento do direito à privacidade

A seguir, como forma de elucidar o caminho percorrido e os avanços do direito da privacidade no decorrer do tempo, a exposição de marcos internacionais sobre o desenvolvimento do direito à privacidade e o modo como ele vem sendo aplicado e compreendido pelo ordenamento jurídico nacional e internacional, buscamos compreender a formação conceitual da privacidade e do direito à privacidade e expor como esse direito é exercido diante das ferramentas tecnológicas disponíveis na atualidade.

O direito à privacidade, para Magrani (2019), está fortemente relacionado aos direitos à proteção da dignidade e da personalidade humanas. Além disso, é consequência da importância que a Constituição Federal de 1988 tem dado à intimidade, à vida privada e à inviolabilidade de dados. No âmbito internacional, não tem sido diferente: prova disso são os marcos internacionais no que diz respeito ao desenvolvimento da privacidade, como passamos a apresentar a seguir.

2.1.1 Declaração de Direitos do Homem e do Cidadão (1789)

A Declaração de Direitos do Homem e do Cidadão traz os direitos e os deveres naturais e inalienáveis e sagrados do homem como forma de coibir a corrupção governamental. Assim:

> Declaração de Direitos do Homem e do Cidadão. Em 1789 A França já dispunha de uma Lei que assegurava aos seus cidadãos direitos fundamentais, como pode ser observado em seu preambulo e no seu artigo 4º: DECLARAÇÃO DOS DIREITOS DO HOMEM E DO CIDADÃO DE 1789 Os representantes do povo francês, constituídos em ASSEMBLEIA NACIONAL, considerando que a ignorância, o esquecimento ou o desprezo dos direitos do homem são as únicas causas das desgraças públicas e da corrupção dos Governos, resolveram expor em declaração solene os Direitos naturais, inalienáveis e sagrados do Homem, a fim de que esta declaração, constantemente presente em todos os membros do corpo social, lhes lembre sem cessar os seus direitos e os seus deveres; a fim de que os actos do Poder legislativo e do Poder executivo, a instituição política, sejam por isso mais respeitados; a fim de que as reclamações dos cidadãos, doravante fundadas em princípios simples e incontestáveis, se dirijam sempre à conservação da Constituição e à felicidade geral. Artigo 4º- A liberdade consiste em poder fazer tudo aquilo que não prejudique outrem: assim, o exercício dos direitos naturais de cada homem não tem por limites senão os que asseguram aos outros membros da sociedade o gozo dos mesmos direitos. Estes limites apenas podem ser determinados pela Lei. (MPF, 2020).

O Artigo 4º traz a ideia de liberdade como um direito natural inalienável e imprescindível contra a desgraça pública e a corrupção dos governos. Essa Lei foi acompanhada no século seguinte por diversas outras que configuraram verdadeiros marcos entre as nações.

2.1.2 Art. 12 da Declaração Universal dos Direitos Humanos (1948)

Em seu Artigo 12, a Declaração Universal dos Direitos Humanos traz, em seu escopo, a proteção à vida privada dentro dos direitos à proteção da dignidade e da personalidade humanas.

> Art. 12
> Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. (NAÇÕES UNIDAS, 2009, p. 3).

De acordo com Fico e Mota (2020), o conceito de proteção de dados vem sendo usualmente atrelado ao conceito da privacidade, direito que é reconhecido internacionalmente como um direito humano, ao menos desde a Declaração Universal de Direitos Humanos em 1945. (FICO; MOTA, 2020).

2.1.3 Art. 5 da 9ª Conferência Internacional Americana (1948)

No mesmo ano de surgimento da Declaração Universal de Direitos Humanos, surge a Declaração Americana sobre os Direitos e Deveres do Homem, ratificando os direitos fundamentais já definidos pelas suas antecessoras, fortificando a ideia de proteção a personalidade.

De acordo com a Conferência Internacional Americana, “Art. 5. Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular”. (OEA, 1948).

Silva (2012) defende que os direitos fundamentais são definidos como o conjunto de direitos e garantias do ser humano, cuja finalidade principal é o respeito a sua dignidade, com proteção ao poder estatal e a garantia das condições mínimas de vida e desenvolvimento do ser humano. Desse modo, visa garantir ao ser humano o respeito à vida, à liberdade, à igualdade e à dignidade para o pleno desenvolvimento de sua personalidade.

2.1.4 Art.8º da Convenção Europeia dos Direitos do Homem (1950)

Dois anos mais tarde, a Europa, na mesma caminhada em prol da privacidade do indivíduo e limitando a autonomia do estado, em seu Art. 8º, prevê a interferência pública somente nos casos previstos em lei:

> ART. 8°
> Direito ao respeito pela vida privada e familiar 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a *protecção* da saúde ou da moral, ou a *protecção* dos direitos e das liberdades de terceiros. (CONSELHO DA EUROPA, 2013, p. 3).

É inegável a relevância do direito à privacidade do homem em uma sociedade democrática e em constante transformação. Além disso, a Convenção Europeia dos Direitos do Homem, em 1950, em seu Art. 8º, já vislumbrava essa relevância ao

resguardar o respeito da vida privada e familiar, bem como do domicílio e das correspondências de seus cidadãos.

Segundo Lovato (2015), direitos fundamentais significam os direitos do ser humano reconhecidos e positivados em esfera constitucional de um Estado determinado. Em outras palavras, direitos fundamentais são aqueles previstos e protegidos constitucionalmente, observando-se que nos demais países costumam ser positivados também pela sua Constituição da República.

2.1.5 Conferência Nórdica sobre o Direito à Intimidade (1967)

Quase duas décadas mais tarde, a preocupação com a privacidade toma contornos de cunho mundial a partir da Conferência Nórdica sobre o Direito à Intimidade, que ocorreu de 22 e 23 de maio de 1967. Nesse evento, juristas de todo o mundo se reuniram para discutir, em Estocolmo, sobre o direito à intimidade ou à privacidade nos termos do Art. 12 da Declaração Universal dos Direitos Humanos (NAÇÕES UNIDAS, 2018, p. 2). Nesse sentido, observa-se que:

> Art. 12 - Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Naquela oportunidade, foram estabelecidas premissas sobre o direito à intimidade da pessoa, tais como:

a) natureza do direito à privacidade – reconhecido como direito fundamental do homem e de viver só e com o mínimo de interferência;

b) direito ao sigilo – correspondência, telefônica e informações em geral;

c) limitações ao direito – trata da supremacia do direito público e de interesse geral, em que se poderia quebrar tal direito, mas obviamente bem definidos em lei para evitar abusos;

d) leis bem definidas sobre os direitos de intervenção da privacidade;

e) liberdade de expressão, informação e de debate;

f) proteção sobre leis já existentes nos campos civil e criminal.

Em suma, a conferência de Estocolmo ratificou a necessidade de proteção da vida privada e das suas informações. Certamente influenciou e contribuiu para o desenvolvimento de outras leis como a do presente estudo, a LGPD.

2.1.6 A Convenção Americana sobre Direitos Humanos (1969)

Essa Convenção, assinada em São José, na Costa Rica, foi ratificada no Brasil pelo Decreto 678/1992 (BRASIL, 1992). Esse Decreto informa, no Art. 11, a proteção à vida privada:

> Art. 11 – Proteção da honra e da dignidade. §1º – Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. §2º – Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. §3º - Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

2.1.7 Lei de Proteção de Dados do Estado de Hesse (1970)

Surgiu, na Europa, a primeira legislação a tratar da proteção de dados, denominada Hessisches Datenschutzgesetz. Trata-se da Lei de Proteção de Dados do Estado de Hesse, na Alemanha Ocidental.

2.1.8 Lei *Datalegen* (1973)

A Suécia passou a ser o país europeu pioneiro na criação de uma lei nacional sobre proteção de dados. Essa lei foi responsável por trazer conceitos como o registro central de informação de processamento de dados pessoais. Além disso, estabeleceu o procedimento de licenciamento, no qual o registro público foi aberto para votação dos cidadãos e consumidores, usado como uma ferramenta de cumprimento da lei pelas agências de proteção de dados. Esses conceitos e procedimentos foram o pilar das primeiras legislações europeias de proteção de dados. (DONEDA, 2010).

2.1.9 Diretiva Europeia de Proteção de Dados (1995)

De acordo com Monteiro (2018a), foi aprovada a Diretiva Europeia de Proteção de Dados em 1995. Tal diretiva nasceu antes da chamada globalização e da disseminação da *Internet* e das novas tecnologias, salientando-se que, naquele período, os modelos de negócios e o mercado era basicamente presenciais. Consequentemente houve uma drástica atualização, que resultou na atual Regulação Geral de Proteção de Dados da União Europeia - GDPR. (MONTEIRO, 2018a).

O Direito pátrio costuma denominá-lo como direito à privacidade, direito ao resguardo, direito à intimidade, direito ao recato e direito de estar só. Essa proteção deve ser reconhecida pelos ordenamentos jurídicos nacionais e internacionais de maneira positiva.

Assim, restou-se primordial a criação de normativas que regulassem o tratamento de dados pessoais no mundo todo. Mais recentemente, no Brasil, foi publicada a LGPD, em resposta a essa tendência mundial em trazer maior transparência nos processos de manipulação de dados pessoais dos cidadãos.

A Constituição Federal (BRASIL, 1988) elenca o rol de direitos fundamentais, dividindo-os em cinco capítulos. Cada capítulo é dedicado a diferentes tipos de direitos específicos. Ao detalharmos a letra “a”, identifica-se que ela se dedica aos direitos individuais e coletivos. Já na letra “b”, identifica-se a definição de direitos sociais que são aqueles direitos que a sociedade tem a itens básicos como educação. Na letra “c”, por sua vez, tem-se a definição de direitos de nacionalidade ligados ao indivíduo a um determinado Estado ou nação. (BRASIL, 1988).

> Os princípios de direitos fundamentais são, nessa concepção, expressão do arranjo jurídico-institucional possível no Estado Social e Democrático de Direito contemporâneo. O constitucionalismo que legitima esse Estado é, por definição, complexo e aberto às diferentes concepções de qualidade do ensino que buscam alcançar hegemonia na sociedade. Por esse motivo, como previne Alexy (2008), a resposta sobre qual deveria ser o conteúdo de um determinado direito fundamental sempre incluirá as valorações de quem resolve a questão. Essa é a razão pela qual o autor defende a complementaridade necessária entre as abordagens normativa e analítica, já que esta última permite a quem estuda um determinado direito estabelecer as bases a partir das quais constrói sua argumentação. Isso significa que, do ponto de vista normativo, não só é possível como é necessário responder racionalmente à questão sobre o conteúdo do princípio constitucional inscrito no inciso VII do Art. 206. (XIMENES, 2014, p. 1030).

Para Engelmann (2001), os princípios são os responsáveis pelo encadeamento das normas jurídicas na formação do sistema jurídico. Sempre serão necessários quando ocorrerem situações complexas, ou quando as convicções normativas não forem suficientes na resolução de um caso de forma mais acertada e imparcial.

Além dos princípios que são fundamentais e regem todo o ordenamento brasileiro, existem, ainda, os princípios inerentes e intrínsecos à proteção de dados pessoais. Esses princípios são considerados a espinha dorsal da LGPD e imprescindíveis para garantir a eficácia da norma. Os princípios próprios da proteção de dados têm imensa relevância dentro da legislação recentemente criada, pois trazem proteção ao tratamento de dados pessoais, tanto a quem receber a proteção, através de normas próprias, como também para a recolha e o tratamento de dados pessoais que as empresas e organizações devem observar e respeitar nos princípios inerentes a tais atividades.

Além disso, os princípios que regem a proteção de dados estão contidos no Art. 6º da Lei 13.709/2018. Esse artigo traz, de forma taxativa, o rol de princípios que devem ser observados e respeitados por empresas e organizações que realizam tratamento de dados, sob pena de responsabilização e aplicação de penalidade inclusive financeira.

Cabe destacar que o referido Art. 6° vem disciplinar, de maneira bastante específica, os princípios inerentes à proteção de dados, inclusive com relação ao uso e tratamento de dados pessoais pela administração e entes públicos. Disso depreende, com a análise detalhada do Art. 6º e seus incisos da Lei 13.709/2018, o que segue:

a) Princípio da finalidade:

De acordo com o Guia de Boas Práticas (BRASIL, 2020, p. 35), “A finalidade é o fundamento para que os dados sejam tratados. É primordial que seja estabelecido os motivos para que ocorra o tratamento, pois sem a finalidade não ocorrerá”.

Nas palavras de Maldonado e Blum (2018), esse princípio é de suma importância, efetivamente, uma vez que é a partir dele que se oferece ao titular uma garantia sobre a finalidade e o tempo em que serão usados os dados do cliente, restringindo os propósitos do tratamento. Visa a atenuar o risco de uso secundário sem o consentimento do titular.

b) Princípio da adequação:

Esse princípio está intimamente ligado ao princípio da finalidade. Para Magrani (2019, p. 109), “Os dados coletados devem ser usados apenas na medida que forem necessários para atingir os objetivos anteriormente informados e de acordo com o contexto do tratamento”.

c) Princípio da necessidade:

Ainda, para Magrani (2019, p. 109), “Apenas os dados indispensáveis para atingir a finalidade podem ser coletados, como indica o princípio da necessidade [...]”.

d) Princípio do livre acesso:

> Pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados [...]. (DONEDA, 2011, p. 100).

e) Princípio da qualidade dos dados:

Garante que os dados coletados sejam precisos:

> Qualquer imprecisão, seja um dado pessoal equivocado, seja desatualizado, pode ser catastrófico ao titular, como ocasionar um erro de tratamento médico. Recusa de crédito, vedação de participação em concursos públicos, eliminação em processo seletivo, ou, até mesmo, uma prisão injusta [...]. (MALDONADO; BLUM, 2018, p. 149).

f) Princípio da transparência (ou da publicidade):

> Pelo qual a existência de um banco de dados com dados pessoais, deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre a sua existência, ou do envio de relatórios periódicos [...]. (DONEDA, 2011, p. 100).

g) Princípio da segurança:

A falta de segurança para a LGPD é considerada como uma medida irregular. Maldonado e Blum (2018, p. 157) dispõem:

> [...] que tal princípio se mostra na LGPD acertadamente como uma regra, na medida que aduz que os agentes de tratamento devem ter medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

h) Princípio da prevenção, não discriminação e da responsabilização e prestação de contas:

De acordo com Maldonado e Blum (2019, p. 158, grifo dos autores),

> A prevenção esperada no princípio ora analisado deve ser pautada no conceito *Privacy by Design*, que é pautado em sete princípios fundamentais. (fl.158). No da não discriminação ela aduz que nada mais é do que a impossibilidade de uso dos dados para fins discriminatórios. E no que concerne ao da responsabilização e prestação de contas, diz que que não basta cumprir a LGPD, mas deve-se tomar todas as medidas para que a finalidade seja alcançada verdadeiramente de forma plena.

A LGPD traz, de forma ostensiva, um rol de princípios que devem ser observados e respeitados pelas empresas e organizações que trabalham com tratamento de dados. Dessa forma, com a entrada em vigor da referida lei, as empresas terão que adequar os tais princípios para que possam continuar com atividades de recolha e tratamento de dados.

Após os Marcos Internacionais para o Desenvolvimento do Direito à Privacidade, é faz mister um olhar para o direito de privacidade bem como para os dados como um direito de personalidade.

2.2 Direito à privacidade e os dados como novo direito de personalidade

A invasão da privacidade da pessoa, ligada ao acesso ilimitado de seus dados pessoais, nos tempos atuais, foi determinante para que a proteção da pessoa, da sua dignidade e do livre desenvolvimento de sua personalidade fossem tutelados como direito fundamental.

Nas lições de Colombo e Facchini Neto (2019, p. 2):

> [...] os direitos de personalidade têm como objeto os valores voltados ao ser humano, à dignidade da pessoa humana, seu respeito físico, moral e intelectual, tutelando sua identidade, liberdade, igualdade, existência e segurança, honra, reserva da vida privada e desenvolvimento da personalidade, revelando as suas raízes nos direitos humanos [...].

As violações aos direitos de personalidade, em tempos atuais, ou, como pontuam Colombo e Facchini Neto (2019, p. 2), “[...] no meio ambiente digital[...]”, “[...]

vem crescendo exponencialmente, em face da virtualização das relações humanas, diante do crescente número de pessoas que utilizam redes sociais[...]".

De acordo com Cantali (2009, p. 65), "Os direitos da personalidade são posições jurídicas fundamentais do homem, as quais lhe são inerentes, já que os homens as têm pelo simples fato de existir, são condições essenciais do seu ser e de vir[...]". Acerca desse direito, as palavras de Bauman (2004) são esclarecedoras:

> Quanto à 'morte do anonimato' por cortesia da *Internet*, a história é ligeiramente diferente: submetemos à matança nossos direitos de privacidade por vontade própria. Ou talvez apenas consintamos em perder a privacidade como preço razoável pelas maravilhas oferecidas em troca. Ou talvez, ainda, a pressão no sentido de levar nossa autonomia pessoal para o matadouro seja tão poderosa, tão próxima à condição de um rebanho de ovelhas, que só uns poucos excepcionalmente rebeldes, corajosos, combativos e resolutos estejam preparados para a tentativa séria de resistir. (BAUMAN, 2014, p. 20, grifos do autor).

Segundo o autor Rodotá (2008), de modo geral, nos seus primórdios, a privacidade não era tida como um direito natural e individual. Isso porque ela era trabalhada sob a ótica de ser o resultado de uma aquisição de privilégios, que decorriam de alguns raros grupos, o que representava a conotação elitista sob a qual foi erigida.

Esse direito, por vezes citado como o direito de ser deixado só nesses tempos, era tido como um abandono factual dos considerados mais fracos e que gozavam de menos privilégios dentro do cenário de violência social. (COSTA JÚNIOR, 1995). Porém, é importante mencionar que a privacidade, de uma forma muito menor, porém ainda presente, permeia as novas tecnologias como um método de promoção da igualdade e da paridade de tratamento entre os iguais. (COSTA JÚNIOR, 1995).

Os laços com os privilégios da burguesia, portanto, foram cortados, de modo que se começou a fomentar uma discussão acerca da proteção da privacidade. Esse fomento, na realidade, realizará muitos feitos mais para o futuro, visto que, atualmente, existem, sim, mecanismos que têm o objetivo de oferecer proteção, mas são isolados e não são amplos o suficiente. (BARROSO, 2004).

A sociedade da informação constrói-se pautada no acúmulo de informações, em conjunto com a circulação de informações. Segundo Rodotá (2008), essa sociedade da informação também possui a responsabilidade de estabelecer novas situações que envolveram o poder. Porém, para alcançar essa responsabilidade, há

uma dificuldade cada vez mais intensa: a compreensão de que o cidadão é apenas um provedor de dados.

A velha concepção que pautava o direito à privacidade como o direito de ser deixado só deu lugar a uma discussão que pleiteia a oportunidade de que indivíduos e coletividades tenham o controle sobre as informações que serão disponibilizadas a seu respeito. A discussão sobre o controle das informações toma corpo a partir da redação da LGPD, pois afere equilíbrio nas relações de poder que a informação tende a criar. (DONEDA, 2006). As regras que a LGPD pode implementar são padrões tanto para os setores privados como para o setor público.

Quando surgem novas tecnologias, o termo privacidade é utilizado como referência à possibilidade de o usuário conseguir conhecer, controlar e romper o fluxo de informações que a ele sejam relacionadas. Sob essa ótica, a privacidade é um direito que permite o controle sobre as próprias informações e a manutenção sobre elas. Atualmente, a privacidade é muito mais observada sob o ângulo da funcionalidade e abduz todas as formas de estigmatização social que possam ser originadas e decorrentes dela. (RODOTÁ, 2008).

Segundo o mesmo autor, a estratégia de defesa tem o objetivo de “[...] afastar os temores de uma iminente chegada do *1984* de Orwell ou do *Brave New World* imaginado por Aldouls Huxley”. (RODOTÁ, 2008, p. 4, grifos do autor). Nesse sentido, o indivíduo vive em uma engrenagem totalitária de uma sociedade sob o domínio total do Estado. Nesse domínio, tudo é feito coletivamente, mas cada indivíduo vive sozinho e sob a vigilância permanente desse Poder. Esse estado de controle apoia-se na repressão, na tecnologia, no culto do progresso. Com isso, os indivíduos são padronizados quanto as suas características e vontades. Com efeito, contrariamente ao Estado dominante imaginado pelas obras citadas, vivemos em um Estado Democrático de Direito, no qual a vida privada, a intimidade e a liberdade de expressão tomam contornos de direitos e de garantias fundamentais. Tais direitos e garantias embasam o princípio constitucional da dignidade da pessoa humana. De acordo com Sarmento (2016, p. 73), “No Brasil, a dignidade da pessoa humana figura como fundamento da Públic no Art. 1º, inciso III, da Constituição Brasileira”. Frente a essa realidade, passamos, a seguir, à análise dos direitos constitucionais que abarcam o princípio constitucional.

2.2.1 Estudo dos direitos que decorrem do princípio da dignidade da pessoa humana

Os principais fatores que motivaram, de forma determinante, a criação da Lei de Proteção de Dados foram, segundo Lemos, Adami e Sundfeld (2018):

a) Uso, cada vez maior, de dados pessoais:

Com a expansão da comunicação social mundial, que só foi possível a partir da criação da rede mundial de computadores (*Internet*), os usuários desta rede de informações são tidos como indivíduos singulares. Isso porque estão inseridos em um ambiente amplo, cujos usuários são pessoas físicas, jurídicas, instituições e governos.

Nas palavras de Pinheiro (2018b, p. 47, grifo do autor), “A *Internet* é mais que um simples meio de comunicação eletrônica, ela é formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de Indivíduos”. Cabe afirmar que a sociedade atual tornou-se uma geradora de dados em alta escala, e muitos desses dados são hipóteses com as quais, diariamente, deparamo-nos numa coleta de dados pessoais.

É importante salientar que nossos dados pessoais são fornecidos nas mais diferentes atividades diárias, mas também nos registros, tais como: o de nascimento, o de casamento, o militar, o de pesquisa de Censo, o registro de escola, de contratação de seguros, de empregados particulares e públicos, de defesa civil, os financeiros, de dados telefônicos, de fornecimento de dados em operações comerciais via *Internet* ou presencial, entre outros.

Segundo Doneda (apud MARTINS, 2014, p. 61), “Os dados pessoais acabam por identificar ou mesmo representar a pessoa em uma série de circunstâncias nas quais sua presença física não é possível ou conveniente”.

b) O recurso mais valioso do mundo não é mais petróleo, mas dados. (MONTEIRO, 2018b).

Da análise dessa afirmativa, podemos inferir que os dados pessoais que circulam pela *Internet* são uma extensão da nossa inteligência/vontade. S*martphones* ou computadores, redes sociais, aplicativos de geolocalização levam-nos, sob a ótica mundial, à inteligência global digital, também chamada de Big Data.

Podemos referir que os dados pessoais, atualmente, são tão valiosos quanto o petróleo, no sentido de que todo aquele que souber fazer uso de forma correta, segundo toda legislação vigente, só tem a ganhar no manejo dessas informações. É importante mencionar que os dados pessoais, assim como o petróleo, necessitam de

refinamento/mineração para a melhor utilização dos dados. No entanto, no caso dos dados, segundo Mendes (2014, p. 109), “O objetivo da mineração de dados é a extração de inteligência significativa e de padrões de conhecimento, partindo de um banco de dados, por meio de sua ordenação e transformação”.

Dito isso, é importante descrever que a riqueza dos dados pessoais não está nos dados em si, mas na capacidade de serem analisados e transformados em inteligência coletiva. Como resultado da análise dos dados, são indicadas as descobertas capazes de transformar o cenário de organizações de diferentes mercados e, assim, influenciar no destino do mundo.

Por outro lado, no um oposto do que ocorre com o valor do petróleo, os dados pessoais são valorizados porque não necessitam ser procurados, tampouco manuseá-los da melhor forma. Com certeza, estará frente à mais nova fortuna.

c) Era digital, redes sociais, “*analytics*” surgem com a revolução da Era Digital a partir dos anos de 1990:

Com a era digital, passou a ser necessário regulamentar a proteção de dados pessoais, uma vez que teve início um novo modelo de transações e negócios comerciais veiculados por meio do ambiente digital.

Segundo Pinheiro (2018a), o motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais, de forma mais consistente e consolidada, tem origem nos anos 1990, quando se iniciou o próprio desenvolvimento do modelo de negócios da economia digital. Esse modelo passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

Em se tratando de rede social, os indivíduos estão cada vez mais conectados em mídias sociais digitais, nas quais o conteúdo publicado pode acarretar prejuízos irreparáveis. Estes conteúdos, quando publicadas e compartilhadas geram um fluxo de livre acesso e sem fronteiras. (PINHEIRO, 2018b). Portanto, é a partir da “*analyctis*” que podemos conceituar como a transformação de um volume grande de dados em informações úteis, fazendo com que os dados adquiram valor.

Segundo Frazão (2017, p. 23), “[...] a possibilidade de extrair correlações, padrões e associações que possam ser consideradas informações ou mesmo conhecimento a partir dos dados” com o uso de algoritmos e máquinas responsáveis para o processamento desses dados é cada vez mais comum.

d) Com a criação da LGPD, há a possibilidade de impactos nas vidas das pessoas, negócios e até nas eleições, pois o usuário da rede terá a oportunidade de dispor de suas informações pessoais de forma mais transparente:

Nas palavras de Pinheiro (2018b, p. 42):

> Logo, o pano de fundo da nova regulamentação está em se trazer o empoderamento sobre o controle da gestão dos dados pessoais para o usuário titular legítimo dos dados, que poderá saber com mais transparência o que está sendo feito com sua informação por parte das empresas [...].

O princípio da transparência passa a ser fundamental no tratamento de dados, trazendo uma linguagem mais simples, com mais clareza para o titular de dados. Isso, de acordo com Pinheiro (2018b), proporciona um empoderamento ao dono dos dados sobre como seus dados pessoais estão sendo tratados. Assim, cumpre mencionar que tais impactos também ocorrerão para as empresas, caso não venham a se adequar a LGPD.

Ao analisarmos os impactos da LGPD, percebemos que atividade negocial, segundo o entendimento de Mendes (2014, p. 96):

> O fornecedor deve adotar todas as medidas técnicas e procedimentais necessárias para garantir a segurança dos dados pessoais processados, levando em conta, especialmente, a rápida evolução tecnologia e o surgimento de novos riscos e ameaças.

No que se refere ao impacto causado nos pleitos eleitorais, é importante considerar o fato de estarmos imersos em uma realidade na qual as *fake news*, bem como os disparos em massa, prestam-se a fragilizar nossa jovem democracia, haja vista o surgimento de novas tecnologias, bem como o uso da inteligência artificial, com o objetivo de aumentar a polarização das informações e conquistar o voto do eleitor. (PIERGALLINI *et al*., 2020).

Com aumento das pessoas conectadas à *Internet*, surge um novo negócio com finalidade econômica: a postagem em sites sensacionalistas para difundir notícias falsas. O certo é que muitas pessoas leem essas notícias e passam a compartilhá-las sem tomar a precaução de checar a veracidade de tais conteúdos. Segundo Coura (2017, p. 24, grifo do autor), “É possível ser remunerado por essa prática graças aos anúncios do *Google Adsense*”.

Como exemplo da finalidade econômica da divulgação de notícias falsas, segundo Coura (2017, p. 45), “Nos Estados Unidos, um dono de um site de notícias falsas afirmou em entrevista ao Washington Post arrecadar US$ 10 mil dólares por mês com a prática”.

Na esteira do escândalo ocorrido nas eleições norte-americanas de 2018, quando foram usados, sem o consentimento da população, os dados pessoais de 87 milhões de usuários do *Facebook*, não há como não gerar o pavor de que, no Brasil, de igual forma, sejam usados os dados pessoais dos usuários da rede para o benefício próprio de um ou outro político. Diante desse temor, fez crescer, no Brasil, o debate acerca da regulação do marketing eleitoral e o consequente abuso no uso dos dados pessoais.

A LGPD não prevê nenhuma hipótese de segurança dos dados pessoais no tocante aos fins político-partidários, bem como para campanhas eleitorais. Assim sendo, caberá à legislação específica um aprimoramento no sentido de não permitir o uso dos dados pessoais conforme preconizado pela LGPD. (PIERGALLINI, 2020).

e) Ausência de um marco regulatório nacional quanto à proteção de dados:

A LGPD foi criada na esteira da promulgação da GDPA na União Europeia. Até este momento, no Brasil, só tínhamos o Marco Civil da *Internet*, que trouxe uma inovação legislativa, pois regulou matéria até então estranha ao ordenamento jurídico. É importante salientar que o Marco Civil da *Internet*, segundo Pinheiro (2018a, p. 17), “[...] tem como fundamento principal o direito à liberdade de expressão e assim privilegia a manutenção de informação publicada na rede em detrimento da imediata remoção do conteúdo”.

Assim sendo, na ausência de lei, no Brasil, para disciplinar a proteção dos dados pessoais, e, ainda, em consonância com a regulamentação da matéria pela GDPA em solo europeu, surge a LGPD no âmbito da chamada sociedade da informação. (MENDES, 2014).

f) Acontecimentos recentes e outros fatores:

Segundo Pinheiro (2018a, p. 34, grifos do autor):

> Muitas mudanças ocorreram no mundo após os escândalos trazidos pelo ex-agente da *National Security Agency*, Edward Snowden, especialmente quanto à espionagem praticada pelo governo norte-americano nos computadores de milhões de usuários ao redor do planeta.

g) *Cambridge Analytic*:

Trata do recente caso da Cambridge Analytic, que serve para exemplificar como e com qual finalidade funcionam a invasão e o uso dos dados pessoais dos usuários da rede. De acordo com Araújo (2018, p. 31, grifo do autor):

> Por meio do tratamento dos dados pessoais de cada usuário coletados no Facebook, a empresa conseguiu desenvolver perfis 'psicográficos' para cada usuário e permitir um direcionamento de discurso ainda mais subjetivo.

Anteriormente, esse tema já foi assunto de pesquisa da Universidade de Cambridge, com a publicação de artigo no sentido de que todo o conteúdo disposto na rede social *Facebook* que recebe "curtida" serve para construir traços da personalidade do titular da rede. De posse desses dados, foram cruzados com os dados de preferência, tendo como resultado um padrão. Essa técnica serviu para que a empresa Cambridge Analytics, na corrida eleitoral americana, levasse Donald Trump ao poder. (ARAÚJO, 2018).

h) GDPR surge da necessidade de regulamentar a proteção dos dados pessoais e ganha uma maior importância a partir dos anos 1990, tendo como origem o modelo de negócio da economia digital:

Nessa nova forma de realização de negócios, o fluxo de dados toma uma dimensão internacional, em especial aos que dizem respeito às pessoas e dentro dos avanços trazidos pela nova realidade tecnológica e pela globalização.

É no contexto de regulamentar a proteção dos dados pessoais que foi promulgada, na União Europeia, o Regulamento GDPR Europeu nº 679, aprovado em 27 de abril de 2016. Segundo Pinheiro (2018a, p. 18, grifo do autor), "[...] teve como objetivo abordar a proteção dos dados das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido pela expressão *free data flow*".

Com a GDPR, na esteira da regulamentação europeia, os países e empresas que tivessem interesse em manter relações comerciais com a União Europeia deveriam adequar-se a uma legislação no mesmo nível da GDPR. Com efeito, países que não possuíssem uma lei do calibre da GDPR ficariam de fora de qualquer transação econômica com o bloco europeu. Dessa forma, com LGPD, no atual

contexto econômico, garante que o Brasil possa fazer qualquer transação econômica com o bloco europeu. (PINHEIRO, 2018a).

Assim sendo, a LGPD nasceu na esteira da regulamentação europeia, tendo como objetivos, segundo Pinheiro (2018a, p. 19), “[...] trazer mecanismos de controle para equilibrar as relações em um cenário de negócios digitais sem fronteiras”.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE), fundada em 1961, em Paris, é uma organização que reúne 36 países entre as maiores economias do mundo. Essa organização abarca as maiores economias, entretanto nada impede que países emergentes também venham a fazer parte. É o caso do Chile e do México.

Podemos dizer que o principal objetivo da OCDE é promover a cooperação e a discussão de políticas públicas a fim de promover o desenvolvimento econômico de seus países-membros. O Brasil oficializou o pedido de entrada na OCDE em 2017, para melhorar sua visibilidade comercial no cenário internacional, valendo-se de benefícios que são exclusivos aos participantes da organização. No início do ano de 2020, após várias concessões brasileiras, o Brasil teve a entrada negada e perdeu espaço para a Argentina.

Por certo, a criação da LGPD é um fator determinante para a admissão do Brasil como membro da OCDE, haja vista que, em 23 de setembro de 1980, foram criadas as linhas diretrizes da OCDE para a proteção da privacidade e fluxo transfronteiras de dados pessoais. (RODOTÁ; 2008). Essas linhas diretrizes estão dispostas nos Art.s 1(c), 3(1) e 5(b) da Convenção da Organização para a Cooperação e Desenvolvimento Econômico. Entre outras disposições, essas diretrizes reconhecem o interesse comum na proteção da privacidade e das liberdades individuais e em conciliar valores fundamentais, porém conflitantes, como a privacidade e o livre fluxo de informação.

j) Lei do Cadastro Positivo:

De acordo com a Lei 12.414/2011, conhecida como a Lei do Cadastro Positivo, cuja principal característica, segundo Mendes (2014, p. 145),

> [...] reside no fato de ter ampliado a possibilidade do fluxo de dados no mercado, ao possibilitar a formação de bancos de dados com informações de adimplemento, ao mesmo tempo em eu buscou estabelecer regras de proteção à privacidade e métodos de controle e fiscalização dessa atividade.

A referida lei, na esteira das disposições do CDC (BRASIL, 1990), traz, em seu bojo, o princípio da qualidade dos dados pessoais (artigo 3º, § 1º). Além disso, descreve os direitos de acesso, retificação e cancelamento dos dados, descritos no Art. 5º, II e III. Adiante, já nos Art.s 2º, I; 5º, VII e 7º, prevê acerca da extensão da finalidade para a coleta dos dados, cujas hipóteses são bem limitadas. Segundo Mendes (2014, p. 145):

> Realização de análise de risco de crédito do cadastrado ou para subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente.

Quanto ao tocante do princípio do consentimento, importante destacar que a referida lei, em seus Art.s 4º, 5º e 9º, traz a prerrogativa sobre a análise de crédito. Acerca disso, segundo Mendes (2014, p. 146), "[...] estabelece mecanismos de controle do indivíduo sobre os seus dados, atribuindo a ele o poder de decidir se tem interesse ou não em formar esse histórico e de decidir quando deseja cancelá-lo".

A titularidade dos dados pessoais não pode ser objeto de transferência, uma vez que o destino de tais dados pessoais cabe somente ao titular. (MENDES; 2014).

Importante mencionar o fato de que a Lei 12.414/2011 (BRASIL, 2011) vedou explicitamente o princípio da proibição do armazenamento de informações sensíveis e excessivas, o que pode gerar a discriminação do cidadão na sociedade, violando, com isso, o princípio constitucional da igualdade.

Ainda segundo Brasil (2011), a Lei 12.414/2011 trouxe também um aspecto novo quando prevê a possibilidade de o titular pedir a revisão de decisão realizada exclusivamente por meios automatizados. É o conteúdo disposto no Art. 5º, inciso VI. Sobre esse artigo e inciso, leciona Mendes (2014, p. 147): "Trata-se de uma regra de justiça, que visa assegurar a possibilidade de defesa do titular e a sua participação em um processo de decisão tomado com base em seus dados [...]".

Essa possibilidade de rever decisão assume importância quando levado em conta o sistema de avaliação de risco, uma vez que ao consumidor é possível rever uma nota ou valor aplicado em dado errôneo, desatualizado ou captado através de informação com vedação de armazenagem. (MENDES, 2014).

É inegável o progresso desta lei (Lei 12.414/2011), sendo importante mencionar que prevê necessidade de controle da atividade de processamento de

dados por autoridade administrativa. De acordo com o Art. 17 da referida lei, foi criado um sistema administrativo de fiscalização e resolução de conflitos em conjunto com um sistema clássico judicial de solução de lides. (MENDES, 2014).

Da análise do conjunto de fatores expostos até aqui, podemos observar que a criação da LGPD, em nosso ordenamento jurídico, se deu após um sucedâneo de fatos e inovações de leis esparsas que já regulavam, em parte, a matéria dados pessoais. Salientamos que o avanço da sociedade, na era digital, exigiu do legislador um movimento maior, no sentido de proteger e resguardar os direitos fundamentais da liberdade e da privacidade, decorrentes do livre desenvolvimento da pessoa natural no Estado Democrático de Direito.

2.3 Privacidade, intimidade e vida privada

A lei CF/88 tratou de ampliar o uso de termos, objetivando acoplar todas as possibilidades de tutela ou violação. Porém, segundo Doneda (2006), as possibilidades de tutela ou violação somente fomentaram o fato de que a lei não possui uma definição-chave que consiga reunir todos os conceitos.

Segundo Doneda (2006), a falta de uma definição-chave para a lei é resultado direto do percurso histórico que se encaminhou até o tratamento atual. Para que se pudesse eleger uma definição, o processo enfrentava o dilema do ordenamento jurídico em conjunto com as particularidades que cada sociedade possui internamente para tratar do assunto. O autor Doneda aponta o fato de que essa indefinição, talvez, não deva ser vista como um obstáculo, mas como “[...] uma característica ontológica da própria construção da esfera privada”. (DONEDA, 2006, p. 89).

De acordo com Sarmento (2016), a Carta Magna de 1988 (Constituição Federal de 1988), em uma forma diferente e inovadora do disposto em textos antecessores, elencou, pela primeira vez, a igualdade como direito fundamental. Com isso, tratou de garantir o direito à liberdade, à vida, à igualdade, à propriedade e à segurança como direitos fundamentais, sendo descritos no Art. 5°, *caput*. Esse mesmo artigo também garante a proteção ao que alcunhou de intimidade, além da proteção vida privada, bem como da honra e imagem. Nesse contexto, tem por objetivo garantir a proteção da pessoa humana, visto que o direito à vida e à liberdade fundamentam o princípio constitucional da dignidade da pessoa humana, explicitamente mencionado no Art. 1º, inciso III da Carta Política de 1988. (SARMENTO, 2016).

> 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. (BRASIL, 1988).

Da análise das Constituições Brasileiras anteriores, podemos inferir a semelhança e inovação existentes entre o Art. 5° de Brasil (1988), do Art. 179 de Brasil (1824), do Art. 72° de Brasil (1891), e do Art. 113 de Brasil (1934). Também no Art. 122 de Brasil (1937); o Art. 141 de Brasil (1946) e o Art. 153 de Brasil (1967). Dentre as semelhanças, podemos citar que as constituições passadas elencavam as mesmas garantias e direitos fundamentais. A Constituição Federal de 1988 foi a Primeira Constituição a prever, de forma específica, o direito à privacidade, por meio do Art. 5º, inciso X. “Anteriormente, qualquer construção acerca da defesa da inviolabilidade da intimidade, vida privada, honra e imagem eram tuteladas mediante construções doutrinárias”. (FERNANDEZ JUNIOR, 2014).

Isso significa dizer que devem ter um olhar garantista, de proteção. Segundo o autor Doneda (2006, p. 121), não é o melhor caminho “[...] insistir em uma conceitualística que intensifique as conotações e diferenças semânticas dos dois termos”, ou seja, intimidade e vida privada.

Os termos da intimidade e da vida privada utilizados pela Constituição Federal de 1988 devem ser integrados, de forma que o ordenamento jurídico cumpra o seu papel de unir, integrar, consolidar por meio da atividade de interpretação. O autor Doneda (2006) conclui que os termos intimidade e vida privada não devem ser valorizados sob conceitos diferentes, ou seja, devem ser interpretados sempre de forma garantista, não justificando a sua ausência de distinção terminológica por parte da doutrina e jurisprudência.

> [...] à luz da Constituição Federal de 1988, é o conjunto do modo de ser e viver, como direito de o indivíduo viver sua própria vida ao que se refere aqui? Consiste ainda na faculdade que cada indivíduo tem de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano. (GUERRA, 2004, p. 49).

O ponto principal da discussão acerca da falta de definição doutrinária do uso das palavras intimidade e vida privada, de origem terminantemente doutrinária, é apenas o de trazer unificação a leitura legislativa, de modo que o direito fundamental tivesse sua aplicação garantida. (DONEDA, 2006).

Nas lições de Doneda (2006), uma grande inquietação em relação à tutela da privacidade é própria dos dias atuais. A ideia de privacidade em si não é de agora. Com os diversos sentidos que possui, pode ser vislumbrada em outros tempos e em diversas sociedades. No entanto, com novas nuances, a privacidade passou a chamar a atenção do ordenamento jurídico. E tão somente nos últimos anos do século XIX, a privacidade passou a ter suas características contemporâneas. Ainda, podemos citar o nobre professor em Doneda (2006, p. 127, grifo do autor):

> Esta moderna doutrina do direito à privacidade, cujo início podemos considerar como sendo o famoso artigo de Brandeis e Warren, *The right to privacy*, tem uma clara linha evolutiva. Em seus primórdios, marcada por um individualismo exacerbado e até egoísta, portava a feição do direito a ser deixado só.

A Noção inicial de privacidade, de acordo com Doneda (2006), deve estar atrelada à análise dos conceitos que a lei brasileira determina como relacionados a ela. Essas podem ser lembrados, de acordo com Doneda (2006), nos termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como privatividade e privacidade, por exemplo.

Em se tratando do conceituo de privacidade, nas lições de Rodotá (2008, p. 24), a privacidade pode ser definida como “[...] conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre os quais o interessado pretende manter um controle exclusivo”.

Nas palavras de Mendes (2014, p. 36, grifo do autor):

> [...]a privacidade, antes compreendida, como direito negativo de ser deixado em paz (*right to be let alone*), passa a significar também o controle dos dados pelo próprio indivíduo, que decide como e onde os seus dados pessoais devem circular.

A privacidade dos tempos atuais traz a ideia de poder sobre seus dados, que passam a ser de controle exclusivo do titular.

Nas lições de Canotilho *et al*. (2013), o direito à intimidade concede um poder ao indivíduo para controlar a circulação de informações pessoais. As informações que se encontram protegidas são aquelas de caráter “privado”, “particular” ou “pessoal”.

Já no que se refere a segredo e sigilo, nas lições de Nunes (2017), segredo e sigilo são usados como se fossem a mesma coisa, mas possuem algumas diferenças. Tanto um quanto o outro dão a ideia de não exposição de algo em público, no entanto o sigilo representa um dever legal para que algo se mantenha em segredo, como é o caso de inúmeras profissões que exigem o chamado sigilo profissional. Há também o sigilo das telecomunicações e o sigilo das correspondências:

Nas palavras de Ferraz Júnior (1993, grifos do autor):

> O sigilo, no inciso XI do artigo 5º, está referido à comunicação, no interesse da defesa da privacidade. Isto, no texto, em dois blocos: a constituição fala em sigilo ‘da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas’. Note-se, para a caracterização dos blocos, que a conjunção e une correspondência com telegrafia, segue-se uma virgula e, depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica. (apud NIGRI, 2006).

Ou seja, o objeto protegido não são propriamente os dados, mas as informações que são compartilhadas de forma privativa e que, de alguma forma, são violadas por uma pessoa estranha à relação.

O recato vem a ser, de acordo com Bueno (2020), sinônimo de resguardo, prudência, honestidade no qual, deve preservar a privacidade.

De acordo com a lição de Canotilho *et al*. (2013, p. 300), é “A reserva legal do Art. 5º pode ser classificada num primeiro momento como qualificada se entendermos que ela já fixa o propósito que deverá ser perseguido pela lei concretizadora”. Isso quer dizer que o objetivo seria garantir que determinados profissionais tenham aptidão mínima para desenvolver suas atividades, principalmente o profissional liberal.

Em se tratando da Intimidade da Vida Privada, consoante ensina Mendes (2014, p. 169), ela abrange os dados pessoais de forma indireta:

> [...] embora os dados pessoais em si não se enquadrem no inciso XII do artigo 5º da Constituição, eles se inserem no âmbito de proteção do direito à inviolabilidade da intimidade e da vida privada, garantido pelo inciso X do artigo 5º da Constituição, interpretado de forma sistemática com o princípio da dignidade humana e à luz da garantia do habeas data.

Do que ensina Mendes, conclui-se que a proteção dos dados pessoais está abrangida no princípio da dignidade da pessoa humana de forma implícita. Assim sendo, o Art. 5º, inciso X da Constituição Federal de 1988, pode ser compreendido como a outorga de um sistema de proteção de direitos fundamentais de personalidade.

Nesse novo espectro, é preciso que haja uma redefinição dos conceitos de intimidade e vida privada, uma vez que, com a evolução da tecnologia, é imperioso que se busque um novo sentido e alcance ao direito de privacidade. Assim sendo, o direito à privacidade, que era tido a partir de um caráter fortemente individualista em seus primórdios, com a conceituação do direito de ser deixado só (*right to be let alone*), Warren e Brandeis foram os precursores na definição do direito à privacidade. No decorrer do século XX, a transformação da sociedade, junto à revolução da tecnologia, trouxe à baila a necessidade de uma nova conotação que contribuísse para a modificação de um direito extremamente egoísta no sentido de passar a ser considerado uma garantia de controle de informações pessoais democrático. Dessa forma, pode-se dizer que o século XIX presenciou um processo de reinvenção da privacidade. (DONEDA, 2006).

O termo que se utilizará daqui para frente unifica todos os valores que os demais usados pelas constituições anteriores a de 1988 tentaram expressar. Da mesma forma, opta-se pela sua aplicação, visto que se distingue de forma necessária dos demais termos que envolvem a imagem, a honra e a identidade pessoal. (CALDAS, 1997).

Identificando privacidade como o termo ideal, que melhor expressa a intimidade e a vida privada diante da revolução tecnológica atual, é preciso considerar as definições dos pioneiros no assunto, Warren e Brandeis, que conectam a sua proteção à inviolabilidade da personalidade, colocando fim ao costume anterior, que relacionava a proteção da vida privada à propriedade. (MENDES, 2014).

Foi apenas a partir do século XX, quando começaram a surgir os primeiros meios de comunicação em massa, que o conceito de privacidade sofreu uma intensa reformulação, principalmente diante dos novos eixos de gravitação do ordenamento jurídico. Esse período ficou marcado por grandes mudanças nos conceitos que se tinha a respeito de privacidade, bem como nos meios de se protegê-la. (DIAS; REIS, 2011).

Autores renomados, como Stefano Rodotá (2008), Ferraz Júnior (1993 apud NIGRI, 2006) e Daniel Sarmento (2016), debruçaram-se ao estudo da origem do direito à privacidade. Um ponto em comum nos estudos de todos é a definição que Warren e Brandeis (1890) deram a esse direito como sendo “o direito de ser deixado só” (*Right to be alone*).

> Mesmo o artigo de Warren e Brandeis, publicado em 1890 na revista *Harvard Law Review*, sobre o *right to privacy,* parte de um conceito mais ampliado de privacidade, desvinculando sua proteção do direito de propriedade. Nesse sentido, a sua defesa se daria em torno da proteção da pessoa humana em si, vindo a ocupar futuramente na jurisprudência americana o lugar de um verdadeiro direito geral de personalidade. O contexto do supracitado artigo se deu a partir do surgimento de um novo fato social que correspondia às mudanças trazidas pelas tecnologias de informação da época, como jornais e fotografias, bem como ao fenômeno da comunicação em massa. Nesse sentido, o artigo possibilitou que o direito à privacidade nos Estados Unidos fosse tido como uma garantia Constitucional. (COSTA, 2018, p. 37-38, grifo do autor).

Diante disso, é possível identificar que a partir do artigo de Warren e Brandeis – The right to privacy (1890) que surgiu a necessidade de definição de um conteúdo que fosse comum para o direito à privacidade, bem como fosse fruto dessa enxurrada de informações, isso auxiliaria na ampliação da necessidade de se fortificar as variadas formas de proteção. Esse momento histórico (século XX), segundo Robert Ellis Smith (1979), pode ser exemplificado a partir da análise do direito começando em 1970, quando essa noção se mesclou com a noção ampla de privacidade em conjunto com o problema do armazenamento de dados. Acerca disso, leia-se:

> [...] hoje, quando se fala sobre privacidade, geralmente refere-se não apenas ao direito de manter o caráter confidencial de fatos pessoais, porém ao direito de saber quais informações sobre si próprio são armazenadas e utilizadas por outros, e também o direito de manter estas informações atualizadas e verdadeiras. (SMITH, 1979, p. 20, tradução nossa).

Segundo o artigo de Beales III e Muris, publicado na obra The Aspen Institute Congressional Program (2019), a privacidade e o consumo sendo monitorados por robôs ou *cookies*[2] na *Internet* podem ser vistos como uma problemática a ser mais

[2] Um *cookie* é um pequeno arquivo robô usados por servidores de *Internet* para diferenciar seus usuários e para capturar os dados relacionados à navegação de cada usuário em um site. Serve tanto

aprofundada. Se, de um lado, há a proteção dos dados do consumidor, por outro, há o armazenamento de informações pessoais (*cookies*) que são disponibilizados aos fornecedores de produtos e/ou serviços, que acabam rastreando os usuários da rede (obtenção de dados por onde o consumidor navega na *Internet* através dos robôs). Essa navegação faz com que as informações sejam úteis para ofertas de produtos e serviços personalizados na experiência de navegação do cliente.

As informações deixam de ser completamente apenas do consumidor e passam a ser de quem as coletou também. Complementam os autores J. Howard Beales III e Timothy J. Muris, quando dizem que as informações poderiam ser úteis para ambas as partes em uma transação comercial, apesar de dificilmente se saber quando iriam ser necessárias. Os autores concluem afirmando que não há base científica que afirme a propriedade exclusiva de dados pessoais para nenhuma das partes, pois dados pessoais possuem significados diferentes dependendo do momento. Ainda assim, os autores terminam exemplificando que o controle de fraudes é construído sobre uma base prévia de dados, tais como as armazenadas pelos robôs que armazenam os *cookies*. (BULES III; MURIS, 2019).

2.4 Evolução da proteção de dados no Brasil

A regulamentação sobre proteção de dados pessoais até então existente era feita de forma esparsa e era deficiente em relação à uniformidade e à assecuridade da segurança jurídica. É importante observar que, até o presente momento, a Constituição Federal de 88 era a pedra angular na qual se pautavam todas as resoluções de divergências e questionamentos que porventura viessem a aparecer. (COELHO, 2018).

Desde 1988, muitos problemas surgiram, como a coleta de dados pessoais de forma indiscriminada, e com a inexistência do consentimento do titular dos dados, sendo a hiperconectividade apenas um deles. Não se esperava do constituinte originário que ele pudesse prever, principalmente no final da década de 1980, os riscos que seriam gerados relacionados à proteção de dados como nos anos finais do século XX e início do século XXI se tem. (LEMOS; ADAMI; SUNDFELD, 2018).

---

para armazenar os dados de um usuário no momento de efetuar compras on-line, como para dar permissão de acesso a um determinado usuário do site (SAFERNET, 2020).

O Art. 5º, inciso X da Constituição Federal de 1988, no entanto, conseguiu prever a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, além de assegurar o direito de "[...] indenização pelo dano material ou moral decorrente de sua violação". (BRASIL,1988).

No âmbito infraconstitucional, leis esparsas antes da LGPD, revelavam a preocupação do legislador com o tratamento de dados pessoais, como, por exemplo, no Código de Defesa do Consumidor, Lei 8078/90 (BRASIL, 1990) , Art.s 43, 72 e 73, no Marco Civil da *Internet* (BRASIL, 2014), Art.s 3º, III; 7º, VII, VII, IX, X; 10; 11; 16, II, (BRASIL, 2016), (Capítulo III), na Lei do Cadastro Positivo (BRASIL, 2011), Lei 12.414/11, Art. 5º, V, VI e VII, (BRASIL, 2013), Art. 4º, VII), Lei de Acesso a Informações (BRASIL, 2011), Lei 12527 de 18 de novembro de 2011 Seção V), dentre outras.

Brasil (2018) surgiu em resposta a tendência mundial de trazer maior transparência nos processos de uso de dados pessoais dos cidadãos. "[...] na Europa, a partir da evolução constante do conceito de privacidade, já na década de 1980 havia instrumento juridicamente vinculante, versando sobre referida matéria". (MALDONADO; BLUM, 2018, p. 88)[3]. Dessa maneira, com o advento de Brasil (2018), o nosso país passou a fazer parte dos países que possuem legislação específica a respeito da privacidade e proteção de dados.

Para Mota (2019), a evolução da proteção de dados emana da própria privacidade, que é reflexo dos avanços da tecnologia e que, portanto, deve acontecer também na esfera jurídica.

> A proteção de dados pessoais tem uma gênese na privacidade. A privacidade foi o primeiro elemento com o qual a humanidade se deparou como sendo um valor social que precisava de uma proteção jurídica e, assim, foi criado o direito à privacidade. Isso foi só o início. Temos, agora, uma construção baseada no desenvolvimento científico-tecnológico. Com esse desenvolvimento, os entes públicos e privados começaram a ter mais condições de processar dados. E aí surgiu a necessidade de criar obrigações relacionadas ao processamento dos dados. E essas obrigações foram traduzidas no que se conformou como sendo o direito à proteção de dados. A conclusão foi que não basta respeitar a privacidade, é preciso também observar a forma como os dados são processados. E isso para preservar tanto a privacidade como qualquer outra liberdade civil que o cidadão detenha. Ou seja, a necessidade de constitucionalizar a

[3] Trata-se, como apontado pela Professora Viviane Nóbrega Maldonado, da Convenção para a Proteção das Pessoas Singulares no que diz respeito ao tratamento automatizado de dados pessoais (Convenção 108, de 28 de janeiro de 1981) (MALDONADO; BLUM, 20118).

> proteção de dados pessoais surge desta visão de que privacidade é um elemento, e a proteção de dados é outro, sendo uma evolução demandada pela própria humanidade. E no meio dessa evolução, que partiu dos aspectos tecnológico e econômico, também tinha que acontecer uma evolução jurídica. (MOTA, 2019).

O ensinamento que se extrai é de que a Constituição Federal, Brasil (1988) abrange também a proteção de dados como um direito fundamental, independente da privacidade, devido a nova forma de sociedade, muito mais tecnológica e com uma economia que lida com dados pessoais de uma pessoa viva, identificada ou identificável, o tempo todo, dados pessoais que necessitam de uma legislação específica.

De acordo com o Art., 1º, III e 5º, X da Constituição Federal:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos; III - a dignidade da pessoa humana. 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. (BRASIL, 1988).

Brasil (1988) já trazia, em seu Art. 5º, inciso X, a intimidade, a vida privada, a honra e a imagem da pessoa natural como direito fundamental inviolável.

De acordo com o Art., 43 do Código de defesa do Consumidor

> Art. 43. O consumidor, sem prejuízo do disposto no Art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. [...]. (BRASIL, 1990).

O Código de Defesa do Consumidor (BRASIL, 1990) define quais são os direitos básicos dos quais o consumidor goza. Dentro das práticas comerciais, muitas são utilizadas com o intuito de captar dados, e dentro de um contexto, caso fossem analisadas, já estariam enquadradas dentro das práticas abusivas que o CDC (BRASIL, 1990) elenca.

Segundo Maldonado *et al*. (2018), caso o consumidor viesse a ter seus dados eventualmente coletados pelo fornecedor sem se atentar para esse fato ou anuir essa

conduta, já estaria enquadrado em uma situação de vulnerabilidade técnica. Ou seja, ensejaria manifestação de vontade viciada, uma vez que o consumidor não foi, de forma correta, informado acerca das características essenciais desse serviço ou produto.

A prática de não informar o consumidor violaria um dos princípios basilares do CDC (BRASIL, 1990), qual seja, o princípio da boa-fé, além de violar os direitos básicos do consumidor A informação adequada e clara sobre a contratação de serviços, ou quando o consumidor adquire algum produto, mesmo que esses dados sejam usualmente fornecidos pelo consumidor, o fato, por si só, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz, não está implícita e automaticamente autorizando o comerciante a divulgá-los no mercado. Conforme entende o STJ no Recurso Especial nº 1.758.799:

> [...] O propósito recursal é dizer sobre: [...] (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente. 3. Segunda Seção decidiu que, no sistema credit scoring, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. 5.[...] de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar [...]9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. [...]. (BRASIL, 2019).

Nota-se a relevância da vontade e do consentimento de forma inequívoca e a boa-fé dos atores principais no controle do uso indevido de dados pessoais,

juntamente com a finalidade específica para o negócio entabulado, pois o STJ vem se posicionando sobre a inobservância dos deveres associados ao tratamento dos dados do consumidor.

Independentemente de os dados serem fornecidos pelos próprios titulares, no momento de entabular um negócio jurídico, como, por exemplo, uma compra, não se afasta, por si só, a responsabilidade dos agentes de tratamento de dados de manter o titular informado sobre seus dados pessoais confiados para o negócio que foi pactuado e não para terceiros ou estranhos. Tem-se a relação de confiança do consumidor ao fornecedor e a proteção de seus dados pessoais.

O Art. 21 do Código Civil reza sobre a inviolabilidade da vida privada:

> Art. 21. 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. (Vide ADI 4815). (BRASIL, 2002).

O Código Civil Brasileiro (BRASIL, 2002) já resguardava a vida privada da pessoa natural como direito inviolável, todavia nada previa nos casos de violação pela *Internet*. Nas lições de Sarmento (2016, p. 145, grifo do autor):

> [...] No Brasil, a proteção da autonomia privada como dimensão da dignidade humana vem sendo salientada em diversas decisões do STF. No julgamento que resultou do reconhecimento do direito à constituição de união estável homoafetiva, o relator, Ministro Carlos Ayres Britto, salientou ‘a proteção constitucional que faz da livre disposição da sexualidade do indivíduo um autonomizado instituto jurídico(...), dado elementar da criatura humana em sua intrínseca dignidade. [...].

Depreende-se, do texto de Sarmento (2016), a relevância da autonomia privada como verdadeira extensão da dignidade da pessoa humana. Essa extensão da dignidade do indivíduo dá o direito de decidir até mesmo sobre sua identidade como pessoa humana. Frequentemente, os juízes deparam-se com situações inusitadas e complexas que advêm de uma nova sociedade, denominada sociedade digital ou sociedade da informação, que evoluiu rapidamente, trazendo a necessidade de inovação também na esfera jurisdicional.

Nas palavras de Hoch (2019, p. 16):

> [...] As relações interpessoais são estabelecidas mediante um simples clique no mouse, a vida privada das pessoas torna-se vulnerável a invasões e o Poder Judiciário é desafiado a solucionar demandas relacionadas à utilização das novas tecnologias e à violação de direitos fundamentais, como a intimidade.

Assim, revela-se uma verdadeira evolução no que diz respeito à dignidade, à intimidade, à vida privada e à privacidade, verdadeiros precursores do direito à proteção de dados.

O Marco Civil da Internet (BRASIL, 2014) em muito se assemelha à lei do consumidor (BRASIL, 1990), uma vez que ambas buscam consolidar suas preocupações relacionadas com a tutela da segurança e da privacidade dos dados pessoais.

Nas lições de Magrani (2009, p. 118, grifo do autor):

> O Marco Civil da *Internet* (Lei nº 12.965/2014 — MCI)175, aprovado em 2014, estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil. Antes da sua sanção, restava claro que a ausência de disposições sobre direitos fundamentais básicos como a liberdade de expressão, o acesso ao conhecimento e o direito à privacidade dificultavam a aplicação da legislação em vigor e geravam inúmeras decisões judiciais conflitantes para as mais diversas controvérsias envolvendo o uso da *Internet*.

Dessa preocupação, dentro do MCI (Marco Civil da *Internet*) (BRASIL, 2014), surgiram: a previsão de institutos com regras de consumo; a inviolabilidade da intimidade da vida privada, bem como o sigilo no fluxo de comunicações pela *Internet;* a guarda e a disponibilização dos registros de acesso. Também as aplicações de *Internet* vêm nessa esteira, devendo atender à preservação da intimidade, honra e imagem das partes envolvidas.

Nesse sentido, o Art. 7°, inciso X do MCI (BRASIL, 2014), já previa o direito do usuário à "[...] exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de *Internet*, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei".

Contudo, o avanço da tutela de privacidade tem sido feito de forma bastante gradual, principalmente naquilo que diz respeito aos dados pessoais. É uma evolução lenta, principalmente diante dos desafios dos novos tempos, que se mostram avassaladores. De acordo com Castells (2018, p. 88).

> [...] A informação e conhecimentos sempre foram elementos cruciais no crescimento da economia, e a evolução da tecnologia determinou em grande parte a capacidade produtiva da sociedade e os padrões de vida, bem como as formas sociais de organização econômica.

Segundo Castells (1999), a revolução tecnológica deu origem ao informacionalismo, a base para uma nova sociedade – sociedade em rede, na qual a tecnologia da informação é considerada uma ferramenta indispensável na manipulação da informação e construção do conhecimento pelos indivíduos. “[...] a geração, o processamento e a transmissão de informação tornam-se a principal fonte de produtividade e de poder”. (CASTELLS, 1999, p. 21).

Nas lições de Boff *et al*. (2018, p. 109, grifo nosso):

> Se, por um lado, o Marco Civil da *Internet* representa um avanço na construção normativa relacionada às demandas da sociedade da informação, recepcionando terminologias adequadas ao contexto da *Internet*, por outro lado, trouxe a necessidade de regulamentação de dispositivos específicos, como é o caso da seção que trata da proteção da privacidade e dos dados pessoais na rede.

O Marco Civil da *Internet* (BRASIL, 2014), em um primeiro momento, mostrou-se um microssistema de proteção de dados pessoais, que desabrochou em uma necessidade de se tutelar questões específicas. Mesmo assim, existem questões sensíveis, relacionadas à proteção na *Internet,* que não são abordadas de forma mais latente nele. Isso porque, apesar do grande avanço inicial, ainda há espaço e diálogo para debater o assunto.

De acordo com Magrani (2019, p. 74, grifo do autor):

> O Marco Civil da Internet se pretendeu como a ‘Constituição da *Internet*’ no Brasil e salvaguardou diversos princípios e direitos fundamentais. A proteção da privacidade, dos dados pessoais e da liberdade de expressão são expressamente previstas no Marco Civil da Internet representando um grande avanço face ao cenário anterior ao diploma, que levava a uma quantidade maior de abusos e violações de direitos.

Não obstante, todas as previsões do Marco Civil da *Internet* (BRASIL, 2014) e do Código de Defesa do Consumidor (BRASIL, 1990) que visam tutelar a privacidade e a segurança dos usuários da *Internet*, os dispositivos existentes não são capazes

de elidir as lacunas que permeiam a privacidade de dados, trazendo a necessidade de criação de uma lei que complementasse as já existentes.

> Em 2014, o Marco Civil da *Internet* entrou em vigor no Brasil, estabelecendo princípios, garantias, direitos e deveres para o uso da *Internet* no país. Foi uma forma de reconhecer e regulamentar as novas relações jurídico-virtuais, em razão da existência de inúmeros usuários e provedores, bem como de empresas que trabalham online, dado que grande parte não estava adaptada à nova realidade digital. O MCI trata dos delitos praticados online (crimes cibernéticos) e da neutralidade da rede, estabelecendo direitos e garantias para liberdade de expressão, e, apesar de cuidar da privacidade, acabou restando uma lacuna sobre o tratamento de dados pessoais, pois não foi dada a devida atenção ao seu uso, destino, comercialização, etc. (SOUZA, 2018, p. 15).

A tutela da segurança e da privacidade do usuário, na forma do Código de Defesa do Consumidor (CDC) (BRASIL, 1990) e do Marco Civil da *Internet* (BRASIL, 2014), será complementada pela entrada em vigor da Lei Geral de Proteção de Dados, que é composta por 65 artigos no total, dividida em 10 capítulos.

A LGPD foi sancionada no dia 14 de agosto de 2018, no Congresso Nacional. O PLC 53/2018, o qual dispunha sobre a proteção de dados pessoais e previa alterações a lei n° 12. 965 de 2016 (Marco Civil da *Internet*), consolida-se assim como a Lei de Proteção de Dados Brasileira (BRASIL, 2016).

A LGPD, Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018), é uma lei que elenca princípios, direitos e obrigações sobre o uso de dados pessoais, um dos “ativos mais valiosos” da chamada “sociedade digital”. (PINHEIRO, 2018a).

Essa proteção deve ser realizada a fim de garantir que todas as informações coletadas sejam autorizadas pelo usuário, ou seja, esse usuário deve ter ciência de quais informações foram coletadas e para qual finalidade será utilizada.

De acordo com o Art. 1º da LGPD:

> Ela 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 de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018).

Desse modo, Maldonado e Blum (2018, p. 19) explicam:

> A Lei Geral de Proteção de Dados Brasileira (LGPD) se preocupa e versa apenas e tão somente sobre o tratamento de dados pessoais. Ou seja, não atinge os dados da pessoa jurídica, documentos sigilosos, ou confidenciais, segredos de negócio, planos estratégicos, algoritmos, fórmulas, softwares, patentes, entre outros documentos ou informações que não sejam relacionados a pessoa natural identificada ou identificável.

A elaboração e a promulgação de uma lei (LGPD), que especifica a proteção de dados pessoais, passa a ser necessária, cada vez mais, com a evolução da tecnologia, além de equiparar o Brasil ao resto do mundo no combate ao uso irrestrito de dados pessoais no ciberespaço. Essa lei ainda vem a viabilizar um melhor diálogo e a interação entre o Direito e as novas tecnologias, sobretudo as tecnologias que envolvem o ciberespaço e a mídia digital.

O cuidado com o tratamento dos dados é um dos destaques da nova lei brasileira (LGPD), dada a responsabilidade sobre o armazenamento e uso dos dados pessoais por quem quer que seja. Essa lei traz consequências, tais como: multas, sanções, retratação pública e respeito às boas práticas em governanças coorporativas. As consequências podem gerar uma conduta reputacional fundada no respeito à privacidade, respeito à inviolabilidade da expressão, de informação, de comunicação, de opinião, da intimidade, da honra e da imagem da pessoa. Ainda assim, tem-se o favorecimento do livre desenvolvimento da personalidade, da dignidade e do exercício da cidadania das pessoas naturais.

A Lei Geral de Proteção de Dados (BRASIL, 2018) expõe, de forma taxativa, 10 bases legais para o tratamento de dados pessoais (Art. 7º do inciso I ao X). E ainda, no Art. 6.º, têm-se os princípios, que embora não abranjam, de forma direta, o escopo do presente estudo, devem ser analisados para maior compreensão do tratamento de dados. Entre eles, são descritos: a) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular; b) Necessidade: limitação do tratamento de dados ao mínimo necessário; c) Livre acesso: consulta facilitada e gratuita aos titulares sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados; d) Qualidade dos Dados: exatidão, clareza, relevância e atualização dos dados; e) Transparência: informações claras, precisas e facilmente acessíveis sobre o tratamento de dados, observados os segredos comerciais e industrial; f) Segurança: utilização de medidas técnicas e administrativas para evitar acesso não autorizados e situações acidentais ou ilícitas de perda, alteração, etc.

Ainda assim, tem-se: g) Prevenção: adoção de medidas para prevenir a ocorrência de danos aos titulares; h) Não Discriminação: não utilização de dados pessoais para fins discriminatórios ilícitos ou abusivos; i) Responsabilização e prestação de contas: demonstração das medidas adotadas para cumprimento das diretrizes da Lei Geral de Proteção de Dados (BRASIL, 2018), inclusive a eficácia destas medidas descritas na própria LGPD.

Também traz diversos aspectos do Regulamento Geral de Proteção de Dados Pessoais da União Europeia (UE, 2016), no qual a LGPD se inspirou, como, por exemplo, a previsão e a aplicação de sanções gradativas e multas administrativas, que, no caso da GDPR, podem chegar a 20 milhões de euros ou a 4% do faturamento anual da empresa. No caso da LGPD, podem chegar a 2% do faturamento da organização privada, limitados a um total de 50 milhões por infração, No entanto, é a LGPD (BRASIL, 2018) única em diversos aspectos, como, por exemplo: possuir lacunas e ser muito menos específica em relação a determinados fatores como os parâmetros que devem ser analisados para indicar quando uma pessoa é potencialmente identificável. De fato, questões relevantes acabaram sendo deixadas de fora na legislação nacional.

Os direitos do titular, inseridos no capítulo III da LGPD (BRASIL, 2018) no *caput* do Art. 17 , aduzem que “Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade”. (BRASIL, 2018). Portanto, como bem leciona Pinheiro (2018b), em sua obra *Proteção de Dados Pessoais - Comentários à Lei nº 13.709/2018*, um dos escopos da LGPD (BRASIL, 2018), uma vez que os dados pessoais fazem parte da privacidade do indivíduo – com maior relevância por se tratar de ambiente digital, é garantir o livre desenvolvimento da personalidade da pessoa natural e a proteção. Além disso, demonstra uma relação dessa garantia da pessoa natural à titularidade de seus dados à inviolabilidade de sua vida privada em consonância ao disposto no Art. 5º inciso X da Constituição Federal de 1988 (BRASIL, 1988) e do artigo 21 do Código Civil (BRASIL, 2002).

O sentimento de que, finalmente, o Brasil passa a ser amparado por uma lei que abrange também as relações dentro e fora da *Internet* traz a falsa ideia de que tal norma garantirá a segurança jurídica de que o cidadão necessita, todavia o direito deve responsabiliza-se de tal forma que a LGPD (BRASIL, 2018), além de criada, também seja eficaz.

3 OS IMPACTOS NAS OPERAÇÕES DE NEGÓCIOS COM A PRORROGAÇÃO DO PRAZO DE VIGÊNCIA DA LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

Neste terceiro capítulo, abordam-se os impactos nas operações de negócios com as inúmeras prorrogações para a entrada em vigor da Lei 13.709/2018 (LGPD). Além disso, explana-se sobre o panorama da proteção de dados na LGPD e a GDPR como modelo para a legislação brasileira. Por fim, o capítulo disserta sobre o tratamento de dados pessoais e seus desafios.

Antes mesmo de sua entrada em vigor, a lei de proteção de dados já vem sofrendo modificações substanciais.

O aumento do índice de vazamento de dados na era digital vem impactando drasticamente as operações de negócio das empresas e exigindo um conjunto extra de atividades, que incluem medidas previamente definidas e planejadas que esses eventos podem acarretar.

Posteriormente, dada a complexidade da LGPD e do curto período que contariam as empresas e organizações para se adaptarem, aliada ao fato das inúmeras prorrogações de sua entrada em vigor, levarão a economia brasileira caminhar a passos lentos. Sobre essa temática, na opinião de Pinheiro (2019), o Brasil acaba perdendo oportunidades comerciais com a União Europeia, caso as empresas não aproveitem os adiamentos para se adequarem a LGPD. Acrescenta que todo adiamento que envolve a transparência não é uma boa escolha, por isso reforça a importância da criação da Autoridade Nacional de Dados, bem como a aplicação inicial de advertências e multas como boas alternativas para as primeiras medidas punitivas, ao invés da aplicação imediata das multas previstas em Lei. No entendimento de Bioni (2028), a prorrogação da LGPD é ruim não só para o cidadão, mas também para o próprio governo, que precisa de uma agenda econômica positiva. A LGPD tem um efeito colateral positivo, que é destravar um mercado econômico, algo essencial para a retomada do País.

Na visão de Doneda (2011), o adiamento da LGPD é inexplicável e arbitrário. “É algo que mostra o amadorismo como a proteção de dados vem sendo tratada pelo Executivo Federal”.

Assim, foi necessário tal prazo ser estendido conforme Figura a seguir:

Figura 1 – Vigência da Lei Geral de Proteção de Dados

Fonte: Ilarraz (2018).

A primeira prorrogação se deu por meio da Medida Provisória 869/18. A referida MP veio a suprimir partes do projeto de lei de proteção de dados pessoais, assim como modificou partes do texto original, como o período de *vacatio legis* para a nova lei entrar em ação, que passou de 18 meses (14 fev. 2020) para 24 meses (14 ago. 2020). A MP 869 trouxe ainda novidades à LGPD (BRASIL, 2018), com a criação da ANPD, o que já existia previsão no projeto de lei original e acabou ficando de fora, sendo vetada da nova lei, sob a alegação de vício de iniciativa legislativa, pois que é iniciativa privativa do Presidente da República a criação de órgãos da administração pública. Posteriormente, o próprio Presidente que vetou a criação do referido órgão veio a prever sua criação por meio de medida provisória que foi convertida na Lei 13.853, de 8 de julho de 2019, que altera a LGPD (BRASIL, 2018)

Por derradeiro, a MP 959/2020 (BRASIL, 2020), emitida em abril de 2020, sugeriu, mais uma vez, o adiamento da vigência da lei para maio de 2021, por entender que parte da sociedade não teve condições de se adaptar à LGPD por causa da pandemia do coronavírus. No entanto, essa MP foi aprovada no dia 26 de agosto de 2020, na Câmara dos Deputados. Também foi votada no Senado, mas sem o Art. 4º, que adiava a vigência da LGPD para 31 de dezembro de 2020 (BRASIL, 2020),

pois os Senadores derrubaram, por unanimidade, o artigo, por entenderem que a matéria já havia sido votada meses atrás. Portanto, uma vez sancionada a lei de conversão da MP, entrará em vigor a LGPD (BRASIL, 2018) de forma imediata, a partir da sanção presidencial. No que diz respeito às sanções que serão aplicadas pela Autoridade Nacional de Proteção de Dados, essas terão aplicação somente em 2021, decidido por decreto presidencial no dia 27/08/2020. (BRASIL, 2020).

Assim, haverá impactos nas operações de negócios com a prorrogação do prazo de vigência da lei geral de proteção de dados pessoais. Embora sua última prorrogação tenha sido antecipada, as punições ainda serão prorrogadas, o que continuará impactando as operações negociais e colaborando para a instauração da crise financeira no Brasil. Isso porque a falta de um órgão fiscalizador, que somente passará a aplicar sanções em 2021, deixará o Brasil descredibilizado frente aos grandes *players* mundiais.

3.1 O panorama na proteção dos dados pessoais na LGPD e a GPDR como modelo para a legislação brasileira

Uma das principais características que a referida Lei Geral de Proteção de Dados possui é a de se embasar nos ditames do Regulamento Geral de Proteção de Dados da União Europeia – RGPD (EURO-LEX, 2020), que revogou a Diretiva de Proteção de Dados.

De acordo com Lima e Carvalho (2019, p. 58):

> [...] Foi em maio de 2018 que se tornou aplicável na UE a mais recente ferramenta legislativa em matéria de proteção de dados pessoais: o GDPR. Este novo diploma procura garantir um elevado e uniforme nível de proteção das pessoas singulares neste campo através de vários direitos subjetivos, como o direito ao apagamento dos dados, postulado no artigo 17, n.1, GDPR. [...].

Nas palavras de Maldonado e Blum (2018, p. 30):

> O GDPR se aplica às empresas sediadas na união Europeia mesmo que não armazenem os dados no território da União, pois, no mínimo, haverá a consequência natural do tratamento de dados de indivíduos situados na União. (como os colaboradores que atuam nos estabelecimentos comerciais de países europeus).

Segundo Engelmann (2019, p. 101):

> A União Europeia, de certa maneira vanguardista, estabeleceu, em maio de 2018, a chamada General Data Protection Regulation (GDPR), visando à proteção dos dados pessoais dos cidadãos europeus. Sem dúvidas, essa legislação gerou fortes influências legislativas no mundo todo, afinal, estabeleceu que as empresas europeias ficariam impedidas de negociar com empresas de países que ainda não possuíam legislações de proteção de dados semelhantes à GDPR.

A Lei Geral de Proteção de Dados Pessoais (LGPD) nasce para unificar os mais de quarenta diferentes estatutos que atualmente governam os dados pessoais, on-line e off-line, substituindo certas regulações e suplementando outras.

O Regulamento Geral de Proteção de Dados foi promulgado no ano de 2016, no intuito de reduzir os riscos que ocorriam decorrentes da coleta, tratamento e transferências de dados dentro da União Europeia (UE). A Lei sofreu uma *vacatio legis* de dois anos antes de entrar em vigor em maio de 2018. A partir da sua confecção, começou a ser estabelecido um novo regime regulatório para todos os membros da UE, de modo que esse novo diploma legal substituiu a antiga Diretiva 95/46 de 1995[4].

A influência da GDPR dentro do processo de confecção da LGPD se dá, principalmente, em decorrência de uma característica da Lei Europeia: a influência da GDPR extrapola os limites territoriais, de modo que afeta organizações e empresas que se encontram fora do perímetro da União Europeia. Trata-se de empresas que realizam negócio dentro desse território ou daquelas companhias que oferecem serviços que coletem dados pessoais que, de alguma forma, estejam relacionados com a UE. (MAGRANI, 2018).

Como bem pontua Monteiro (2018a, p. 44):

> A União Europeia e as instituições do velho continente há décadas lideram as discussões sobre leis de proteção de dados. Em 1995, foi aprovada a Diretiva Europeia de Proteção de Dados. Concebida em uma era anterior ao surgimento da *Internet* comercial e muito antes da difusão dos modelos de negócio e tecnologias que se valem do uso

[4] Essa diretiva, 95/46 não está mais em vigor desde o dia 24 maio 2018, nem no Parlamento Europeu nem no Conselho. Essa diretriz, em vigor desde 24 de Out 1995, estava relacionada com a proteção das pessoas em relação aos tratamentos de dados pessoais e á livre circulação de dados, consoante o seguinte verbete: “Directive No. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data”. Disponível em: https://wipolex.wipo.int/en/text/313007. Acesso em 07 jun de 2020.

> intenso de dados pessoais e que são quase que onipresentes na vida das pessoas, precisou passar por um processo de atualização que culminou com a atual Regulação Geral de Proteção de Dados da União Europeia. (GDPR, da sigla em inglês, grifo nosso).

Um dos pontos principais acerca do GDPR é quanto ao consentimento do usuário, sendo necessário que seja claro, explícito e anterior à coleta e uso dos dados pessoais, podendo ainda ser revogado a qualquer tempo.

Nas palavras de Engelmann (2019, 102, grifo do autor):

> Em decorrência de um verdadeiro ‘efeito dominó’ ocasionado pela GDPR europeia, foi promulgada no Brasil a Lei nº 13.709, em 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), visando à normatização do tratamento.

Nas lições de Maldonado e Blum (2018), ao se ler o que dispõe o Art. 1º do GDPR, pode-se observar que a legislação se aplica à proteção de dados de pessoas singulares, havendo atenção também ao livre movimento desses dados.

Conforme os advogados portugueses Henriques e Luís, no artigo intitulado “Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral”, publicado no Anuário de Proteção de Dados (2019), a alteração ou aperfeiçoamento de procedimentos e formas de atuação já enraizadas na prática comercial diária daquele país, relativamente às atividades de tratamento de dados pessoais, bem como o exigente entorno legal que foi associado ao descumprimento desas regras, é tipo de assunto que tem provocado debate na doutrina e jurisprudência nacionais portuguesa. Nelas, existe a questão do consentimento dos trabalhadores como fundamento de licitude para o tratamento de dados pessoais dos trabalhadores por parte das entidades empregadoras. Afirma-se que a licitude de tal prática se dará sob o consentimento do empregado, consagrando o fundamento legal da própria GDPR sobre tal possibilidade, ou, de outro modo, será considerado tratamento de dados pessoais ilegal. Concluem afirmando que a licitude do tratamento de dados de empregados passa por uma verificação prévia e concreta de proporcionalidade das operações de tratamento de dados, de modo que sejam obedecidos os seus direitos, liberdades e garantias fundamentais dos dados desses trabalhadores.

Consoante Caldas (2019), o tratamento de dados pessoais por sistemas informatizados e algoritmos computacionais são de difícil compreensão para o sujeito

envolvido, pois há a expressa previsão de direito fundamental do mesmo em entender, ou melhor, de que lhe seja devidamente explicado os impactos com o claro objetivo de acionar os mecanismos de salvaguarda do direito fundamental na GDPR para a proteção de dados contra decisões automatizadas que afetem significativamente o direito a transparência do perfil do sujeito. A regra da GDPR é de que as decisões individuais automatizadas são sempre geradoras de obrigações e de direitos. Disso resulta que esse sujeito deva "[...] receba informações sobre a existência de tais decisões, sobre a sua lógica e sobre a importância e consequências previstas que possam ter". (CALDAS, 2019, p. 47).

Outro tópico importante abordado no artigo de Lima e Carvalho (2019), intitulado *O Direito ao apagamento de dados como realidade global*, sobre o direito de supressão de hiperligações ou à desindexação como sendo uma consagração de um direito ao apagamento de dados pessoais do sujeito e dos limites de tal direito. Os autores passam por uma discussão acerca dos efeitos, no continente, de uma ordem emanada por uma autoridade de uma nação que tenha que ser respeitada em outras nações da Comunidade Europeia e que, com isso, não impliquem ferir direitos constitucionais ou internacionais entre os estados-membros. Discute-se também sobre o cumprimento de determinações legais de caráter de extraterritorialidade (em outros países) e de apagamento tenha efetividade da tutela, de modo a salvaguardar o efeito útil desse direito do sujeito, sob pena de esvaziamento do direito ao esquecimento.

O objetivo da GDPR é a proteção de direitos e de garantias fundamentais dos cidadãos, com o intuito de diminuir os riscos em relação a um possível tratamento de dados, a partir da coleta e do futuro uso, compartilhamento, armazenamento, entre outros, desses dados. Desse modo, o alvo da GDPR é a proteção de dados pessoais em geral, de forma que o titular possa ter total controle sobre o tratamento de seus dados, do início ao fim, ou seja, até a exclusão dos dados. Da mesma forma, o autor aduz que a aplicação material do Regulamento (GDPR) está no seu Art. 2º, o qual prevê quais ramos de atividades são expostos à GDPR, compreendendo os tratamentos de dados automatizados e não automatizados em arquivo ou sem arquivo. Enfim, o GDPR deve ser aplicado no âmbito da *Internet* ou não (com ou sem tecnologia, em papel ou computador).

Por derradeiro, o referido artigo traz quais as situações em que não serão aplicadas as disposições da GDPR.

No Art. 3º, inciso I da GDPR, consta a aplicação da referida Lei em estabelecimentos localizados na união. Essa aplicação vai depender de onde está situado fisicamente o estabelecimento (extrapola os limites territoriais).

No que diz respeito à LGPD, foi intimamente influenciada pela GDPR, que teve sua eficácia plena em 25 de maio de 2018, após dois anos de *vacatio legis*, surgindo como modelo emblemático e importante legislação, tornando-se modelo para o mundo, inclusive para o Brasil, suas entidades públicas, privadas e cidadãos. Dessa forma, o estudo da GDPR tornou-se indispensável para o entendimento sobre proteção de dados pessoais. (MALDONADO *et al*., 2018).

De acordo com Pinheiro (2018b, p. 19):

> [...] a proteção das pessoas físicas relativamente ao tratamento de seus dados pessoais é um direito fundamental, garantido por diversas legislações em muitos países. Na, Europa, já estava previsto na carta dos Direitos Fundamentais Da União Europeia e no Tratado sobre o Funcionamento da União Europeia; no Brasil já tinha previsto no Marco Civil da *Internet* e na Lei do Cadastro Positivo, mas a questão ainda era, difusa e sem objetividade.

Outrossim, seguindo os moldes do regulamento europeu, a Lei Geral de Proteção de Dados brasileira (LGPD) foi inspirada no GDPR, tendo ambas o intuito de resguardar os dados dos cidadãos, para que esses tenham o conhecimento prévio das informações que estão fornecendo e a finalidade de sua utilização.

Assim, a LGPD é inspirada e influenciada diretamente pela GDPR, sendo que a primeira é uma resposta a segunda no que concerne à privacidade e ao tratamento de dados pessoais. Ambas são de caráter lógico e alicerçadas nos direitos fundamentais da pessoa humana.

3.1.1 Coleta de dados

Segundo o regulamento da GDPR, é preciso começar mencionando que, para que possam coletar dados, as empresas precisam necessariamente obter um consentimento dos usuários de forma expressa e inequívoca. Essa autorização prévia, determinada pela lei, deve ser muito clara ao dirimir a despeito da coleta e do tratamento de dados, bem como a finalidade para a qual serão utilizadas. (SÁ, 2019).

Nesse primeiro espectro, a lei ainda sinaliza que esse termo deve conter, de forma clara, quais serão os mecanismos e instrumentos de que o usuário poderá dispor caso preciso ou queria revogar esse consentimento. É importante mencionar que, segundo essa lei, esse consentimento poderá ser feito a qualquer momento. (SÁ, 2019).

Para Maldonado e Blum (2019), embora o consentimento seja primordial para o tratamento de dados, ele é somente uma das dez situações em que a lei permite tal tratamento. As demais possibilidades não envolvem o consentimento.

De acordo com Moniz (2018), há a seguinte reflexão acerca dos direitos do titular dos dados pessoais e do direito à portabilidade:

> A legislação de proteção de dados pessoais reconhece um lugar de relevo à vontade individual. De facto, um princípio nodal daquela é a participação do titular dos dados, o que, por um lado, lhe garante uma medida de influência nas operações de tratamento e, por outro, se reflete numa cartilha de direitos assegurados mesmo nos casos em que a licitude do tratamento consubstancia um controlo individual sobre os dados pessoais, independentemente do fundamento jurídico do tratamento. (MONIZ, 2018, p. 13).

De acordo com Moniz (2018), espelhando-se na proteção de dados na União Europeia, a vontade do indivíduo se sobressai no sentido de que sua participação nas operações de tratamento lhe confere mais proteção e controle sobre seus dados e de forma irrestrita das razões do tratamento.

Para Colombo e Facchini Neto (2017, p. 66-67, grifo dos autores):

> Atualmente, o fenômeno das modernas formas de gigantesca coleta de dados pessoais alterou a visão tradicional da privacidade em vários aspectos. Em primeiro lugar, as questões relacionadas à privacidade, que classicamente envolviam um indivíduo isolado (o clássico *right to be let alone*), envolvem simultaneamente milhões de pessoas, considerando a coleta de dados pessoais de consumidores, contribuintes, pacientes, usuários de todos os tipos de serviços, empregados, clientes, pensionistas, assalariados, ou seja, de todos nós. Em segundo lugar, vários dispositivos são capazes de transmitir informações a nosso respeito – celulares, GPS, cartões de crédito, redes sociais, etc. – de forma a se poder reconstituir quem nós somos, por onde circulamos, o que consumimos e o que pensamos. Em terceiro lugar, todas essas informações podem ser utilizadas não só para compreender quem nós somos e o que fazemos, mas principalmente para influenciar nossas condutas, principalmente enquanto consumidores.

Além disso, o fenômeno deixou de ser territorial para ser global, já que o tratamento de dados passou a envolver elementos transnacionais e globais, envolvendo pessoas localizadas em várias partes do mundo, sujeitas a jurisdições diversas e a diferentes normas de proteção de dados pessoais.

Portanto, a coleta de dados pode ser hodiernamente considerada transfronteiriça, uma vez que não se limita a um determinado local ou país. Além disso, a coleta pode ser feita de inúmeras formas e por meio de dispositivos diversos, proporcionando a circulação de informações de forma rápida e principalmente traçando um perfil do gosto e das necessidades de compras do consumidor, bem como influenciado suas decisões.

3.1.2 Direito e esquecimento

Para Magrani (2019), o Direito ao Esquecimento, no GDPR EU (2018), elencado no Capítulo III ‘Direitos do Titular de Dados na Seção 3 ‘Retificação e Apagamento’, os Art.s 16 a 20 abordam o tema. O Art. 17 trata especificamente do direito ao apagamento dos dados ou direito ao esquecimento. Isso se dá diferentemente do Brasil, que não mencionou expressamente tal direito na LGPD. O dispositivo pode ser utilizado nos casos em que a coleta de dados venha a infringir o mencionado Regulamento ou alguma outra legislação concernente a União Europeia ou a algum Estado-Membro a que o controlador esteja sujeito. (MAGRANI, 2019).

De acordo com os Art. s 7º e 8º da Carta dos Direitos Fundamentais da União Europeia EU (2000, grifo dos autores):

> O Direito ao Esquecimento tem suas origens e referências através dos autores Samuel D.Warren e Louis D. Brandeis quando do tema ‘The Right to Privaty’ abordaram a tese ‘Right to be let alone’. A partir dessa tese, em que defende como pressuposto do direito da propriedade. Assim, ao se deparar com o direito da privacidade este decorreria do direito da propriedade. Ideias estas amparadas na crença de cunho político-ideológico dos países americanos. Preceito este em contrassenso a partir das recentes normas do direito europeu. No âmbito legislativo e na fomentação da esteira dos direitos humanos vinculados estes ao direito do homem no Tribunal Europeu, alicerçou-se em meados de 2000, a ideia de que os direitos humanos, que são direitos fundamentais, devem resguardar o direito à vida privada e familiar e da proteção dos dados pessoais.

Maldonado e Blum (2018) explicam um caso em que, embora o direito ao esquecimento não tenha sido deferido, ele foi ventilado, demonstrando que já havia, em 1990, discussão a respeito na Europa:

> No direito ao esquecimento, ou direito de ser esquecido, não pode ser considerado novo em solo europeu, na medida em que são conhecidas decisões judiciais antigas, provenientes de jurisdições diversas, em que houve discussão acerca do tema. Um dos emblemáticos casos referentes ao homicídio de Walter Sedlmayr, ator que veio a ser assassinado em 1990 por dois meio-irmãos, que foram condenados à prisão perpétua. Concedidos os benefícios os benefícios do livramento condicional, nos anos de 2007 e 2008, postulou-se remoção de informações referentes aos autores do crime da plataforma Wikipedia, sendo certo que, em 2009, a Corte constitucional alemã afastou a pretensão. (MALDONADO; BLUM, 2018, p. 29).

Nas lições de Colombo e Facchini Neto (2017, p. 69):

> [...] a capacidade humana de relembrar, que nos acompanha desde a época das cavernas, permitiu que o homem comparasse, aprendesse e evoluísse. Igualmente importante, porém, é a habilidade humana de esquecer, deixando para trás o peso do passado e permitindo viver o presente de forma mais intensa. Por milênios, a relação entre lembrar e esquecer permaneceu clara. Lembrar é difícil e custoso e os humanos tinham que deliberadamente escolher o que lembrar. O normal era o esquecimento. Na era digital, essa questão se inverteu.

Ou seja, com a propagação da *Internet,* as informações permanecem guardadas, fazendo com que o passado se perpetue nas memórias dos computadores, ferindo tal direito muito mais facilmente. Para Mayer-Schönberger (2009, p. 196):

> Os dois lados da moeda – privacidade clássica e proteção de dados – muitas vezes estão ligados, como é o caso do direito ao esquecimento. A capacidade humana de relembrar, que nos acompanha desde a época das cavernas, permitiu que o homem comparasse, aprendesse e evoluísse. Igualmente importante, porém, é a habilidade humana de esquecer, deixando para trás o peso do passado e permitindo viver o presente de forma mais intensa. Por milênios, a relação entre lembrar e esquecer permaneceu clara. Lembrar é difícil e custoso e os humanos tinham que deliberadamente escolher o que lembrar. O normal era o esquecimento. Na era digital, essa equação se inverteu. Com a facilidade de armazenar um volume impressionante de informações, a memória digital tornou o passado um eterno presente. Lembranças passam a ser eternas e o esquecimento tornou-se exceção. (apud COLOMBO; FACCHINI NETO, 2017, p. 69).

Em suma, em uma sociedade em que tudo é publicado em nome de "*likes*" e "*deslikes*", o direito a ser esquecido, ou deixado só, assume extrema importância. Tendo em vista que tudo fica armazenado na rede, isso torna o passado sempre presente, ferindo diretamente a privacidade do indivíduo.

Um exemplo de caso no qual o direito ao esquecimento foi pleiteado ocorreu no ano de 2010 na Espanha. O autor (Mario Costeja González) ajuizou ação contra a editora La Vanguardia Ediciones SL e contra as empresas Google Spain e Google Inc. perante a Agência Espanhola de Proteção de Dados (AEPD). O autor alegou que seu nome, ao ser digitado nos mecanismos de busca do grupo Google (Google Search), apresentava a reportagem de um jornal sobre um leilão imobiliário para a quitação de dívidas devidas pelo requerente.

O autor pleiteou que a editora apagasse ou modificasse a reportagem dos mecanismos de buscas do Google a fim de resguardar seus dados pessoais. A AEPD entendeu que o conteúdo publicado era verídico e que a notícia havia sido feita de acordo com a Lei. Porém, acatou o pedido no sentido de que ambas as empresas apagassem os dados pessoais do autor de suas indexações, impossibilitando que seu nome fosse associado à reportagem. As empresas Google Spain e Google Inc. recorreram da decisão perante a Audiência Nacional (National High Court). O processo foi suspenso e encaminhado para o Tribunal de Justiça da União Europeia (TJUE):

> Pelos fundamentos expostos, o Tribunal de Justiça (Grande Secção) declara: 1) O artigo 2.°, alíneas b) e d), da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, deve ser interpretado no sentido de que, por um lado, a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na *Internet* por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência deve ser qualificada de «tratamento de dados pessoais», na aceção do artigo 2.°, alínea b), quando essas informações contenham dados pessoais, e de que, por outro, o operador desse motor de busca deve ser considerado «responsável» pelo dito tratamento, na aceção do referido artigo 2.°, alínea d). 2) O artigo 4.°, n.° 1, alínea a), da Diretiva 95/46 deve ser interpretado no sentido de que é efetuado um tratamento de dados pessoais no contexto das atividades de um estabelecimento do responsável por esse tratamento no território de um Estado-Membro, na aceção desta disposição, quando o operador de um motor de busca cria num Estado-Membro uma sucursal ou uma filial destinada a assegurar a promoção e a venda dos espaços publicitários propostos

> por esse motor de busca, cuja atividade é dirigida aos habitantes desse Estado-Membro. 3) Os artigos 12.°, alínea b), e 14.°**, primeiro parágrafo, alínea a), da Diretiva 95/46 devem ser interpretados no sentido de que, para respeitar os direitos previstos nestas disposições e desde que as condições por elas previstas estejam efetivamente satisfeitas, o operador de um motor de busca é obrigado a suprimir da lista de resultados, exibida na sequência de uma pesquisa efetuada a partir do nome de uma pessoa, as ligações a outras páginas web publicadas por terceiros e que contenham informações sobre essa pessoa, também na hipótese de esse nome ou de essas informações não serem prévia ou simultaneamente apagadas dessas páginas web, isto, se for caso disso, mesmo quando a sua publicação nas referidas páginas seja, em si mesma, lícita.** 4) Os artigos 12.°, alínea b), e 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46 devem ser interpretados no sentido de que, no âmbito da apreciação das condições de aplicação destas disposições, importa designadamente examinar se a pessoa em causa tem o direito de que a informação em questão sobre a sua pessoa deixe de ser associada ao seu nome através de uma lista de resultados exibida na sequência de uma pesquisa efetuada a partir do seu nome, sem que, todavia, a constatação desse direito pressuponha que a inclusão dessa informação nessa lista causa prejuízo a essa pessoa. Na medida em que esta pode, tendo em conta os seus direitos fundamentais **nos termos dos artigos 7.° e 8.° da Carta, requerer que a informação em questão deixe de estar à disposição do grande público devido à sua inclusão nessa lista de resultados, esses direitos prevalecem, em princípio, não só sobre o interesse económico do operador do motor de busca mas também sobre o interesse desse público em aceder à informação numa pesquisa sobre o nome dessa pessoa. No entanto, não será esse o caso se se afigurar que, por razões especiais como, por exemplo, o papel desempenhado por essa pessoa na vida pública, a ingerência nos seus direitos fundamentais é justificada pelo interesse preponderante do referido público em ter acesso à informação em questão, em virtude dessa inclusão.** (ESPANHA, 2014, p. 19-20, grifos nossos).

Deve-se buscar um equilíbrio justo entre o interesse legítimo dos internautas de obterem informações e os direitos fundamentais da pessoa, ao abrigo dos Art.s 7.º3 e 8.º4 da Carta dos Direitos Fundamentais da União Europeia. (PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA; COMISSÃO EUROPEIA, 2000).

3.1.3 Princípios *Data Protection by* Design e *by Defalt*

Os princípios *Data Protection By Design* e *By Defalt* são considerados fundamentais e advêm do princípio da responsabilidade, que é uma das principais características do GDPR, tendo em vista que se alicerçam no pilar do risco como

fundamento para a responsabilização. Nesse sentido, a autora portuguesa Lopes (2018, p. 51) aduz:

> Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, cabe ao responsável pelo tratamento aplicar as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o Regulamento.

O responsável pelo tratamento, à luz do princípio da responsabilidade, passa a aplicar medidas técnicas e organizativas para assegurar o cumprimento das regras de proteção de dados. Para isso, o regulamento Europeu ainda traz os princípios data *protection by design* e *by defalt*, nos termos do Art. 25º do GDPR. Esses princípios têm o intuito de assegurar a aplicabilidade da responsabilização, tendo em vista que visam "[...] promover o cumprimento por parte do responsável pelo tratamento das regras de proteção de dados durante todo o ciclo de vida dos projetos que envolvem o tratamento de dados pessoais, desde a fase de sua conceptualização, até o momento do próprio tratamento de dados". (LOPES, 2018).

Assim, a partir do princípio *data protection by design*, os agentes de tratamentos de dados deverão promover, durante todo o ciclo de vida do tratamento dos dados, desde seu início até o final do tratamento, as condutas especializadas próprias a fim de garantir e comprovar a aplicação efetiva dos princípios inerentes ao tratamento (tal como o da minimização), de forma para assegurar o cumprimento das regras de proteção de dados, bem como a cumprir com o GDPR. (LOPES, 2018).

Conclui a autora portuguesa que, da mesma forma, no que diz respeito ao princípio *by defalt*, os agentes de tratamento devem garantir que os dados dos titulares sejam tratados pelo menor tempo possível e da forma menos evasiva, tendo em vista os parâmetros do princípio da minimização de dados. Tudo isso deve-se dar já na fase inicial do tratamento para, de acordo coma GDPR, promover a privacidade dos dados do titular. Assim, a GDPR foi a primeira legislação a trazer esses conceitos chamados de *Privacy by Design* e *Privacy by Default*, que norteiam, por exemplo, *Frameworks*, para serem aplicados por empresas que pretendem se adequar às leis de proteção de dados.

3.2 Tratamento de dados pessoais e desafios

A LGPD estabelece que as atividades de tratamento de dados pessoais devem observar boa-fé nos princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e contribuição, de acordo com o Art.6 da Lei nº 13.709/18. (BRASIL, 2018).

Um dos principais desafios relacionados com o tratamento de dados pessoais, é a insegurança que a informação na era digital oferece. Diversas leis foram escritas no intuito de trazer proteção fora do âmbito virtual, como o Código de Defesa do Consumidor (BRASIL, 1990), porém, nos últimos anos, com o avanço desenfreado da *Internet*, aumenta, também, exponencialmente a insegurança no meio virtual, principalmente no que diz respeito a informações pessoais.

Nas palavras de Pinheiro (2018b), tratamento de dados é toda operação realizada com algum tipo de manuseio de dados pessoais.

No que concerne à responsabilidade do tratamento de dados, ensina Lopes (2018) que, nos termos da Diretiva 95/46/CE, o responsável pelo tratamento é identificado como a pessoa ou entidade que determina as finalidades e os meios de tratamento dos dados pessoais.

A evolução das relações virtuais trouxe um alerta importante relacionado com o fomento e a origem de um direito cibernético muito mais eficiente, que promovesse, antes de tudo, segurança aos usuários da rede de computadores, sobretudo naquilo que diz respeito a seus dados e informações pessoais.

De acordo com a LGPD, tratamento de dados pessoais entende-se por

> [...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2018).

Os requisitos para o tratamento de dados estão dispostos nos Art.s 7º,8º,9º e 10º da LGPD, ressaltando-se que, no Art. 7º, constam as dez hipóteses em que o tratamento é possível, conforme se observo Quadro 1, na página seguinte.

Quadro 1 – Hipóteses de tratamento de dados pessoais

	HIPÓTESES	DISPOSITIVO LEGAL	REQUER CONSENTIMENTO DO TITULAR?
1	Mediante consentimento do titular	LGPD, Art. 7º, inciso I	Sim
2	Para o cumprimento de obrigação legal ou regulatória	LGPD, Art. 7º, inciso II	Não
3	Para a execução de políticas públicas	LGPD, Art. 7º, inciso III	Não
4	Para a realização de estudos e pesquisas	LGPD, Art. 7º, inciso IV	Não
5	Para a execução ou preparação de contrato	LGPD, Art. 7º, inciso V	Termos de consentimento definidos no contrato ou decorrentes da autonomia da vontade
6	Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, Art. 7º, inciso VI	Não
7	Para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, Art. 7º, inciso VII	Não
8	Para a tutela da saúde do titular	LGPD, Art. 7º, inciso VIII	Não
9	Para atender interesses legítimos do controlador ou de terceiro	LGPD, Art. 7º, inciso IX	Não
10	Para proteção do crédito	Art. 7º, inciso X	Não

Fonte: Brasil (2020).

"I - Mediante o fornecimento de consentimento pelo titular". (BRASIL, 2018):[5]

O consentimento é apenas uma das formas em que é possível o tratamento de dados pessoais. No entanto, de acordo com o §6º do Art. 7º da LGPD, não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Para Pinheiro (2018b), o consentimento do titular é a linha mestra do tratamento de dados e apenas excepcionalmente o tratamento ocorrerá sem tal hipótese expressa, porém sempre respeitando a sua finalidade específica.

Segundo Magrani (2019), o processamento não baseado em consentimento deve considerar a natureza dos dados pessoais, as possíveis consequências do processamento e a existência de garantias apropriadas.

[5] Para diferenciar os artigos e incisos da lei analisados do restante do texto e citações, serão colocados em itálicos e entre aspas.

“*II - Para o cumprimento de obrigação legal ou regulatória pelo controlador*”. (BRASIL, 2018):

Ou seja, os dados pessoais poderão ser operados em todas as situações em que as relações jurídicas assim o exigirem, em virtude de determinação legal ou regulatória, não podendo o titular impugnar o tratamento.

“III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei”. (BRASIL, 2018):

De acordo com esse inciso, a administração pública poderá tratar dados pessoais quando imprescindíveis para execução de políticas públicas positivadas em leis e regulamentos, ou fundamentados em contratos, convênios, entre outros.

“*IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais*”. (BRASIL, 2018):

A LGPD, trouxe como hipótese ou justificativa para tratar os dados pessoais o caso em que órgãos de pesquisa, como por exemplo o IBGE, realizem estudos imprescindíveis para a execução de políticas públicas, todavia garantindo sempre a anonimização dos dados. Ou seja, entende-se por dados anonimizados aqueles que sejam pessoais ou sensíveis, que foram tratados para que suas informações não possam ser vinculadas ao seu titular original. Pela própria definição da lei, ele “[...] perde a possibilidade de associação, direta ou indireta, a um indivíduo”

“*V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados*”. (BRASIL, 2018)

Nessa hipótese, de acordo com a LGPD (BRASIL, 2018), o tratamento de dados ocorrerá a pedido do próprio titular dos dados. Nesse inciso, o tratamento de dados também ocorre mediante um consentimento, todavia, nesse caso, o titular dos dados não poderá revogar o seu consentimento a qualquer momento, tendo em vista que a outra parte do estará resguardada pela Lei para poder manter os dados fornecidos pelo titular enquanto o contrato estiver em vigor.

"*VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)*". (BRASIL 2018):

Esse inciso, garantido pela LGPD, traz a possibilidade de garantir o direito de produção de provas de uma parte contra a outra em um processo judicial (na maioria das vezes), administrativo ou arbitral, esse último nos termos da Lei de Arbitragem.

Nas lições de Maldonado e Blum (2019, p. 184):

> [...] Nas situações em que se entender que determinados dados pessoais poderão servir como elemento para exercícios de direitos em demanda em geral, eles poderão ser armazenados, desde que para essa única e exclusiva finalidade, enquanto subsistir tal finalidade.

Assim, permitir que uma das partes se oponha a esse tipo de tratamento de dados seria cercear o direito de defesa da outra.

"*VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros*". (BRASIL, 2018):

O objetivo desse inciso autorizador é garantir a proteção de bens de grande interesse público, tais como a vida, que é uma garantia fundamental prevista no Art. 5º, caput da Constituição Federal Brasileira. Também protege a incolumidade física, desde que devidamente comprovada essa necessidade e exposta a finalidade do tratamento dos dados nesta situação. Lembra-se que essa necessidade, que é uma limitadora para o tratamento, é dada pelos princípios contidos no Art. 6º da LGPD.

"*VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)*". (BRASIL, 2018).

O inciso VIII é mais uma das hipóteses autorizativas para o tratamento de dados pessoais, independentemente do consentimento do titular. Enquadram-se nessa hipótese, de acordo com Maldonado e Blum (2019, p. 185):

> [...] Os profissionais da área da saúde, (médicos, farmacêuticos, enfermeiros, educadores físicos, fisioterapeutas, psicólogos, nutricionistas, biólogos, biomédicos, entre outros) e as entidades que são membros do SNVS (Agência Nacional de Vigilância Sanitária), Laboratórios Centrais de Saúde Pública (LACENS; Instituto Nacional

> de Controles de Qualidade em Saúde (INCQS); Fundação Oswaldo Cruz (FIOCRUZ), além de outras entidades, inclusive estaduais e municipais. [...].

"IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais". (BRASIL, 2018).

Esse inciso autorizador, apesar de subjetivo, deve ser compreendido à luz do Art. 10º da LGPD, pois, no referido Art., traz as possibilidades em que o legítimo interesse do controlador "[...] somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas", mas com limitações também dispostas no Art. 10º.

"*X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente*". (BRASIL, 2018).

Esse último inciso protege, de certa forma, a economia, pois, nesse caso, não se está protegendo o titular de dados inadimplente.

É imperioso observar que as hipóteses são taxativas, uma vez que o legislador utilizou a palavra "somente" para enumerá-las.

> § 1º (Revogado). (Redação dada pela Lei nº 13.853, de 2019).
> § 2º (Revogado). (Redação dada pela Lei nº 13.853, de 2019).
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. (BRASIL, 2018).

A boa-fé é um dos pilares do consentimento, juntamente com a finalidade. Já o interesse público sempre deve sobrepor-se ao privado. Dessa feita, é imprescindível que se diga que mesmo que os dados pessoais sejam de acesso público, eles não deixam de pertencer ao titular de dados.

> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

Esse parágrafo deve ser analisado conjuntamente com o inciso I, do Art. 7º e o Art. 8 da LGPD, pois falam acerca do consentimento. No inciso I, fala da hipótese de

tratamento dos dados pessoais a partir do consentimento do titular dos dados. Já no Art. 8 º, aduz que o consentimento dado deve ser comprovado de forma inequívoca, por via expressa ou por outros meios, cabendo ao controlador o ônus de comprová-lo.

De acordo com Moreira (2019, grifos do autor):

> Ao contemplar essas obrigações pelo viés prático, é inegável que a ‘gestão dos consentimentos’ pode ser tarefa de elevada complexidade e potencialmente problemática. Qualquer uso de dados com finalidade diversa da autorização conferida, ou a ausência de comprovação efetiva do consentimento recebido, tornam os controladores passíveis de receberem as sanções legais previstas na LGPD (Arts. 52 a 54) e de serem responsabilizados ao ressarcimento de danos causados ao titular dos dados pelo uso indevido destes.

“§ 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

§ 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular”. (BRASIL, 2018):

> § 6º do Art. 8º da LGPD procura assegurar o seu pleno direito de informação, prevendo que “Em caso de alteração de informação referida nos incisos I, II, III ou V do Art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

“*§ 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei*”[6]. (BRASIL, 2018):

[6] Incluído pela Lei nº 13.853, de 2019.

Na LGPD, a segurança é um princípio a ser observado no tratamento de dados pessoais, conjuntamente com as hipóteses do Art. 7º, destacado pelo Art. 6º, inciso VII.

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

De acordo com o Guia de Boas Práticas da LGPD (BRASIL, 2020), a empresa deve comprovar que está em conformidade com a LGPD por meio do cumprimento das regras de proteção de dados pessoais. Essa comprovação deve ser analisada caso a caso, sempre com a prévio conhecimento por parte do titular no que concerne às hipóteses para o tratamento dos dados:

> O importante é avaliar caso a caso e documentar a(s) hipótese(s) aplicável(is), uma vez que o titular deverá conhecer a hipótese legal que autoriza o processamento de seus dados pessoais. Além disso, o princípio da responsabilização e prestação de contas requer que o órgão ou entidade que realiza o tratamento de dados pessoais possa demonstrar que está plenamente aderente à LGPD, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto a sua eficácia. (BRASIL, 2020, p. 22).

O Art. 8º e seus parágrafos da LGPD tratam do consentimento do titular dos dados pessoais:

*"*Art. *8º O consentimento previsto no inciso I do* Art. *7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular*.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais". (BRASIL,2018)

> Mesmo a declaração escrita não necessariamente atenderá, por si só, aos requisitos legais do consentimento, pois deverá ser contextualizada diante dos demais critérios atestadores da formação livre e informada da vontade, dentre os quais o previsto no § 1º do Art. 8º da LGPD, segundo o qual 'Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. (FRAZÂO, 2018).

"*§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.*

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento". (BRASIL, 2018).

O consentimento deve ser inequívoco.

"*§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas*". (BRASIL, 2018):

> § 4º do Art. 8º da LGPD reforça a observância ao princípio da finalidade, prevendo que 'O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.' A LGPD não exige necessariamente o consentimento escrito, limitando-se o seu Art. 8º a prever que "O consentimento previsto no inciso I do Art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (FRAZÃO, 2018).

"*§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do* Art. *18 desta Lei*". (BRASIL,2018)

Este inciso demonstra o empoderamento do titular e de seus dados e a relevância do direito de liberdade e privacidade, pois o consentimento pode ser revogado a qualquer tempo, de forma facilitada e gratuita.

"*§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do* Art. *9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração*". (BRASIL, 2018):

> § 6º do Art. 8º da LGPD procura assegurar o seu pleno direito de informação, prevendo que 'Em caso de alteração de informação referida nos incisos I, II, III ou V do Art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração. (FRAZÃO, 2018).

O Art. 9º, nas lições de Magrani (2019, p. 122):

> [...] em regra, há dados que não podem sofrer tratamento por nenhuma pessoa ou entidade, como aqueles que revelem a origem racial ou étnica, as opiniões políticas ou dados biométricos que permitam identificar uma pessoa de forma inequívoca. Há, entretanto, exceções a esta exclusão, previstas no item 2 do artigo 9º.

"Art. *9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso. [...]*". (BRASIL, 2018).

Nas lições de Pinheiro (2018a), sobre a questão da transparência, apontam-se quais são as particularidades atinentes ao livre acesso à informação. O Art. 9º, de acordo González (2019), dá direito ao titular de dados de ser informado e de ter informações sobre o tratamento de seus dados, a finalidade a duração, a forma de tratamento, assim como saber se seus dados estão sendo ou foram compartilhados com outros agentes. Cabem aos agentes de tratamento (controladores e operadores) essas obrigações.

O primeiro parágrafo aduz que, se o consentimento não for dado na forma da LGPD, ele será considerado nulo. Além disso, caso a finalidade do tratamento mude, o consentimento deverá ser dado novamente pelo titular, que tem a opção de não renovar seu consentimento para essa nova possibilidade.

O controlador ainda deve deixar claro ao titular de dados sobre os produtos e serviços a que ele deixará de ter acesso caso não forneça o consentimento. Dessa forma, garante-se a plena ciência do titular e seu discernimento sobre consentir ou não sobre o tratamento de seus dados para os fins apresentados.

O conceito de "legítimo interesse" é subjetivo, pois a LGPD não traz sua definição. Todavia, só será possível compreender exatamente sua extensão e aplicação a partir das situações concretas que forem aparecendo ao longo da atuação da ANPD após a entrada em vigor da lei.

É ônus da autoridade nacional fiscalizar, por meio da solicitação de relatórios, sobre o impacto que as atividades de legítimo interesse têm sobre a proteção dos dados pessoais tratados.

No que concerne aos desafios da proteção da privacidade sob a ótica da exclusão, não faz mais sentido, principalmente se a proteção somente é constatada

quando a violência é externa. Deve ser levada essa proteção em consideração, também como fomento da cidadania. Desse modo, ela possui uma dimensão coletiva, porque a cidadania é um dos pressupostos de uma sociedade democrática moderna, e também é função promocional na busca por promoção da proteção da pessoa humana. (DI FIORE, 2012).

A partir desse ponto, a proteção à privacidade deixou de ser observada somente por meio da administração de “bens” ou “espaços”, mas passou a ser conceituada como uma determinação que adentra a nossa própria esfera pessoa. Ela nem constituiria um valor em si mesma, seria um modo se tutelar a pessoa. Além disso, apresenta um caráter relacional, pois está intimamente ligada à relação da pessoa com o mundo exterior e com outras pessoas. (JABUR, 2000).

É possível identificar, atualmente, quais são as empresas, servidores, plataformas que possuem os seus dados como indivíduo. Da mesma forma, é possível ter conhecimento da finalidade que estão tendo a partir da sua coleta. Ter acesso a esse tipo de informação significa que o controle das suas informações está em sua posse e, desse modo, entender que a privacidade, para a seu compreendida em sua amplitude, como um direito à autodeterminação informativa. (BODIN, 2020).

A vigilância, nesse sentido, pode ser ampliada, pautada nas inovações e implantação de novas técnicas. Porém, dentro desse mesmo contexto, em conjunto com as formas de controle, passam cada vez mais desapercebidas e se tornam mais nocivas ao próprio direito à liberdade.

A busca atual, diante desse cenário, é por medidas de cunho institucional que tenham o condão de conter esse expressivo e avassalador avanço paulatino. Dentro do tratamento que é ofertado aos dados pessoais, a proteção ao indivíduo é o cerne que envolve a questão de forma mais ampla. (BAIÃO; GONÇALVES, 2014).

O tratamento de dados deve considerar tanto a identidade social como a identidade individual do usuário. Também devem ser aferidos o corpo físico e o contexto eletrônico. Isso deve ser feito com a finalidade de obter proteção pelos meios adequados. Dentro do universo da *Internet*, no entanto, segundo Baião e Gonçalves (2014), é preciso fazer o equilíbrio entre o supracitado princípio da liberdade de acesso, em conjunto com o princípio da dignidade da pessoa humana.

O princípio da dignidade da pessoa humana é um princípio basilar dentro da esfera do ordenamento jurídico brasileiro, conforme a redação do Art. 1° da CF/88:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado democrático de direito e tem como fundamentos:[...]III – a dignidade da pessoa humana. (BRASIL, 1988).

Como princípio fundamental, possui unidade conferida pelo princípio da dignidade. Esse princípio é o responsável por conferir ao homem o seu direito de ser tratado como um fim em si mesmo e não meramente como um meio, condicionado à vontade dos demais. Por isso, é um valor universal que goza de incondicionalidade, tendo liberdade para reger toda e qualquer ação.

Qualquer condição que, partindo desse pressuposto, tende a querer limitar a condição do ser humano, como a um objeto, pode ser concebida como desumana ou anto-humana. Esse tipo de ação costuma legitimar a prática de discriminações ou promover a redução das pessoas que estão inseridas na nova sociedade da informação.

Nesse sentido de coibir as coisas que atentam contra a dignidade da pessoa, comparando-a a um objeto, de acordo com Moraes (2020, p. 34), “[...] as coisas têm preço; as pessoas, dignidade”. Essa sua afirmação surge da concepção de que o homem, sob essa ótica, poderá, a qualquer tempo, ser instrumentalizado como forma de alcançar alguma finalidade, quaisquer que sejam elas.

Essa autonomia, que antigamente era compreendida por meio de uma ótica individualista e patrimonialista, passa por um processo de reformulação, que permite que, ao se ampliarem e abrangerem aspectos existenciais, contribua para a construção de identidades e da garantia da própria dignidade. Desse modo, essa nova concepção de dignidade é o epicentro do ordenamento jurídico brasileiro atual. Ela possui a garantia de permitir que um indivíduo possa agir de maneira autônoma, e isso abrange pessoas em todas as suas possíveis concepções e emanações.

Essa é uma das formas de promoção da Constituição Federal de 1988 (BRASIL, 1988) e suas diretrizes fundamentais e garantias. A dignidade é parte fundamental do conceito de ser humano, dele não pode ser desvinculado. É também, no entendimento de Baião e Gonçalves (2014), condição intrínseca do próprio direito à liberdade, de modo que não existe dignidade se não existir autonomia.

Logo, pode-se presumir que a autonomia é um elemento consistente e ético da própria noção de dignidade. Dessa forma, deve ser assegurada em conjunto com a possibilidade de autodeterminação do indivíduo. Ele deve ter a capacidade de

conseguir desenvolver de forma livre a sua personalidade, arbitrando os cursos de sua própria existência. (BAIÃO; GONÇALVES, 2014).

4 *COMPLIANCE* APLICADO À PROTEÇÃO DE DADOS COMO FORMA DE MITIGAÇÃO DE RISCOS

Neste quarto e último capítulo, aborda-se o *compliance* como forma de mitigação de riscos, os padrões de segurança que as empresas devem seguir, os termos de uso, políticas de privacidade como melhores práticas a serem seguidas. Ao final, propõe-se um *Framework* como alternativa para as empresas se adequarem à Lei Geral de Proteção de Dados.

Tendo em vista a relevância do assunto *compliance* para as empresas e para a proteção de dados pessoais, necessita-se de uma análise sobre o tema. As inovações e transformações ocorridas em época contemporânea, em especial depois do advento da revolução trazida pela era tecnológica, fizeram com que fosse necessária a criação de mecanismos que propiciem que as empresas e organizações funcionem de acordo com as leis e normas vigentes.

A Lei Geral de Proteção de Dados entrará em vigor em 2020, e as organizações deverão cumprir com as normas e regulamentos dispostos nesta lei. No sentido da palavra *compliance,* de origem inglesa, que tem como origem o verbo *to comply with*, cuja tradução em nossa língua tem o significado de agir de acordo com, ou seja, agir de acordo com o que determinam as leis do país onde a empresa tem sua sede, ou, ainda, agir de acordo com a legislação dos países com os quais a organização se relaciona. (CAPRA, 2019).

Em se tratando dos objetivos que se busca alcançar com o *Compliance,* cumpre destacar as palavras de Blum (2020, p. 7):

> O combate à prática de atos lesivos no meio corporativo deve ser uma constante e medidas preventivas devem ser sempre priorizadas, para que, por consequência, esse ambiente não seja comprometido por uma violação à segurança da informação, da marca, reputação, dados pessoais, entre outros importantes valores e ativos empresariais.

Segundo o entendimento de Blum (2020, p. 7, grifo do autor), a “[...] sistemática de um *compliance* digital tem o condão de permitir a prevenção e resolução dos efeitos de condutas lesivas, negligentes, culposas, ou mesmo não intencionais”.

Esse conjunto de ações que se traduzem em *compliance* nada mais são do que medidas efetivas e práticas tomadas pela administração da empresa ou organização, as quais têm por finalidade aplicar e submeter princípios éticos às decisões tomadas

pela empresa. No tocante aos princípios norteadores dessas condutas, ensinam Oliveira *et al.* (2019, p. 6, grifo do autor): “Inicialmente, o empresário que usa, coleta ou armazena dados de qualquer pessoa deve observar, além da boa-fé, os princípios trazidos pela Lei 13.709/2018, no Art. 6º, para se manter em *compliance*”. Para a realização dessas práticas, deverão as empresas e organizações contar com um setor de gestão para tratar essas questões em conformidade com a nova legislação.

O consumo, no século XXI, impõe a existência de empresas confiáveis, de modo que é necessária a implantação de códigos de ética, de conduta, padrões de integridade, sendo o *compliance* a observância de regras e condutas para agir em conformidade com a lei.

A forma como será implementado esse conjunto de ações – *Compliance* -, não será uma tarefa simples, haja vista que os negócios na atualidade estão globalizados, os dados pessoais estão circulando pela *Internet* de forma internacionalizada. Por isso, há a necessidade de aplicação de uma abordagem de direito comparado e de direito internacional. (PINHEIRO, 2018a).

Para a implementação dos requisitos de conformidade à LGPD, deverão ser observadas etapas, as quais consistem, em um primeiro momento, na realização de um levantamento de dados com o fim de se identificar como a organização se encontra no que se refere aos indicadores de conformidade e quais elementos faltam para cumprir aos controles exigidos. Pode-se definir esse levantamento como um inventário dos dados pessoais (quais são e onde se encontram). Em um segundo momento, é necessário montar o padrão de tratamento dos dados pessoais (quais os tipos de tratamento e para qual finalidade). Seguindo, em um terceiro momento, precisa-se verificar de que forma está sendo realizado o controle de gestão de consentimentos. Com base nesses dados, desenvolve-se o mapa de risco e elabora-se o plano de ação. Nessa fase, é possível elaborar a cotação dos investimentos necessários para a adequação, os quais serão implementados em quatro níveis, a saber: nível técnico (ferramentas), documental (adequar normas, políticas e contratos), procedimental (adaptar a governança e a gestão dos dados pessoais) e cultural (realização de treinamentos e campanhas de conscientização das equipes, dos parceiros, fornecedores e clientes). (PINHEIRO, 2018a).

Segundo Pinheiro (2018a), resumidamente, essas etapas podem ser assim descritas:

> a) na revisão e atualização da política de privacidade para estar em conformidade com as novas regulamentações de proteção de dados pessoais;
> b) na atualização das cláusulas de contratos (seja com titular de dados pessoais consumidor final ou funcionário);
> c) na atualização das cláusulas de contratos com os parceiros e fornecedores que realizam algum tipo de tratamento de dados, principalmente fornecedores de soluções de gestão de informação, nuvem, monitoração, mensageria, e-mail marketing, credit score, big data, mídias sociais (coleta, produção, recepção, classificação, acesso, utilização, transmissão, armazenagem, processamento, eliminação, enriquecimento);
> d) no mapeamento do fluxo de dados para definição da nova governança junto ao TI dos controles de consentimento (ciclo de vida do dado - coleta, uso, compartilhamento, enriquecimento, armazenamento nacional ou internacional, com ou sem uso de nuvem, eliminação, portabilidade);
> e) no modelo de resposta para o Notice Letter do Órgão de Controle de Dados (sobre nível de conformidade da empresa e controles auditáveis) para prevenção e aplicação de multas e fiscalizações;
> f) no modelo de check-list de compliance para uso da área de compras para novos fornecedores e parceiros, que precisarão estar em conformidade com as novas regulamentações de proteção de dados pessoais;
> g) no modelo para gestão e guarda de trilha de auditoria para gestão dos logs de consentimento. (PINHEIRO, 2018a).

De acordo com o previsto na legislação, a empresa deverá atualizar os documentos de gestão, com o fim de realizar o *Compliance*. A seguir, listam-se os documentos que necessitam ser atualizados. (PINHEIRO, 2018b).

- Mapa de fluxo de dados pessoais (*Personal Data Flow Map*):

Trata-se de um documento essencial quando o objetivo é adequar a empresa ou organização aos ditames da LGPD e GDPR. Segundo esse mapa ou planilha, é possível ter ciência do caminho percorrido pelo dado pessoal dentro da organização. Dessa forma, nesse trajeto, são demonstrados o processo e o procedimento nos quais o dado transita. Com efeito, esse documento permite saber qual a origem (a forma como foi capturado), a base legal que legitima a coleta do dado pessoal, o nível de segurança da base de dados à qual o dado pertence, bem como outras informações que servem como base para a avaliação de vulnerabilidade técnica e jurídicas. (BRANDÃO, 2020).

No tocante ao fluxo internacional de dados, escreve Somadossi (2018):

> Outro aspecto de relevo é o fluxo de dados para outros países, a chamada transferência internacional de dados, que somente será permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais compatível com a lei brasileira ou mediante oferecimento de garantias do regime de proteção de dados local.

- Tabela de temporalidade de guarda de *logs* de consentimento;
- Política de gestão de dados pessoais (que deve ser assinada inclusive *inter companies* – entre empresas do mesmo grupo econômico, entre matriz e filiais);
- Política para tratamento de dados pessoais para terceirizados (*providers* que realizam tratamento de dados pessoais – vários procedimentos trazidos no GDPR e na LGPD sobre fluxo, padrão de criptografia, guarda de logs, etc);
- Termo de uso e Política de privacidade (atualizar batendo tratamento x finalidade de uso x justificativa jurídica x matriz de consentimentos, novos direitos dos usuários como portabilidade, exclusão, minimização de uso, limitação e outros);
- Contratos (atualizar com cláusulas que preveem GDPR e LGPD);
- NDA (atualizar com cláusulas que preveem GDPR e LGPD);
- *Check-list Compliance* (atualizar com cláusulas que preveem GDPR e LGPD);
- Código de Conduta (atualizar com cláusulas que preveem respeito à proteção de dados pessoais);
- Política de Segurança da Informação (atualizar com cláusulas que preveem GDPR e LGPD).

4.1 Os padrões de segurança das empresas e a proteção de dados

Uma maneira possível para as empresas e organizações que manejam dados pessoais adaptarem-se aos requisitos trazidos pelas leis de proteção de dados pessoais é instituir o uso e fazer as adaptações a cada caso dos *Frameworks* ou padrões de segurança, mormente se essa empresa ou organização já faz uso de

alguma ferramenta de segurança digital. (NAKAMURA; FORMIGONI FILHO; IDE, 2019).

Dito isso, pode-se salientar que esses Programas de Integridade – *Compliance* – têm se mostrado uma excelente ferramenta para a efetivação de adequação à LGPD.

É importante salientar que o programa ou sistema a ser adotado poderá ser proporcional ao porte da corporação, bem como aos riscos que ela enfrenta. (OLIVEIRA *et al.*, 2019).

Com efeito, cumpre mencionar que, de acordo com a Portaria Conjunta da CGU e do Ministério da Micro e Pequena Empresa n. 2279/2015, indica-se a adoção de procedimentos de integridade menos formais, bem como mais singelos, com a finalidade de garantir o manejo dos dados pessoais de forma ética e íntegra, entre microempreendedores e empresas de pequeno porte. (OLIVEIRA *et al.*, 2019).

Portanto, conforme o exposto, é possível afirmar que, quanto maior for a empresa e quanto maiores forem os riscos aos quais possa estar sujeita, de maior complexidade será a tarefa de incorporar um sistema de conformidade com a LGPD.

Adiante, um dos *Frameworks* mais utilizados são as normas da família ISO 27000. Essas normas tratam de um programa para pôr em execução um Sistema de Gestão de Segurança da Informação (SGSI), sendo as mais conhecidas a ISO 27001. (ISO 27001, 2006).

Sobre estes programas, ensinam Nakamura, Formigoni Filho e Ide (2019, p. 3):

> [...] Descreve um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI e a ISO 27002 [ABNT NBR ISO 27002, 2005], que oferece objetivos de controles de segurança, que serão implementados pelos responsáveis pelo SGSI, dependendo da aplicabilidade e resultados da análise de riscos e também dos requisitos de segurança identificados naquele contexto.

Inobstante o fato de que as empresas, de um modo geral, utilizam o ISO 27000 como *Framework* para a segurança da informação, pode-se dizer que a implementação de forma isolada dessa ferramenta não garante a segurança da informação nos moldes do preconizado nas legislações pertinentes. O objeto de abrangência da família 27000 diz respeito à segurança da informação do ponto de vista da organização que está implementando o SGSI, não incluindo assim os direitos

dos indivíduos. Pode-se citar, à luz da LGPD, como exemplos de direitos das pessoas não abrangidos pelo ISSO 27000 o direito de ter informações removidas e o consentimento do dono das informações.

Assim sendo, no tocante aos mecanismos para desenvolver a conformidade com a LGPD, o grupo de normas ISO 27000 mostra-se como uma moderna e importante ferramenta de proteção de dados, notadamente a ISO 27001. Tais normas definem requisitos para um sistema de gestão de segurança da informação (SGSI) bem como sua operação. (OLIVEIRA *et al*., 2019).

Cumpre mencionar que a referida normativa é adotada como padrão internacional, sendo reconhecida e validada para a segurança da informação. Conforme essas normas, seguem um sistema de gestão no qual são avaliados os riscos de segurança e proteção, adotando procedimentos de controle e de monitoramento do desempenho dos processos. Atua, ainda, de forma conjunta para reforçar os programas de integridade que visam proteger os dados pessoais e a privacidade dos indivíduos. (OLIVEIRA *et al*., 2019).

Sobre esse assunto, escreve Pinheiro (2018b, p. 45):

> Dependendo do ramo do negócio, da empresa e da maturidade da governança dos dados pessoais, é fundamental criar um programa de compliance digitall, com risk assessment, planos de respostas a incidentes, treinamentos e comunicação, due diligence de terceiros em um contexto multissetorial dentro do negócio e com visão holística para a legislação nacional e internacional.

Assim, para se manter em *compliance* com a LGPD, devem as instituições observar outras questões práticas, tais como a elaboração de um adequado Termo de Uso e de Políticas de Privacidade.

4.2 As funções dos termos de uso e das políticas de privacidade

Com o advento da LGPD, inicia-se uma nova etapa, na qual a tutela material dos dados pessoais tratados no ambiente digital ou fora dele é dever que se impõe.

Anteriormente ao surgimento da GDPR em solo europeu e a LGPD em nosso país, as relações digitais eram tratadas de uma forma incompleta, haja vista que tais relações eram regidas pela Lei nº 12.965/14, conhecida como “Marco Civil da *Internet*” (BRASIL, 2014). Nessa realidade, a prática de atos abusivos cometidos pelas

empresas no tocante à coleta, ao tratamento e à exploração de dados pessoais era uma conduta rotineira. Fora do ambiente digital, a situação ainda era mais precária, diante da inexistência de um controle mínimo quanto ao manejo das informações pessoais, mesmo havendo outras normas dispostas em leis esparsas, sendo o Código de Defesa do Consumidor e as leis do Cadastro Positivo (nº 12.414/11) e de Acesso à Informação (nº 12.527/11), ainda, a disposição constitucional da garantia fundamental à vida privada, assegurada no Art. 5º, X, da Constituição Federal. (OLIVEIRA *et al.*, 2019).

Para Magrani, essa nova realidade mundial traz mudanças significativas, uma vez que os indivíduos a cada dia mais utilizam o ambiente virtual para desenvolver as relações sociais, produzindo um grande volume de dados – o chamado Big Data Analytics.

No entanto, tudo acaba ferindo a privacidade do indivíduo, gerando as chamadas “bolhas de Informação” (*filter bubbles*), que são as respostas obtidas de forma especializada a partir das preferências dos titulares de dados.

Portanto, as mudanças às quais a atividade empresarial deverá adaptar-se dizem respeito à forma como procederá no gerenciamento desses dados pessoais, uma vez que, para continuar a exercer suas atividades típicas, deverá seguir os ditames das novas legislações criadas.

É certo que, nas últimas décadas, a informação ganhou extrema importância, revestindo-se da característica de ativo dotado de valor financeiro e de mercado. Como resultado dessa nova realidade, cresceram exponencialmente as atividades empresariais com atividade de exploração de dados, sistematização da informação e formação de banco de dados. (DONEDA, 2010).

Com o surgimento desses novos negócios no ambiente virtual, há o incremento dos documentos intitulados “Termos de Uso” e “Política de Privacidade”, que se destinam a regular as relações dos usuários de sites e serviços de *Internet*, inclusive no que tange às ações ligadas ao tratamento de dados pessoais, desde a coleta, passando pelo armazenamento, até sua eliminação. (OLIVEIRA *et al.*, 2019).

Para Oliveira *et al.* (2019, p. 186, grifos dos autores):

> Torna-se, portanto, obrigatório adotar, desde a concepção de serviços, produtos e modelos de negócio, a prática de se garantir direitos de proteção à privacidade e aos dados pessoais. São os chamados *privacy by design e by default*, em que o primeiro modelo permite uma

> adequação do formato e níveis de privacidade a ser cedida por determinado usuário, enquanto o segundo não se concebe tal possibilidade.

Em se tratando da natureza jurídica e relativamente aos efeitos que geram esses documentos “Termos de Uso” e “Política de Privacidade”, não há na doutrina e jurisprudência uma posição uniforme. Com efeito, é possível moldá-los às ferramentas já existentes no ordenamento jurídico pátrio relativamente aos contratos de adesão, cuja principal característica é a existência das figuras do proponente e do aderente. O primeiro é o responsável por estabelecer cláusulas e condições contratuais, enquanto o segundo tem apenas a opção de aceitar ou rejeitar o contrato como um todo, renunciando à possibilidade de negociar os termos do contrato. (OLIVEIRA *et al.*, 2019).

Quanto a essa relação adesiva, leciona Magrani (2019, p. 158): “[...] malgrado tratar-se de espaços privados, os usuários não podem sujeitar-se a termos de uso abusivos que restrinjam de forma desproporcional seus direitos garantidos na Constituição”. Dito isso, é correto afirmar que o ambiente virtual não deve ser tão somente um espaço para o exercício do direito disponível, devendo ser uma forma para a efetivação de inúmeros direitos sociais e individuais.

É importante destacar que as empresas que oferecem serviços no ambiente digital, para entrar em *compliance* com a LGPD, deverão dispor, em seus Termos de Uso e Políticas de Privacidade, informações claras e transparentes quanto à forma como os dados pessoais serão tratados, atendendo aos princípios dispostos nos incisos do Art. 6º, sendo estes (I) finalidade, (II) adequação (III) necessidade e (VI) transparência.

4.3 Privacidade *by Design* e Privacidade *by Default*

A metodologia que visa resguardar a privacidade dos usuários no ambiente digital recebe a denominação de Privacidade *By Design* e Privacidade *by Default*, estando essas condutas inseridas nos Art.s 46, § 2º e 49 da Lei 13.709/18 – Lei Geral de Proteção de Dados. (MURARO, 2020).

As medidas elencadas no *caput* do Art. 46 da LGPD são medidas de segurança, técnicas e administrativas, que têm por finalidade a proteção dos dados pessoais de acessos não autorizados, proteção quanto a episódios acidentais ou ilícitos de

destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Essas medidas deverão ser observadas pelos agentes de tratamento desde a concepção do produto ou serviço até a fase de sua consumação. (MALDONADO; BLUM, 2019).

Assim sendo, no conceito de Maldonado e Blum, o termo *privacy by design*: "[...] refere-se, portanto, à metodologia que visa proteger a privacidade do usuário desde a concepção de quaisquer sistemas de tecnologia da informação ou de práticas de negócio que sejam concernentes ao ser humano". (MALDONADO; BLUM, 2019, p. 336). Nessa metodologia, o ponto inicial para se desenvolver um projeto de proteção de dados parte da questão da proteção à privacidade.

A expressão *privacy by design*, nas palavras de Alves e Vainzof (2016):

> Foi cunhada na década 1990, por Ann Cavoukian, ex-comissária de Informação e Privacidade da Província de Ontário, no Canadá, correspondendo a uma forma de abordagem à proteção da privacidade, por meio da qual esta é incorporada diretamente às estruturas tecnológicas desenvolvidas, aos modelos de negócio e às infraestruturas físicas por eles utilizadas.

Como resultado do emprego do *privacy by design*, surge também o conceito de *privacy by default*, que, nas palavras de Maldonado e Blum (2019),

> Se refere à metodologia que adota por padrão a configuração de privacidade mais restritiva possível na fase da coleta de dados pessoais por qualquer sistema de tecnologia da informação, a fim de garantir a proteção dos dados pessoais de forma automática, ainda que nenhuma interação com a máquina tenha sido feita pelo usuário nesse sentido.

No ano de 2009, Ann Cavoukian publicou um artigo que se tornou um marco essencial a respeito do assunto, tendo consolidado na doutrina os seguintes princípios basilares do *privacy by design.* (MALDONADO; BLUM, 2019). Nas palavras de Dantas (2019, grifos do autor):

> **Proativo, não reativo; Prevenir, não remediar** – Por este princípio a privacy by design reconhece o valor de agir proativamente para antecipar, identificar e prevenir invasões antes que elas ocorram. O melhor é não esperar que riscos de privacidade cheguem a se materializar, e sim, evitar que eles aconteçam.
> **Privacidade por padrão** - O conceito de Privacy by Design também engloba o *Privacy by Default*, e isso permite que em um sistema que

> se guie por essas regras, mesmo que um usuário não faça nada, sua privacidade continue intacta. Dessa forma, não é necessário desativar a coleta de dados extras, já que ela deve vir desativada por padrão.
> **Privacidade embarcada no design** - A privacidade deve ser algo totalmente embutida no design, arquitetura de TI e práticas corporativas. Não é algo adicional ou complementar, mas faz parte integral de toda a estrutura do produto ou serviço. Sempre que possível, relatórios de prováveis impactos e riscos devem ser criados e publicados, claramente documentando os riscos de privacidade e todas as medidas tomadas para mitigá-los.
> **Total funcionalidade** – Ao implementar privacidade em um produto ou serviço, ela deve ser feita de forma a somar funcionalidades ao projeto, e não prejudicar nenhuma funcionalidade. As funcionalidades que conflites com princípios de privacidade devem ser modeladas de forma criativa para que possam funcionar juntos.
> **Segurança ponta**-a-ponta – A privacidade deve ser continuamente protegida através de todo o ciclo de vida dos dados em questão. A segurança dos dados deve estar em mente desde o planejamento até a execução, implantação e manutenção do projeto.
> **Visibilidade e Transparência** – A coleta, processamento e armazenamento de dados devem ser documentados de forma totalmente transparente, incluindo informações sobre a responsabilidade dos dados em caso de algum vazamento ou invasão.
> **Respeito pela privacidade do usuário** – Deve ser sempre respeitada a decisão e a proteção dos dados do usuário, já que os dados são de sua propriedade. É necessário que haja o consentimento no uso dos dados pessoais do usuário, com informações corretas e atualizadas conforme a necessidade. O usuário deve sempre ter acesso aos seus dados.

Os modelos do *privacy by design* e do *privacy by default* foram difundidos amplamente entre pesquisadores e autoridades nos anos que se sucederam, ganhando um reconhecimento internacional, visto que seus conceitos foram incorporados pelas legislações: em 1995, a Diretiva 95/46 da União Europeia sobre a proteção de dados pessoais considerou o assunto em sua Consideranda 46; em 2016, a GDPR menciona em seu Art. 25 e em sua Consideranda 78, os conceitos de privacy by design como pressupostos para a proteção de direitos e liberdades do indivíduo; ainda, em 2018 a Lei Geral de Proteção de dados positivou o *privacy by design* em seu Art. 46 e parágrafos. (MALDONADO; BLUM, 2019).

Com efeito, a atividade que deriva do conceito do *privacy by design* é uma perfeita conexão entre o direito e tecnologia, com a finalidade de implantar no desenho da arquitetura da rede aparatos técnicos que possam garantir os direitos de seus usuários, por padrão, em benefício da pessoa humana. Em assim considerado, o

espaço digital ganhará mais segurança, ética e saúde, consolidando uma cultura de proteção de dados. (MALDONADO; BLUM, 2019).

4.2 *Framework* como uma ferramenta que poderá conceder agilidade e flexibilidade à empresa no cumprimento do tratamento de dados pessoais

De acordo com o Guia de Boas Práticas (BRASIL, 2020), é imperioso ter e seguir uma lista de documentos para aprimorar a administração de riscos de segurança cibernética. Nesse sentido, o *Framework* é uma ferramenta eficaz no cumprimento do tratamento de dados pessoais com métodos e indicações para que sejam aplicados princípios e melhores práticas de gerenciamento de riscos que darão agilidade e segurança para as empresas se adequarem a LGPD.

O intuito de desenvolver um *Framework* é a resolução de problemas frequentes, tendo como escopo uma abordagem genérica, que permite ao seu desenvolvedor focalizar todos os esforços possíveis na resolução do problema em si. Desse modo, deixa-se de gastar um bom tempo hábil na reescrita de um novo *software.*

4.3 *Framework*: funcionalidade e estrutura

O *Framework* funciona como um armazenamento, semelhante a um aglomerado de bibliotecas ou de componentes, que tem a função de ser utilizado como base de dados, de onde surgirá a estrutura que possibilitará, no contexto dessa dissertação, dar maior visibilidade às exigências que a LGPD dispõe.

A estrutura do *Framework* deve ser o mais clara possível, identificando quais são os pontos principais da LGP, e suas implicações, exigências relacionadas à lei, bem como a explanação sobre a sua violação ou inobservância. Os *Frameworks* são ótimas ferramentas para o desenvolvimento rápido e seguro de aplicações. Conhecendo a fundo a sua tecnologia, é possível disponibilizar um material acessível e eficiente. Para compreender o espectro de um Framework, é necessário conhecer os aspectos básicos do Javascript. A partir do momento que se conhece a Tecnologia da *Framework*, é possível modificá-lo de acordo com seus objetivos, procurando atender às necessidades do desenvolvedor.

O *Framework* constitui, inicialmente, uma forma de argumentação.

Existem muitos *Frameworks* de argumentação diferentes. Para ilustrar, cita-se o *Framework* de John Latham (2014), que afirma ser toda a estrutura de um projeto, basicamente composto por dois grupos, chamados de “T” e “U”. O grupo “T” é composto por: problema, objetivo, questões de pesquisa e estrutura *Framework* “estrutura conceitual”. O grupo “U” é composto por: revisão bibliográfica (metodologia), coleta de dados, análise de dados e conclusões, e sugere a seguinte configuração que ilustra os conjuntos “T” (em azul) e “U” (em salmão):

Abaixo o modelo de John Latam como formato inicial do modelo que será apresentado:

Quadro 2 – *Framework* de John Latam (2014)

1. Problema 1. Identificar o problema; 2. Descrever os sintomas indesejáveis; 3. Identificar as faltas de conhecimento para resolução do problema; 4. Discussão sólida e revisada das informações com pares.	**2. Objetivo** O que? Descrever o novo conceito e os resultados pretendidos que irão preencher as faltas de conhecimento identificadas com o problema, o tipo de problema;	**3. Questões de Pesquisa** 1. Identificar os tipos de questões necessárias para responder ao problema proposto; 2. Desenvolver o corpo de questionamento principal e secundário de pesquisa; 3. Desenvolver as prováveis hipóteses aplicáveis ao caso.
9. Conclusões 1. Identificar a maior aplicação e significado encontrado; 2. identificar como a aplicação contribui para os gaps de conhecimento; 3. Identificar as limitções associadas com o resultado encontrado e suas conclusões.	**4. Estrutura Conceitual** 1. Identificar e diagramar as **variáveis chaves** das questões da pesquisa; 2. Identificar e diagramar as **principais relações** entre as variáveis; 3. Identificar e diagramar os principais **fatores de contexto**; 4. Descrever a estrutura.	**5. Revisão da Literatura** 1. Criar um esboço ou "mapa mental" de principais teorias e conceitos; 2. Mergulhar fundo na literatura "revisada" para cada teoria e conceito e criar um mapa bibliográfico e anotar a literatura; 3. Escrever a revisão da literatura;
8. Análise de dados 1. Com base nas questões da pesquisa, a abordagem geral e os dados coletados, identificar o métodos de análise de dados (ser específico); 2. Identificar os problemas e métodos de validação e confiabilidade para resolver os problemas;	**7. Coleta de dados** 1. Desenvolver um plano de medição para as variáveis na questão e nas hipóteses de pesquisa (pesquisa, entrevista guiada, etc.); 2. Desenvolver um plano de coleta de dados, incluindo estratégia de amostragem e processo de coleta de dados;	**6. Abordagem geral** 1. Identificar o "nível" de conhecimento empírico (revisão de literatura); 2. Identiricar o tipo de conhecimento necessário (declaração de propósito); 3. Identificar as opções e selecionar a abordagem baseada no "arco de pesquisa"; 4. Descrever a abordagem.

Adaptado de Lathan, J.R. (2014) *The Research Canvas* . A Framework for Desingning and Aligning the "DNA" of Your Study. Leadership Plus Design, Ltd.

Fonte: Adaptado de Latham (2014).

Cumpre ressaltar que o método de Latham (2014) insere-se como uma forma de solução de problemas mediante o estudo aprofundado do objeto-problema. Conforme se pode observar na metodologia, possui passos meticulosamente

elaborados em ordem lógica a fim de contribuir com a pesquisa e o aprofundamento do conhecimento com objetividade ao buscar respostas para os problemas propostos.

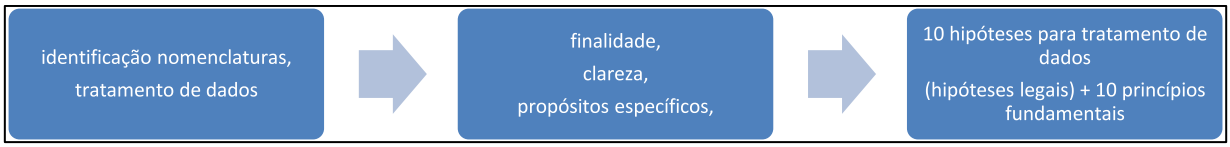
Da mesma forma, tal metodologia pode ser aplicada para o fundamento, embasamento e monitoramento contínuo da LGPD nas organizações. Trata-se, pois, do estudo do problema como a resposta aos imperativos legais da LGPD no tratamento de dados e a necessária economia de recursos humanos, financeiros e mesmo logísticos para o cumprimento da norma no tratamento de dados pessoais.

No capítulo a seguir, mostram-se os passos para o tratamento de dados pessoais, segundo a LGPD brasileira, com a apresentação de uma proposta de *Framework* primeiramente com o mesmo sentido do de Latham (2014) no que concerne à solução de problemas com base em um estudo meticuloso do objeto problema, no entanto, com passos baseados exclusivamente na própria LGPD para a implantação do chamado “Tratamento de dados pessoais”

4.3.1 Primeira parte do *Framework*

Como forma de elucidação, apresenta-se uma figura na qual essa questão relativa à primeira parte do *Framework* aparece esquematizada:

Figura 2 – Passos para o Tratamento dos Dados Pessoais



Fonte: Elaborado pela autora (2020).

Passos para o Tratamento dos Dados Pessoais:

a) Identificar se houve alguma das vinte nomenclaturas trazidas pela Lei como sendo “tratamento de dados” (acesso, armazenamento, arquivamento, avaliação, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração – modificação, processamento, produção, recepção, reprodução, transferência transmissão, utilização). (BRASIL, 2018);

b) O agente, antes mesmo de iniciar o tratamento, deve certificar-se de que a operação cumpre sua finalidade e que foi informado ao titular de dados de forma clara, explícita e para propósitos específicos. de acordo com o Guia de Boas Práticas – Lei Geral de proteção de Dados - LGPD. (BRASIL, 2020);

c) Conforme o Art. 7º da LGPD, devem ser observadas as dez hipóteses que permitem o tratamento de dados, *e* “[...] os requisitos para execução de tal procedimento. São as chamadas bases legais de tratamento de dados pessoais.” Esses critérios devem ser observados no tratamento de dados. (BRASIL, 2018).

Conjuntamente com o enquadramento em uma das hipóteses legais autorizativas para se iniciar o tratamento de dados pessoais, é imprescindível garantir que os dez princípios fundamentais listados no Art. 6º e a boa-fé sejam atendidos. (Guia De Boas Práticas - Lei Geral De Proteção De Dados). (BRASIL, 2020).

A LGPD estabelece também, em seu Art. 6º, que o tratamento de dados pessoais deve observar a boa-fé e dez princípios fundamentais específicos. São eles:

> Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> 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; 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; 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; 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; 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; Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e 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. (BRASIL, 2018)

De acordo com Pinheiro (2018b), o tratamento de dados é tido como sendo toda ação feita a partir do manejo de dados da pessoa natural que envolva a utilização, coleta, acesso, transmissão, produção, classificação, recepção, distribuição, armazenamento, avaliação, edição, difusão ou extração, transferência, reprodução,

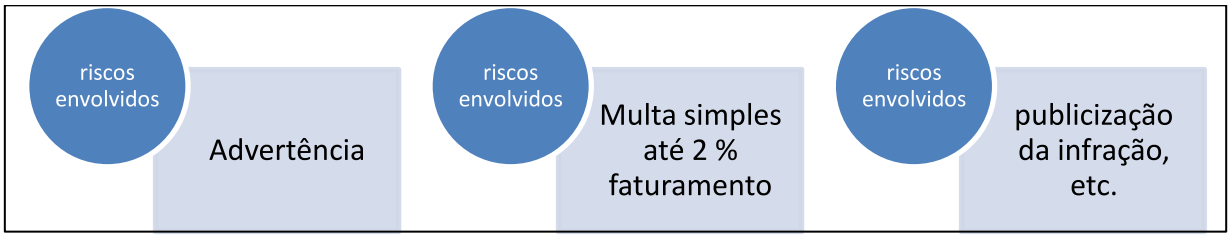
processamento, arquivamento, eliminação, controle da informação, modificação, comunicação.

Não basta, portanto, o enquadramento em uma das hipóteses legais autorizativas para se iniciar o tratamento de dados pessoais. É fundamental garantir que os princípios listados acima sejam respeitados.

4.3.2 Segunda parte do *Framework*

Como forma de elucidação, apresenta-se uma figura na qual essa questão relativa à segunda parte do *Framework* aparece esquematizada:

Figura 3 – Segunda parte do *Framework*



Fonte: Elaborado pela autora (2020).

Riscos envolvidos com a não adequação à LGPD: a não observância da LGPD acarretará sanções para a empresa, nos termos do Art. 52 da LGPD. Trata-se de sanções como: advertência, multa simples de até 2% do faturamento da empresa, publicização da infração, entre outras.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas[...] advertência, 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; multa diária, observado o limite total a que se refere o inciso II; publicização da infração ; bloqueio dos dados pessoais; eliminação dos dados pessoais; 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. (BRASIL, 2018).

Nas palavras de Pinheiro (2018b, p. 36), “[...] um programa de gestão de dados pessoais bem implementado pode ajudar na redução das penas, na hipótese de ocorrência de um tipo de infração que enseje a aplicação de alguma penalidade”.

De acordo com o Art. 46 da LGPD, é necessário identificar medidas de segurança, técnicas ou administrativas para tratar os riscos.

> 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. (BRASIL, 2018).

Uma empresa, para se adequar à LGPD, deve adotar boas práticas em segurança da informação com a observância da presença da privacidade desde a concepção e por padrão (*privacy by design e by default*). Isso é o que se encontra nos termos do §2º do Art. 46 da LGPD (BRASIL, 2018)

Conforme o Guia de Boas Práticas (BRASIL, 2020, p. 50),

> O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Tal privacidade pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais.

A Privacidade por Padrão (do inglês *Privacy by Default)* deve ser feita com observância ao princípio da necessidade, expresso pelo Art. 6º, inciso III da LGPD.

> 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. (BRASIL, 2018).

O conjunto dos elementos estruturantes examinados nesta Dissertação busca auxiliar o empresário a cumprir a LGPD, especialmente no tocante à proteção de dados. Trata-se de uma alternativa para aproximar a nova lei da realidade social na qual ela deverá ser implementada.

4.3.3 Terceira parte do *Framework*

A terceira parte deve falar sobre a mitigação de riscos dentro de uma empresa, a começar pela Segurança da Informação dentro da LGPD, e as implicações do Art. 6°, em conjunto com o Art. 44, 46 e 47 da LGPD, Lei n° 13.709. (BRASIL, 2018).

Os personagens trazidos pela Lei a quem competem as decisões referentes ao tratamento de dados pessoais são os chamados controladores e operadores, que podem ser pessoas físicas ou jurídicas, de direito público ou privado

De acordo com o Guia de Boas Práticas (BRASIL, 2020), no âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois “agentes de tratamento”, o Controlador e o Operador:

> O Controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.
> O Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere. (BRASIL, 2020, p. 32).

Aumenta a cada dia a preocupação com a chamada segurança da informação, principalmente após grandes vazamentos que temos acompanhado nos últimos anos. Para que fosse possível organizar a segurança de dados pessoais, a LGPD também legisla com o intuito de garantir que as empresas ajam de forma lícita e transparente.

Desse modo, o presente estudo traz, por meio do gráfico abaixo, a segurança da informação como pilar e fundamento para a não ocorrência dos Art.s 44, 46 e 47 da LGPD, os quais trazem a responsabilização dos agentes de tratamento. (BRASIL, 2018).

> Art. 44. O tratamento de dados pessoais **será irregular** quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, [...]Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no Art. 46 desta Lei, der causa ao dano.Art. 46. 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**. [...] Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação

> prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. (BRASIL, 2018, grifos nossos).

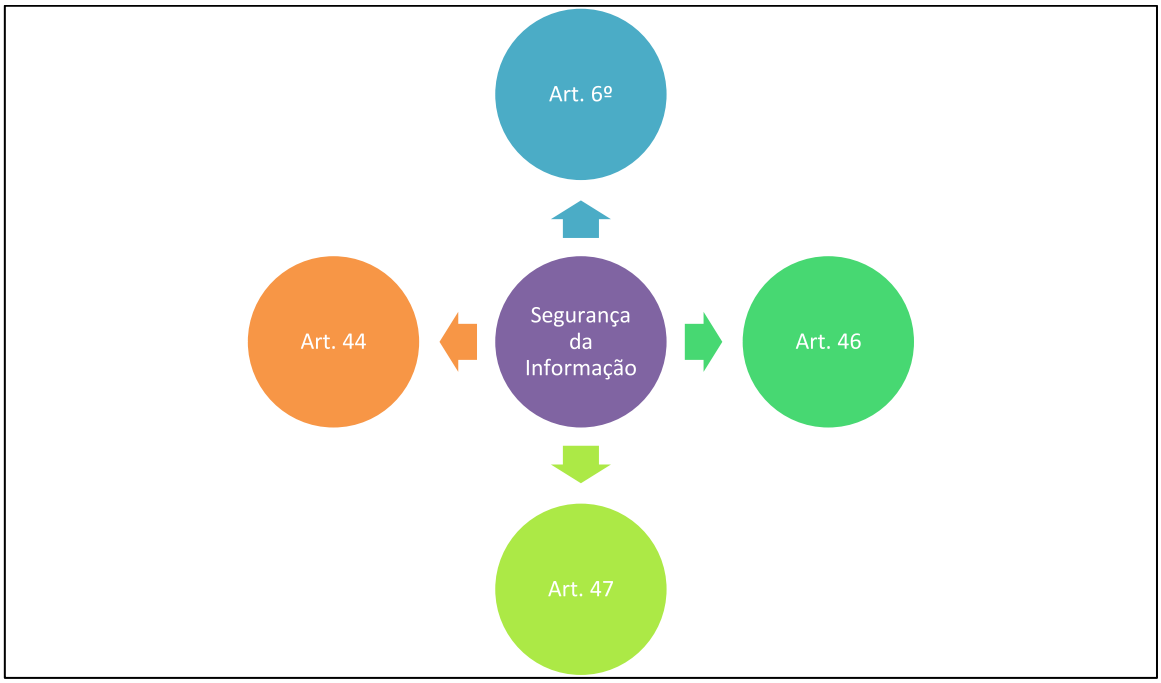
A empresa deve corrigir configurações incorretas, erros de tecnologia e de informações sobre privacidade de forma que sejam, efetiva e comprovadamente, diminuídos. Reza ainda o Guia de Boas Práticas (BRASIL, 2020, p. 47) que “Por isso, avaliações de impacto e risco na privacidade devem ser realizadas e publicadas, documentando claramente os riscos à privacidade e todas as medidas tomadas para mitigá-los”.

Na LGPD, a segurança é um princípio a ser observado no tratamento de dados pessoais, destacado pelo Art. 6º, inciso VII.

> [...]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; [...]. (BRASIL, 2018).

Na sequência, apresenta-se uma figura na qual essa questão relativa à segurança aparece esquematizada:

Figura 4 – Segurança da Informação



Fonte: Elaborado pela autora (2020).

De acordo com Nunes (2020), na “era da informação”, são crescentes os cuidados com segurança da informação, ainda mais após os vazamentos de dados de grande repercussão nos últimos tempos. Em resposta a essa tendência mundial de proteção de dados, estão sendo criadas leis que protejam a segurança dos dados de forma lícita, leal e transparente.

As reputações das empresas que não se adequarem à lei serão fortemente impactadas, pois empresas e usuários que preservam a privacidade de seus dados não terão interesse em parcerias com empresas que não tenham o mesmo nível de comprometimento, zelo e transparência. Assim, é imprescindível a implantação de procedimentos de controle de dados com atenção a LGPD e com a segurança da informação por meio de preceitos únicos e inequívocos para empresas e consumidores. Desse modo, no Brasil, foi criada a Lei Geral de Proteção de Dados (LGPD).

> Estar em conformidade com a LGPD é um desafio que envolve pessoas, processos e tecnologias. Portanto, implantar um projeto de adequação à lei e, mais do que isso, garantir a conformidade não é uma tarefa simples, mas para começar, podemos utilizar metodologias para servir de guia durante todo o processo até atingir maturidade no programa de governança em privacidade e proteção de dados. (NUNES, 2020).

De acordo com Nunes (2020), em uma visão técnica não jurídica, os passos para a implantação que as empresas devem seguir para implementar a segurança da informação, consistem em:

> **Preparação:** A preocupação nesta fase de preparação é em passar a ideia do impacto positivo que esta lei traz do ponto de vista organizacional e pessoal também. Para a conclusão buscamos executar as seguintes ações: Como gerenciar dados com segurança e eficiência com a vigência da lei de Cadastro Positivo Contextualizar colaboradores sobre a importância da adequação à LGPD; Definir um comitê de segurança da informação; Definir um escopo do projeto de conformidade; Planejar atividades do Mapeamento de Dados;
> Definir métricas de acompanhamento O comitê de Segurança da Informação se torna simples de ser construído quando os colaboradores compreendem a importância dessa lei. Este comitê é constituído de pelo menos uma pessoa de cada área da empresa e o objetivo é que estes possam trazer questionamentos de suas áreas e que sejam os que vão difundir a cultura de Segurança da Informação dentro da organização. Outro ponto importante é o planejamento das atividades para que seja possível identificar quais são as áreas que tratam dados pessoais e que representam um risco alto levando em

> consideração a LGPD. **Mapeamento:** Nesta etapa são realizados **os mapeamentos de dados**. Para cada contexto deverá ser criado um fluxo demonstrando todo o ciclo de vida do dado. Para a conclusão desta etapa é necessário executar as seguintes ações: Elaborar um mapa de dados para compreender o ciclo de vida do dado dentro da organização Realizar entrevistas com as áreas para preenchimento do mapa de dados Mapear os processos, políticas internas, tecnologias utilizadas, parceiros e terceiros os colaboradores escolhidos deverão ser estratégicos do ponto de vista de conhecimento sobre a sua área de atuação, acesso aos dados e processos internos, para que a atividade de mapeamento seja efetiva. **Avaliação:** Nessa etapa, é realizada a avaliação dos resultados obtidos através das entrevistas. Além disso é realizada a avaliação de risco para apoiar a definição das prioridades dentro do plano de ação. Para a conclusão desta etapa é necessário executar as seguintes ações: Avaliar o mapa dos dados com base nos requisitos da LGPD (GAP Analysis) Elaborar um relatório de Avaliação de impacto de proteção de dados (DPIA) Realizar a avaliação de riscoCom base no Gap Analysis é possível realizar o planejamento considerando o risco de cada área e de cada processo de tratamento de dados e dessa forma priorizar as ações com maior assertividade. **Planejamento:** Nesta etapa será realizado o plano de ação, de acordo com a avaliação de risco definida na fase de Avaliação. Para a conclusão desta etapa é necessário executar as seguintes ações: Elaborar um plano de ação Definir ações que devem ser realizadas com base no que foi levantado no GAP Analysis Elaborar cronograma de implementação **Execução:** Nesta etapa será realizada a implementação de guias de procedimentos, melhoria ou criação de processos, incluindo, a definição da estratégia de governança de dados, implementação de controles de segurança da informação, revisão de contratos, e gestão de políticas internas. Todas essas ações devem estar documentadas no programa de governança de privacidade e proteção de dados. Este é um documento vivo que deve ser atualizado constantemente. Para a conclusão desta etapa é necessário executar as seguintes ações: Executar as atividades do plano de ação. Atualizar a documentação do programa de governança de privacidade e proteção de dados. **Monitoramento:** Esta etapa consiste em garantir que a organização está mantendo a conformidade com a lei geral de proteção de dados. Para a conclusão desta etapa é necessário executar as seguintes ações: Realizar auditorias periódicas para garantir que a organização está mantendo a conformidade.Garantir o andamento de um programa de conscientização e treinamentos recorrentes. (NUNES, 2020).

Esses são alguns passos que a autora propõe a fim de que seja possível a implantação de um projeto de governança em privacidade e proteção de dados para adequação à LGPD.

Sobre o assunto, Pinheiro (2019) leciona:

> Pinheiro: Para atingir níveis satisfatórios e adequados as normas, é necessário cumprir uma jornada do *compliance* em Privacidade e

> Proteção de Dados e investir em três pilares: soluções tecnológicas, revisão de contratos e procedimentos e capacitação da equipe.

O Art. 50 da LGPD traz formas de mitigação de riscos para conscientização das empresas:

> 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular **regras de boas práticas e de governança** que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.[...]. (BRASIL, 2018, grifo nosso).

O Art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco".

> **Mitigação dos riscos**. O **Relatório de Impacto à Proteção dos Dados Pessoais (RIPD)** representa documento fundamental a fim de demonstrar os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para **mitigação dos riscos** que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados. (BRASIL, 2018, grifos nossos).

Diante de tudo isso, cumpre esclarecer que o *Framework* é apenas uma das inúmeras ferramentas de resolução de problemas cotidianos, tendo como escopo uma abordagem padrão, que tem a função de ser utilizado como base de dados, de onde surgirá a estrutura que possibilitará dar maior visibilidade às exigências da LGPD de forma clara e mais didática possível, trazendo os pontos principais da Lei bem como suas implicações, exigências e causas sobre a não observância da mesma. Além do *Framework* ,a empresa deve desenvolver outras formas de adequação, como a conscientização de toda a equipe de trabalho sobre a importância da LGPD, oferecendo um treinamento eficiente e minucioso ao grupo sobre os ditames da Lei. Além disso, preventivamente, deve definir os chamados agentes de tratamento de dados, sejam terceirizados ou não. Também é imperativo adequar seus contratos e políticas de privacidade, criando documentos capazes de atender às especificações da LGPD. Poderão, ainda, formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os

procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Tudo isso deve estar em consonância com os termos do Art. 50º da LGPD. Por derradeiro, apresenta-se uma proposta de *Framework* onde todo o exposto está esquematizado:

Figura 5 – *Framework*

Fonte: Elaborado pela autora (2020).

O *Framework* cobre os requisitos e artigos da LGPD e deve ser aplicado aliando as boas práticas de governança e segurança da informação. Salienta-se que, para implantação, os profissionais devem aproveitar as práticas de governança já existentes e utilizadas na empresa para melhores resultados.

Portanto, ao se tratar dados pessoais, “[...] em um ambiente competitivo como o que vivemos, todos os agentes econômicos passaram a agir da mesma forma, aumentando exponencialmente o volume de dados que passaram a ser disponibilizados na rede”. (COLOMBO, FACCHINI NETO, 2017, p. 61) as empresas devem fornecer uma governança abrangente para garantir conformidade com os requisitos da LGPD. Os processos de governança devem possibilitar a todos os envolvidos (funcionários, internos e externos) a contar em um conjunto definido de princípios, políticas e procedimentos que definem claramente e explicam como os dados pessoais podem ser processados e tratados. Empresas renomadas, como Google e Facebook, oferecem entretenimento e serviços de forma gratuita no intuito de capturar dados, mais parecendo “mercadores da atenção”. Pois os dados podem ser a chave para controlar a vida no futuro. (HARRARI; 2018, p. 107).

Como bem pontuam Boff, Fortes e Freitas (2018, p. 120):

> A maior parte dos motores de busca, como o Google, foram desenvolvidos para trabalhar em simbiose com os usuários, ou seja, em troca de serviços gratuitos, o usuário fornece seus dados pessoais e consente, ao iniciar o uso dos serviços, que suas informações pessoais de navegação sejam coletadas, armazenadas e utilizadas para diversos fins, inclusive comerciais.

Ocorre que tudo isso é feito em nosso dia a dia sem ao menos perceber. Nessa rotina, diversos são os dados pessoais lançados por meio de aceite que tão rapidamente concedemos nos termos de uso e condições de aplicativos, visitação em sites. Vista essa exposição e até vulnerabilidade desse meio digital, é necessária a existência de mecanismos de controle, principalmente para o mercado empresarial no que concerne a uma provável perda de reputação caso a privacidade e proteção de dados pessoais não seja garantida. O uso do banco de dados vai precisar seguir as novas regras, e as empresas terão que responder de maneira imediata, simples e eficiente a demandas geradas pelos novos direitos do titular de dados, como de confirmação do tratamento de dados, cancelamento do tratamento, exclusão ou retificação dos seus dados.

Portanto, para a elaboração da pesquisa, empregou-se a pesquisa bibliográfica por meio de acesso a bases de dados, como o portal de periódicos da CAPES, a pesquisa documental. Além disso, examinaram-se fontes em outras áreas do saber para a construção do *Framework*. Elaborou-se um *Framework* a começar por algumas ideias baseadas na perspectiva do *Framework* de Jonh R. Latham (2014).

Como término da pesquisa, concluiu-se que o *Framework* é uma forma eficaz de adequação à LGPD, pois aplica com um passo a passo e atende aos princípios indispensáveis para o tratamento de dados pessoais, sugerindo propostas confiáveis, com as etapas essenciais que as empresas deverão observar e como ponto inicial para cumprir a LGPD relativo aos dados pessoais. Além disso, configura-se como forma de mitigar os riscos aos quais os agentes estão expostos, sendo, assim, uma alternativa de adequação à LGPD.

5 CONSIDERAÇÕES FINAIS

Esta dissertação ocupou-se do impacto da LGPD na proteção de dados e da privacidade dos dados pessoais no cenário empresarial e definiu procedimentos e práticas para o tratamento de dados. Além disso, propôs formas de mitigação de riscos e apresentou os impactos com a não adequação empresarial aos ditames da Lei.

Da mesma forma, notou-se que o legislador, ao elaborar a Lei Geral de Proteção de Dados Pessoais, objetivou abordar os direitos fundamentais ligados ao conceito de dignidade da pessoa humana e à sua personalidade, assim pretendendo objetivar a efetivação da lei dentro dos moldes da sua precursora GDPR.

O Cerne do presente estudo foi a análise o conteúdo do Capítulo II, que aborda o tratamento de dados pessoais, Seção I, que estipula os requisitos para o tratamento de dados pessoais, da LGPD, Art.s 7º ao 10º.

Grandes empresas, após permitirem o vazamento de dados pessoais, tiveram que pagar multas milionárias e precisaram adequar-se ao GDPR para permanecerem atuando na Europa. No Brasil, foi criada a LGPD como resposta à Lei Europeia. Ocorre, no entanto, que a entrada em vigor da presente lei precisou ser adiada por diversas vezes tendo em vista o então curto prazo para as mesmas se adequarem à Lei, conjuntamente com os problemas de saúde que assolam não só o Brasil como o mundo.

Considerando esse cenário, o presente estudo constatou que a adequação das empresas à LGPD é medida que se impõe. Para isso, é imprescindível a implantação de medidas de segurança, por parte das empresas, já desde o início do tratamento de dados, com a aplicação de um *compliance* que vise ao atendimento das exigências da Lei. Para melhor estruturação empresarial, foi apresentada como solução a adequação a um *Framework,* viabilizando a adaptação das empresas brasileiras à LGPD, com um passo a passo a ser aplicado à implementação do chamado tratamento de dados pessoais, como alternativa na adequação das empresas e forma de mitigar os riscos que os agentes estão expostos.

O *Framework* apresentado atende e prevê cada uma dessas formas de tratamento dos dados, bem como do respectivo cuidado com cada forma, que envolve os requisitos descritos no capítulo II, seção I da LGPD, que dispõe dos requisitos para o Tratamento de Dados Pessoais conforme a mesma lei. O *Framework* proporcionou o atendimento de princípios, como: a transparência, e trouxe propostas confiáveis

como o *compliance* de cada uma das etapas de tratamento dos dados, a fim de dar conta do direito à explicação de alguma parte que tenha permitido o acesso aos seus dados pessoais.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27001:** Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2006. Disponível em: https://www.academia.edu/36980100/ABNT_NBR_ISO_IEC_27001_Tecnologia_da_informa%C3%A7%C3%A3o_T%C3%A9cnicas_de_seguran%C3%A7a_Sistemas_de_gest%C3%A3o_de_seguran%C3%A7a_da_informa%C3%A7%C3%A3o_Requisitos. Acesso em: 19 ago. 2020.

ALVES, Fabrício da Mota. A importância da PEC de proteção de dados mesmo após o histórico julgamento do STF**.** *In:* Jota Info. [São Paulo], 06 jun. 2020. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/a-importancia-da-pec-de-protecao-de-dados-mesmo-apos-o-historico-julgamento-do-stf-16062020. Acesso em: 18 ago. 2020.

ALVES, Carla Segala; VAINZOF, Rony. Privacy by Design e Proteção de Dados Pessoais não expressamente previstos na lei brasileira, princípios da privacy by design estão de acordo com Marco Civil da *Internet*. *In:* Jota Info. [São Paulo, 06 jul. 2016. Disponível em https://www.jota.info/opiniao-e-analise/artigos/direito-digital-privacy-design-e-protecao-de-dados-pessoais-06072016. Acesso em: 05 ago. 2020.

ARAÚJO, Bernardo. Redes Sociais como canais de distribuição de conteúdo. *In:* Jota Info. [São Paulo], 06 ago. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/redes-sociais-conteudo-informacional-06082018. Acesso em: 27 jan. 2020.

ARPANET. *In:* IME: Instituto de Matemática e Estatística. [São Paulo: Universidade de São Paulo], 16 jul. 1997. Disponível em: https://www.ime.usp.br/~is/abc/abc/node20.html. Acesso em: 25 jan. 2021.

BAIÃO, Kelly; GONÇALVES, Kalline. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **civilistica.com**, Rio de Janeiro, v. 3, n. 2, p. 1-24, dez. 2014.

BARBOSA, Adriana Silva *et al.*. Relações humanas e privacidade na internet: implicações Bioéticas. **Rev. Bioética y Derecho,** Barcelona, n. 30, p. 109-124, 2014. Disponível em: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872014000100008&lng=es&nrm=iso. Acesso em: 11 nov. 2019.

BARROSO, Luis Roberto. Colisão entre liberdade de expressão e direitos da personalidade. Critérios de ponderação. Interpretação constitucionalmente adequada do Código Civil e da Lei de Imprensa. **Revista Trimestral de Direito Civil,** Rio de Janeiro, v. 16, p. 59-102, 2004.

BAUMAN, Zygmunt. **Vigilância Líquida.** Rio de Janeiro: Zahar, 2014.

BEALES III, J. Howard; MURIS, Timothy J. Privacy and Consumer Control. **The Aspen Institute**: Congressional Program. Cambridge, Massachusetts: The Aspen

Institute, 2019, p. 37-42. Disponível em: https://assets.aspeninstitute.org/content/uploads/2019/06/MIT-Conference-Report.pdf. Acesso em: 02 ago. 2020.

BIONI, Bruno Ricardo. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados pessoais. *In:* Jota Info. [São Paulo], 02 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-daprivacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geralde-protecao-de-dados-02072018. Acesso em: 30 abr. 2020.

BIONI, Bruno. Bolsonaro edita MP e adia entrada em vigor da lei de dados para maio de 2021. *In:* Bioni. [S.l], 29 abr. 2020. Disponível em: https://brunobioni.com.br/blog/namidia/bolsonaro-edita-mp-e-adia-entrada-em-vigor-da-lei-de-dados-para-maio-de-2021/. Acesso em: 20 ago. 2020.

BITTAR, Carlos Alberto. **Os direitos da personalidade.** 7. ed. Rio de Janeiro: Forense, 2008.

BLUM, Opice Academy. **Direito digital e LGPD**. Perdizes, SP: Instituto de Direito Contemporâneo, 2020. E-Book. Disponível em http://www.famescbji.edu.br/famescbji/biblioteca/biblioteca/ebooks/Ebook-Direito%20Digital%20e%20LGPD.pdf. Acesso em: 18 ago. 2020.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e à proteção dos dados do consumidor**. São Paulo: Almedina, 2018.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRANDÃO, Graziela. O que é mapeamento de dados? *In:* BL Consultoria.[São Paulo], 27 fev. 2020. Disponível em: https://blconsultoriadigital.com.br/mapeamento-de-dados/. Acesso em: 30 mar. 2020.

BRASIL. [Constituição (1824)]. **Constituição Política do Império do Brazil, de 25 de março de 1824.** Rio Janeiro, RJ: Império do Brazil, 1824. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao24.htm. Acesso em: 20 ago. 2020.

BRASIL. [Constituição (1891)]. **Constituição Política da República do Brasil, de 24 de fevereiro de 1891.** Rio de Janeiro, RJ: Presidência da República, 1891. Disponível em: www.planalto.gov.br/ccivil_03/constituicao/Constituicao91.htm. Acesso em: 20 ago de 2020.

BRASIL. [Constituição (1934)]. **Constituição da República dos Estados Unidos do Brasil, de 16 de julho de 1934.** Rio de Janeiro, RJ: Presidência da República, 1934. Disponível em: www.planalto.gov.br/ccivil_03/constituicao/Constituicao34.htm. Acesso em: 20 ago de 2020.

BRASIL. [Constituição (1937)]. **Constituição dos Estados Unidos do Brasil, de 10 de novembro de 1937.** Rio de Janeiro, RJ: Presidência da República, 1937. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao37.htm. Acesso em: 20 ago. 2020.

BRASIL. [Constituição (1946)]. **Constituição dos Estados Unidos do Brasil, de 18 de setembro de 1946**. Rio de Janeiro. RJ: Presidência da República, 1946. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao46.htm. Acesso em: 20 ago. 2020.

BRASIL. [Constituição (1967)]. **Constituição da República Federativa do Brasil de 1967**. Rio de Janeiro. RJ: Presidência da República, 1967. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao67.htm. Acesso em: 20 ago. 2020.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em:<http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>.Acesso em: 27 maio 2020.

BRASIL. **Decreto nº 678, de 06 de Novembro de 1992**. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São Jose da Costa Rica), de 22 de novembro de 1969. Brasília, DF: Presidência da República, 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 2 ago. 2020.

BRASIL. **Decreto nº 7.962, de 15 de março de 2013.** Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm Acesso em: 19 ago. 2020.

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016.** Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na *Internet* e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm. Acesso em: 19 ago. 2020.

BRASIL. **Lei nº 8.078 de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 18 ago. 2020.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/ Leis/2002/L10406.htm. Acesso em: 20 ago. 2020.

BRASIL. **Lei nº 12.414 de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm Acesso em: 19 ago. 2020.

BRASIL. **Lei nº 12.527 de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do Art. 5º , no inciso II do § 3º do Art. 37 e no § 2º do Art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 19 ago. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, direitos e deveres para o uso da *Internet* no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www. planalto. gov. br/ccivil_03/_ato2011-2014/2014/lei/l12965.html. Acesso em: 03 maio 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção a Dados Pessoais. Brasília, DF: Presidência da República, 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 11 abr. 2020.

BRASIL. **Lei nº 13.853, de 08 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm#:~:text=LEI%20N%C2%BA%2013.853%2C%20DE%208%20DE%20JULHO%20DE%202019&text=Altera%20a%20Lei%20n%C2%BA%2013.709,Art. Acesso em: 19/08/2020.

BRASIL. **Medida provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Mpv/mpv869.htm. Acesso em: 19 ago. 2020.

BRASIL. **Medida provisória 959, de 29 de abril de 2020**. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 19 ago. 2020.

BRASIL. **Projeto de Lei nº 1.179/2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do Coronavírus (Covid-19). Brasília, DF: Senado Federal, 2020. Disponível em: https://legis.senado.leg.br/sdleggetter/documento?dm=8081779&ts=1597151891776&disposition=inline. Acesso em: 19 ago. 2020.

BRASIL. Comitê Central de Governança de Dados. **Guia de boas práticas:** Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Comitê Central de Governança de Dados, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Acesso em: 03 jul. 2020.

BRASIL. Controladoria Geral da União**. Portaria conjunta nº 2.279, de 9 de setembro de 2015**. Dispõe sobre a avaliação de programas de integridade de microempresa e de empresa de pequeno porte. Brasília, DF: Presidência da República, 2015. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/09/2015&jornal=1&pagina=2&totalArquivos=80. Acesso em: 20. ago. 2020.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso especial 1.758.799/MG.** Cuida-se de recurso especial interposto por PROCOB S/A, fundado nas alíneas “a” e “c” do permissivo constitucional, contra acórdão do TJ/MG. Recorrido: José Galvão da Silva. Relatora: Ministra Nancy Andrighi, 12 de novembro de 2019. Disponível em: https://www.conjur.com.br/dl/ausencia-comunicacao-comercializacao.pdf. Acesso em: 20 ago. 2020.

BUENO, Silveira. **Mini dicionário da Língua Portuguesa.** São Paulo: FDT, [s.a].

CALDAS, Gabriela. O direito à explicação no Regulamento Geral sobre a Proteção de Dados. *In*: COUTINHO, Francisco Pereira; MONIZ, Graça Canto (coord.). **Anuário de proteção de dados.** Lisboa: Universidade Nova de Lisboa, 2019. p. 37-54. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf. Acesso em: 01 ago. 2020.

CALDAS, Pedro Frederico. **Vida privada, liberdade de imprensa e dano moral.** São Paulo: Saraiva, 1997.

CANOTILHO, J.J Gomes *et. al*. **Comentários à Constituição do Brasil.** São Paulo: Saraiva/Almeida, 2013.

CANTALI, Fernanda Borghetti. **Direitos da personalidade**: Disponibilidade relativa, autonomia privada e dignidade humana. Porto Alegre: Livraria do Advogado Editora, 2009.

CAPRA, Caroline. Como a LGPD influencia as práticas de compliane? *In:* Migalhas. [S.l], 16 maio 2019. Disponível em https://www.migalhas.com.br/depeso/302395/como-a-lgpd-influenciaaspraticasdecompliance#:~:text=No%20mundo%20corporativo%2C%20estar%20de,das%20boas%20pr%C3%A1ticas%20de%20Compliance.>. Acesso em: 05 ago. 2020.

CARTAXO, Maria Maximina. **Impactos da LGPD em Due Diligence de terceiros**. *In:* LEC. [S.l], 12 nov. 2018. Disponível em: <http://www.lecnews.com.br/blog/impactos-da-lgpd-em-due-diligence-de-terceiros/>. Acesso em: 13 mar. 2020.

CASTELLS, Manuel. **A sociedade em rede.** Tradução de Roneide Venâncio Majer. 19. ed. Rio de Janeiro/São Paulo: Paz e Terra, 2018.

CASTELLS, Manuel. **A era da informação:** Economia, Sociedade e Cultura. Vol. 1. São Paulo, Ed. Paz e Terra, 1999.

CASTRO, Patricia Reis; AMARAL, Juliana Ventura; GUERREIRO, Reinaldo. Aderência ao programa de integridade da lei anticorrupção brasileira e implantação de controles internos. **Revista Contábil Financeira**, São Paulo , v. 30, n. 80, p. 186-201, Ago. 2019. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1519707720190002001 86&lng=en&nrm=iso. Acesso em: 11 abr. 2020.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil.** 8. ed. São Paulo: Atlas, 2008.

CHAVES, Christian Frau Obrador. A luta contra o terrorismo e a proteção de dados pessoais. **Revista Brasileira de Direitos Fundamentais & Justiça**, Porto Alegre, v. 4, n. 12, p. 284-293, jul./set. 2010. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/420/357. Acesso em: 27 maio 2020.

COELHO, Gabriela. MP-DF acusa empresa pública de vender dados pessoais de brasileiros. *In:* Consultor Jurídico. [S.l], 31 maio 2018. Disponível em: https://www.conjur.com.br/2018-mai-31/mp-df-acusa-empresa-publica-vender-dados-brasileiros. Acesso em: 03 maio 2020.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Violação dos Direitos de personalidade no meio ambiente digital: a influência da jurisprudência europeia na fixação da jurisdição/competência dos tribunais brasileiros. **civilistica.com**, Rio de Janeiro, v. 8, n. 1, p. 1-25, abr. 2019.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Mineração de Dados e análise preditiva: Reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para sua adequada implementação à luz do ordenamento brasileiro. **Revista de Direito, Governança e Novas Tecnologias,** São Luís, v. 3, n. 2, p. 59-80, jul./dez.2017.

COMISSÃO EUROPEIA. **Ec.europa.eu**, 2018. Disponível em https://ec.europa.eu/commission/priorities/justiceandfundamentalrights/dataprotection/2018-reform-eu-data-protection-rules_en. Acesso em 11/04/2020.

CONSELHO DA EUROPA. **Convenção europeia dos direitos do homem:** Roma, 4.11.1950. Strasbourg: Tribunal Europeu dos Direitos do Homem, [2013]. Disponível

em: http://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 19 ago. 2020. Esta tradução não é uma versão oficial da Convenção.

COSTA JUNIOR, Paulo José da. **O direito de estar só:** tutela penal da intimidade. São Paulo: RT, 1995.

COURA, Kalleo. Liberdade de Expressão: Mercadores da Mentira. *In:* Jota Info. [São Paulo], 23 jan. 2017. Disponível em: https://www.jota.info/especiais/mercadores-da-mentira-23012017. Acesso em: 23 jan. 2020.

DANTAS, Henrique. LGPD. **O que Privacy by design e Privacy by Default.** *In:* Advogatech. [S.l], 15 jun. 2019. Disponível em: https://www.advogatech.com.br/blog/@HenriqueDantas/lgpd-o-que-e-privacy-by-design-e-privacy-by-default-vc4zyjv. Acesso em: 05 ago. 2020.

DATA protection. **ECEuropa**. 2020. Disponível em:<https://ec.europa.eu/info/law/law-topic/data-protection_en.> Acesso em: 03/05/2020.

DECLARAÇÃO dos Direitos do Homem e do Cidadão. *In:* **Textos Básicos sobre Derechos Humanos**. Tradução de Marcus Claudio Acqua Viva. Madrid: Universidad Complutense, 1973. Disponível em: http://www.direitoshumanos.usp.br/index.php/Documentos-anteriores-%C3%A0-cria%C3%A7%C3%A3o-da-Sociedade-das-Na%C3%A7%C3%B5es-at%C3%A9-1919/declaracao-de-direitos-do-homem-e-do-cidadao-1789.html. Acesso em: 07 jul. 2020.

DI FIORE, Bruno Henrique. Teoria dos círculos concêntricos da vida privada e suas repercussões na praxe jurídica. *In:* Flávio Tartuce. [S.l], 2012. Disponível em: http://www.flaviotartuce.adv.br/assets/uploads/artigosc/201109281258590.Artigo_brunofiore.doc#:~:text=TEORIA%20DOS%20C%C3%8DRCULOS%20CONC%C3%8ANTRICOS%20DA%20VIDA%20PRIVADA%20E%20SUAS%20REPERCUSS%C3%95ES%20NA%20PRAXE%20JUR%C3%8DDICA&text=Bacharel%20em%20Direito%20pela%20Universidade,prote%C3%A7%C3%A3o%20aos%20direitos%20da%20personalidade. Acesso em: 18 abr. 2020.

DIAS, Felipe da Veiga; REIS, Jorge Renato dos. As liberdades comunicativas e a efetivação dos direitos humanos e fundamentais no Estado Democrático de Direito. *In*: REIS, Jorge Renato dos; LEAL, Rogério Gesta; COSTA, Marli Marlene Moraes da; LEAL, Mônia Clarissa Hennig. (Org.). **As políticas públicas no constitucionalismo contemporâneo.** Tomo 3. Santa Cruz do Sul: EDUNISC, 2011, v. 3, p. 509-523.

DIREITO à intimidade e sua proteção baseada nos direitos humanos no mundo. *In*: ÂMBITO jurídico. Rio Grande, 1 jun. 2014. Disponível em: https://ambitojuridico.com.br/cadernos/direito-constitucional/direito-a-intimidade-e-sua-protecao-baseada-nos-direitos-humanos-no-mundo/. Acesso em: 20 ago. 2020.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo:** para além das relações creditícias. Brasília: SDE/DPDC, 2010. Disponível em

https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf> Acesso em: 14 ago. 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. A Proteção da Privacidade e de Dados Pessoais no Brasil. **Revista Observatório Itaú Cultural,** São Paulo, nº 16, jan./jun. 2014. Disponível em: http://d3nv1jy4u7zmsc.cloudfront.net/wp-content/uploads/2014/06/OBSERVATORIO16_0.pdf. Acesso em: 26 mar. 2020.

DONEDA, Danilo. A Proteção de Dados Pessoais Como um Direito Fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

ENGELMANN, Wilson. **Crítica ao Positivismo Jurídico:** Princípios, Regras e o Conceito de Direito. Porto Alegre: Ed. Sérgio Antônio Fabris, 2001.

ESPANHA. Tribunal de Justiça (Grande Sessão). **Acordão C-131/12**. 1 O pedido de decisão prejudicial tem por objeto a interpretação dos artigos 2.°, alíneas b) e d), 4.°, n.° 1, alíneas a) e c), 12.°, alínea b), e 14.°, primeiro parágrafo, alínea a), da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281, p. 31), bem como do artigo 8.° da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»). 2 Este pedido foi apresentado no âmbito de um litígio que opõe a Google Spain SL (a seguir «Google Spain») e a Google Inc. à Agencia Española de Protección de Datos (Agência Espanhola de Proteção de Dados, a seguir «AEPD») e a M. Costeja González, a propósito de uma decisão desta Agência, que deferiu a reclamação apresentada por M. Costeja González contra estas duas sociedades e ordenou à Google Inc. a adoção das medidas necessárias para retirar os dados pessoais respeitantes a M. Costeja González do seu índice e impossibilitar o futuro acesso aos mesmos. Recorrido: Google Spain SL, Google Inc. Relator: V. Skouris, 13 de maio de 2014. Disponível em: https://migalhas.uol.com.br/arquivos/2014/5/art20140514-04.pdf. Acesso em: 27 out. 2020.

EUR-LAX. **DIRECTIVA 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995**, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 1995. Disponível em: https://eurlex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EN. Acesso em: 19 ago. 2020.

EURO-LEX. **Acess to european union**. 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L0680. Acesso em: 02 maio 2020.

FERNANDEZ JUNIOR, Enio Duarte. Brevíssimo aporte sobre o direito fundamental à privacidade e à intimidade na perspectiva do direito brasileiro sobre a proteção de dados pessoais. *In*: ÂMBITO jurídico. Rio Grande, 1 fev. 2014. Disponível em:

https://ambitojuridico.com.br/cadernos/direito-civil/brevissimo-aporte-sobre-o-direito-fundamental-a-privacidade-e-a-intimidade-na-perspectiva-do-direito-brasileiro-sobre-a-protecao-de-dados-pessoais/. Acesso em: 20 ago. 2020.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito:** Universidade de São Paulo, São Paulo, v. 88, p. 439-459, 1993.

FICO, Bernardo de Souza Dantas; MOTA, Juliana da Cunha. A proteção de dados como direito humano. *In:* Jota Info. [São Paulo], 29 fev. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-como-direito-humano-29022020. Acesso em: 11 ago. 2020.

FRAZÃO, Ana. Big Data e impactos sobre a análise concorrencial: Direito da Concorrência é um dos mais afetadas pela importância dos dados – Parte 1. *In:* Jota Info. [São Paulo], 28 nov. 2017. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiioeanalise/coltuicaoempresaemercado/bigdataeimpactossobreaanaliseconcorrencial-28112017. Acesso em: 11 ago. 2020.

FRAZÃO. Ana. Nova LGPD: a importância do consentimento para o tratamento dos dados pessoais. *In:* Jota Info. [São Paulo], 19 ago. 2018. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-a-importancia-do-consentimento-para-o-tratamento-dos-dados-pessoais-12092018. Acesso em: 11 ago. 2020.

FREGADOLLI, Luciana. **O direito à intimidade e a prova ilícita.** Belo Horizonte: Del Rey, 1998.

FROSINI, Vittorio. **Contributi ad un diritto dell'informazione.** Napoli: Liguori, 1991.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro:** Parte geral. 9. ed. São Paulo: Editora Saraiva, 2011.

GONZÁLEZ, Mariana. LGPD Comentada. 2019. *In:* GuiaLGPD. [S.l], 20 dez. 2019. Disponível em: https://guialgpd.com.br/lgpdcomentada/#:~:text=Artigo%209,tratamentos%20de%20seus%20dados%20pessoais. Acesso em: 18 ago. 2020.

GUERRA, Sidney Cesar Silva. **A liberdade de imprensa e o direito à imagem**. 2. ed. Rio de Janeiro: Renovar, 2004.

HARARI, Yuval Noah**. 21 lições para o século 21.** Tradução Paulo Geiger. São Paulo: Companhia das Letras, 2018.

HENRIQUES, Sérgio Coimbra; LUÍS, João Vares. Consentimento e outros fundamentos de licitude para o tratamento de dados pessoais em contexto laboral. *In*: COUTINHO, Francisco Pereira; MONIZ, Graça Canto (coord.). **Anuário de proteção de dados.** Lisboa: Universidade Nova de Lisboa, 2019. p. 13-36.

Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf. Acesso em: 01 ago. 2020.

HOCH. Patrícia Adriani. **Levando a intimidade a sério na Internet:** Reflexões acerca do impacto das novas tecnologias e do Marco Civil da *Internet* nas decisões do STF e do STJ. Porto Alegre, RS: Editora Fi, 2019.

IGLESIAS, Sérgio. **Responsabilidade civil por danos à personalidade.** Barueri: Manole, 2002.

ILARRAZ. Disponível em: https://ilarraz.com.br/. Acesso em: 24 ago. 2020.

IPLD. **Instituto dos profissionais de prevenção à lavagem de dinheiro e ao financiamento do terrorismo**. 2019. Disponível em: https://ipld.com.br/editorial/lei-geral-de-protecao-de-dados-sua-empresa-ja-esta-se-adequando. Acesso em: 11 abr 2020.

JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**. Porto Alegre: RT, 2000.

KOCH, Richie. LGPD: a versão brasileira do regulamento europeu. *In:* SERPRO, [Brasília], 12 set. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dadospessoais#:~:text=A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o,classifica%C3%A7%C3%A3o%20ao%20arcabou%C3%A7o%20legal%20brasileiro.&text=E%20se%20voc%C3%AA%20j%C3%A1%20est%C3%A1,em%20conformidade%20com%20a%20LGPD. Acesso em: 19 ago. 2020.

LATHAM, John R., The Research Canvas. **A Framework for designing and aligning the "Dna" of your study.** Los Gatos, Califórnia: Leadership + Design, 2014. Disponível em: https://www.drjohnlatham.com/*Frameworks*/research-methods-*Framework*/.Acesso em: 19 ago. 2020.

LEI De Proteção De Dados Do Estado De Hesse, 1970. **Empório do direito.** Disponível em: https://emporiododireito.com.br/leitura/a-aplicabilidade-da-lei-geral-de-protecao-de-dados-pessoais-lei-n-13-709-2018-as-pessoas-juridicas. Acesso em: 20, ago. 2020.

LEI De Proteção De Dados: Lei nº 289, Datalagen. 1973, Suécia. **Empório do direito.** Disponível em: https://emporiododireito.com.br/leitura/a-aplicabilidade-da-lei-geral-de-protecao-de-dados-pessoais-lei-n-13-709-2018-as-pessoas-juridicas. Acesso em: 20 ago. 2020.

LEMOS, Ronaldo; ADAMI, Mateus Piva; SUNDFELD, Philippe. Proteção de dados na Administração Pública. *In:* Jota Info. [São Paulo], 14 maio 2018. Online. Disponível em: https://www.jota.info/opiniaoeanalise/artigos/dadosadministracaopublica14052018#sdfootnote3anc. Acesso em: 3 maio 2020.

LIMA, Francisco Arga e; CARVALHO, Mateus Magalhães de. O Direito ao apagamento de dados como realidade global. *In*: COUTINHO, Francisco Pereira; MONIZ, Graça Canto (coord.). **Anuário de proteção de dados.** Lisboa: Universidade Nova de Lisboa, 2019. p. 55-86. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2019/06/ANUARIO-2019-Eletronico_compressed.pdf. Acesso em: 01 ago. 2020.

LIMA, Caio César Carvalho. Objeto, aplicação material e aplicação territorial. *In*: MALDONADO, Viviane Nóbrega; Opice BLUM, Renato (Coord.). **Comentários ao GDPR** – Regulamento Geral de Proteção da Dados da União Europeia. São Paulo: RT, 2018.

LIMA, Vinicius de Melo; GULARTE, Caroline de Melo Lima. Compliance E Prevenção Ao Crime De Lavagem De Dinheiro. **Revista do Ministério Público do Rs**, Porto Alegre, v. 82, p.119-145, abr. 2017. Disponível em: https://www.amprs.com.br/public/arquivos/revista_artigo/arquivo_1527273276.pdf. Acesso em: 11 abr. 2020.

LOPES, Teresa Vale Lopes. Responsabilidade e Governança das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. **Anuário de proteção de dados.** Lisboa: Universidade Nova de Lisboa, 2018. p. 45-70. Disponível em: http://cedis.fd.unl.pt/wp-content/uploads/2018/04/ANUARIO-2018-Eletronico.pdf. Acesso em: 01 ago. 2020.

LOVATO, Ana Carolina; Marília Camargo Dutra. Direitos fundamentais e direitos humanos – Singularidades e diferenças. *In:* SEMINÁRIO INTERNACIONAL DE DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPORÂNEA, 12., 2015, Santa Cruz do Sul. **Anais eletrônicos** [...]. Santa Cruz do Sul: Universidade de Santa Cruz do Sul, 2015. https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/13217/2323.pdf. Acesso em: 11 abr. 2020.

LUCA, Cristina de. Senado aprova que lei de proteção de dados seja adiada para 2021. *In:* Blog Porta 23. [S.l], 03 abr. 2020. Disponível em: https://porta23.blogosfera.uol.com.br/2020/04/03/congresso-comeca-a-votar-hoje-como-adiar-a-vigencia-da-lgpd/?cmpid=copiaecola. Acesso em: 20 ago. 2020.

MACHADO, Maíra Rocha. **Pesquisar empiricamente o direito.** São Paulo: Rede de Estudos Empíricos em Direito, 2017.

MAGRANI, Eduardo. **Entre dados e robôs:** ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélago Editorial, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **Comentários ao GDPR:** Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria **Técnicas de pesquisa.** São Paulo: Atlas, 1999.

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

MONTEIRO, Renato Leite. **Existe um direito à explicação na lei geral de proteção de dados no Brasil?** Rio de Janeiro: Instituto Igarapé, 2018a.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. *In:* Jota Info. [São Paulo], 14 jul. 2018b. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 23 jan. 2020.

MORAES, Maria Celina Bodin de. **Ampliando os direitos da personalidade**. Disponível em: https://www.academia.edu/9689598/Ampliando_os_direitos_da_personalidade. Acesso em: 12 ago. 2020.

MOREIRA, André de Oliveira Schenini. A exceção dos dados pessoais tornados manifestamente públicos pelo titular na LGPD. *In:* Migalhas. [S.l], 07 jan. 2019. Disponível em: https://migalhas.uol.com.br/depeso/293745/a-excecao-dos-dados-pessoais-tornados-manifestamente-publicos-pelo-titular-na-lgpd. Acesso em: 31 jul. 2020.

MOTA, Fabrício da. Proteção de dados pessoais é a evolução da privacidade. SERPRO, [Brasília], 30 ago. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/protecao-dados-evolucao-privacidade. Acesso em: 18 ago. 2020

MURARO. Igor S. A importância do privacy by design e privacy by default nas aplicaçõesO que podemos aprender com o caso Zoom**.** *In:* Jota Info. [São Paulo], 02 maio 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-importancia-do-privacy-by-design-e-privacy-by-default-nas-aplicacoes-02052020. Acesso em: 12 ago. 2020.

NAÇÕES UNIDAS. Assembleia Geral. **Declaração universal dos direitos humanos.** Adotada e proclamada pela Assembléia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro 1948. Brasília, DF: UNICEF, [2018?]. Disponível em: https://nacoesunidas.org/wpcontent/uploads/2018/10/DUDH.pdf. Acesso em: 02 ago. 2020.

NAKAMURA, Emílio Tisseto de; FORMIGONI FILHO, José Reynaldo; IDE, Marcos Cesar. Metodologia na Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais. *In:* SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 19., 2019, São Paulo. **Anais eletrônicos** [...]. São Paulo: Universidade de São Paulo, 2019. Disponível em: https://sbseg2019.ime.usp.br/anais/197877.pdf. Acesso em: 05 ago. 2020.

NAVARRO, Vera Lucia; CARRIJO, Débora Couto de Melo. Ler e planos de demissão voluntária: trajetórias de dor e sofrimento entre bancários. **Cadernos de Psicologia Social do Trabalho**, v. 12, n. 1, p. 157-171, 2009. Disponível em: http://pepsic.bvsalud.org/pdf/cpst/v12n2/a03v12n2.pdf. Acesso em: 11 abr. 2020.

NIGRI, Tânia. Sigilo de dados - os limites da sua inviolabilidade. *In:* Migalhas. [S.l], 11 set. 2006. Disponível em: https://migalhas.uol.com.br/depeso/29716/sigilo-de-dados---os-limites-da-sua-inviolabilidade. Acesso em: 31 jul. 2020.

NUNES, Rizzatto. A vida privada, intimidade, segredo e sigilo. *In:* Migalhas. [S.l], 16 fev. 2017. Disponível em: https://www.migalhas.com.br/coluna/abc-do-cdc/254049/a-vida-privada-a-intimidade-o-segredo-e-o-sigilo. Acesso em: 31 jul. 2020.

NUNES, Samantha. Como implantar um projeto de conformidade com a LGPD? *In:* Computerworld. [S.], 06 fev. 2020. Disponível em: https://computerworld.com.br/2020/02/06/como-implantar-um-projeto-de-conformidade-com-a-lgpd/. Acesso em: 19 ago.2020.

OBSERVATÓRIO da Proteção de Dados Pessoais. **CEDIS**. 2020. Disponível em: http://protecaodedadosue cedis.fd.unl.pt/. Acesso em: 05, ago. 2020.

OLIVEIRA, James Eduardo. **Código Civil anotado e comentado:** doutrina e jurisprudência. Rio de Janeiro: Forense, 2009.

OLIVEIRA, Ana Paula de *et al*. A Lei Geral de Proteção de Dados Brasileira na prática empresarial. **Revista Jurídica da ESA OAB/PR**, Curitiba, v. 4, n. 1, s.p., maio 2019.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). **Declaração Americana dos Direitos e Deveres do Homem**. Aprovada na Nona Conferência Internacional Americana, Bogotá, 1948. Bogotá: 1948. Disponível em: http://www.direitoshumanos.usp.br/index.php/OEA-Organiza%C3%A7%C3%A3o-dos-Estados-Americanos/declaracao-americana-dos-direitos-e-deveres-do-homem.html. Acesso em: 19 ago. 2020.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas: Parlamento Europeu, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 20 ago. 2020.

PARLAMENTO EUROPEU; CONSELHO DA UNIÃO EUROPEIA; COMISSÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Européia, Nice, França, em 07 de dezembro de 2000**. Bruxelas: Parlamento Europeu, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 5 dez. 2018.

PIERGALINI, Ana Silvia de Moura Leite *et al*. Privacidade e Democracia:os impactos da LGPD nas eleições de 2020. *In:* Jota Info. [São Paulo], 07 mar. 2020. Disponível

em: https://www.jota.info/opiniao-e-analise/artigos/privacidade-e-democracia-os-impactos-da-lgpd-nas-eleicoes-de-2020-07032020. Acesso em: 07 mar. 2020.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** Comentários à Lei n. 13.709/2018. São Paulo: Editora Saraiva Educação, 2018a.

PINHEIRO, Patrícia Peck. **Advocacia digital.** São Paulo: Thompson Reuters, 2018b.

PINHEIRO, Patrícia Peck. LGPD: Os prós e contras de prorrogar a Lei para 2022. *In:* **Crypto ID**. [São Paulo], 04 nov. 2019. Disponível em: https://www.cryptoid.com.br/identidade-digital-destaques/lgpd-os-pros-e-contras-de-prorrogar-a-lei-para-2022/. Acesso em: 18 ago. 2020.

RIBEIRO, Marcia Carla Pereira; DINIZ, Patrícia Dittrich Ferreira. **Compliance e lei anticorrupção nas empresas.** Brasília: Senado Federal, 2014.

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** Privacidade hoje. Rio de Janeiro: Renovar, 2008.

SÁ, Marcelo Dias de. **Análise do impacto da nova lei de proteção de dados pessoais nas aplicações de Internet das coisas:** Aplicações mobile do governo. 2019. Trabalho de Conclusão de Curso (Especialização em Informática) – Instituto de Ciências Exatas, Universidade Federal de Minas Gerais, Brasília, 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1843/32040/1/MarceloDiasDeSa.pdf. Acesso em: 12 jul. 2020.

SANTOS, Renato Almeida dos *et al*. Compliance e liderança: a suscetibilidade dos líderes ao risco de corrupção nas organizações. **Einstein**. São Paulo, v. 10, n. 1, p. 1-10, mar. 2012. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S167945082012000100003&lng=pt&nrm=iso. Acesso em: 11 abr. 2020.

SANTOS, Thiago; DUARTE, Bruno. A responsabilidade civil dos provedores de aplicação de Internet no tratamento de dados à luz da Lei nº 12.965/14 denominada o marco civil da Internet. **Revista de Direito da Faculdade Estácio do Pará**, Belém, v. 5, n. 7, p. 79-100, jun. 2018. Disponível: http://www.revistasfap.com/ojs3/index.php/direito/article/view/193. Acesso em: 11 abr. 2020.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional.** Porto Alegre: Revista dos Tribunais, 2012.

SARMENTO, Daniel. **Dignidade da pessoa humana:** conteúdo, trajetórias e metodologia. 2. ed. Belo Horizonte: Fórum, 2016.

SIENA, Omar. **Metodologia da pesquisa científica:** elementos para elaboração e apresentação de trabalhos acadêmicos. Porto Velho: PPGMAD/UNIR, 2007.

SILVA, Keila Brito. Direito à saúde e integralidade: uma discussão sobre os desafios e caminhos para sua efetivação. **Interface:** Comunicação, saúde, educação, Botucatu, v. 16, n. 40, p. 249-259, jan./mar. 2012. Disponível em http://www.scielo.br/pdf/icse/v16n40/aop1812. Acesso em 11 abr. 2020.

SILVA, Raiane Rodrigues de. **A importância do setor de recursos humanos no contexto da estratégia da organização**. 2013. Trabalho de Conclusão de Curso (Especialização em Gestão em Recursos Humanos) – Centro Universitário Barriga Verde, Orleans, 2015. Disponível em: http://www.uniedu.sed.sc.gov.br/wp-content/uploads/2015/02/Monografia-RAIANE-RODRIGUES-DA-SILVA.pdf. Acesso em: 11 abr 2020.

SILVEIRA, Sergio Amadeu da. Marco civil e a proteção da privacidade. **Com Ciência**, Campinas, n. 158, maio 2014. Disponível em http://comciencia.scielo.br/scielo.php?script=sci_arttext&pid=S1519-76542014000400008&lng=pt&nrm=iso. Acesso em: 11 abr. 2020.

SIMOES, José Augusto. Proteção de dados e o novo regulamento geral da União Europeia. **Rev Port Med Geral Fam**, Lisboa, v. 34, n. 5, p. 266-267, out. 2018 Disponível em: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S2182-51732018000500001&lng=pt&nrm=iso. Acesso em: 11 abr. 2020.

SMITH, Robert Ellis. **Privacy, how to protect what's left of it. Londres:** Anchor Press, 1979.

SOLOVE, Daniel J. **The digital person:** Technology and Privacy in the Information Age. New York: NYU Press, 2004.

SOMADOSSI, Henrique. O que muda com a Lei Geral de Proteção de Dados (LGPD). *In:* Migalhas. [S.l], 24 ago. 2018. Disponível em: https://www.migalhas.com.br/depeso/286235/o-que-muda-com-a-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 05 ago. 2020.

SOUZA, Thiago Vieira de. **A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de cookies.** 2018. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Uberlândia, Uberlândia, 2018. Disponível em https://repositorio.ufu.br/bitstream/123456789/23198/3/Prote%C3%A7%C3%A3oDadosPessoais.pdf. Acesso em: 11 abr. 2020.

VIERIA, Thais Leal. **O direito penal do inimigo e suas bases funcionalistas:** fundamentação sociológica e filosófica, reflexos e críticas. 2008. Trabalho de Conclusão de Curso (Bacharelado em Ciências Jurídicas e Sociais) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2008.

VIEIRA, Sérgio. Acordo Mercosul – UE deve baratear produtos, mas forçar eficiência e produtividade. *In:* Senado Federal. [Brasília], 10 set. 2019. Disponível em: http://www12.senado.leg.br/noticias/infomaterias/2019/08/acordo-mercosul-ue-deve-baratear-produtos-mas-forcar-eficiencia-e-produtividade. Acesso em: 18 ago. 2020.

Você sabe o que são *cookies* e como eles interferem em sua privacidade?. *In:* SAFERNET. [S.l], [s.d]. Disponível em: https://new.safernet.org.br/content/voc%C3%AA-sabe-o-que-s%C3%A3o-*cookies*-e-como-eles-interferem-em-sua-privacidade#:~:text=Privacidade-,Voc%C3%AA%20sabe%20o%20que%20s%C3%A3o%20*cookies*,eles%20interferem%20em%20sua%20privacidade%3F&text=Os%20*cookies*%20rastreiam%20o%20comportamento,vendas%20de%20determinados%20produtos%2C%20etc. Acesso em: 02 ago. 2020.

XIMENES, Salomão Barros. O Conteúdo Jurídico do Princípio Constitucional da Garantia de Padrão de Qualidade do Ensino: uma contribuição desde a teoria dos direitos fundamentais. **Educ. Soc**., Campinas, v. 35, n. 129, p. 1027-1051, Dez. 2014. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-73302014000401027&lng=en&nrm=iso. Acesso em: 11 abr. 2020.

WARREN, Samuel; BRANDEIS, Louis. “The Right to Privacy”. **Harvard law review**, Harvard, v. 4, n. 5, p. 193-220, 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf . Acesso em: 24 abr. 2020.

GLOSSÁRIO

ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

ARMAZENAMENTO - ação ou resultado de manter ou conservar em repositório um dado;

ARQUIVAMENTO - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotado a sua vigência;

AVALIAÇÃO - analisar o dado com o objetivo de produzir informação;

CLASSIFICAÇÃO - maneira de ordenar os dados conforme algum critério estabelecido;

COLETA - recolhimento de dados com finalidade específica;

COMUNICAÇÃO - transmitir informações pertinentes a políticas de ação sobre os dados;

CONTROLE - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;

DIFUSÃO - ato ou efeito de divulgação, propagação, multiplicação dos dados;

DISTRIBUIÇÃO - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;

ELIMINAÇÃO - ato ou efeito de excluir ou destruir dado do repositório;

EXTRAÇÃO - ato de copiar ou retirar dados do repositório em que se encontrava;

MODIFICAÇÃO - ato ou efeito de alteração do dado;

PROCESSAMENTO - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;

PRODUÇÃO - criação de bens e de serviços a partir do tratamento de dados;

RECEPÇÃO - ato de receber os dados ao final da transmissão;

REPRODUÇÃO - cópia de dado preexistente obtido por meio de qualquer processo;

TRANSFERÊNCIA - mudança de dados de uma área de armazenamento para outra, ou para terceiro;

TRANSMISSÃO - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;

UTILIZAÇÃO - ato ou efeito do aproveitamento dos dados.