OAB RIO GRANDE DO SUL ESA

REVISTA ELETRÔNICA DA ESA/RS

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

A REGULAMENTAÇÃO BRASILEIRA SOBRE A PROTEÇÃO DE DADOS PESSOAIS DIGITAIS NAS ATIVIDADES DAS EMPRESAS

BRAZILIAN REGULATION ON THE PROTECTION OF DIGITAL PERSONAL DATA IN BUSINESS ACTIVITIES

Gustavo Wentz[1]

Lauren Hanel Lang Tabolka[2]

Lilian Hanel Lang[3]

RESUMO

Este estudo, no seu objetivo buscou identificar as diretrizes regulamentadas em lei, que fazem parte das medidas que devem ser consideradas pelas empresas no tratamento dos dados pessoais de forma lícita que não seja violada a privacidade dos cidadãos. Observa, primeiramente, que as regulamentações têm sido fortalecidas em plano global, impulsionadas pela consolidação da internet quanto ao acesso de todos sobre informações compartilhadas. Em normatização brasileira, tal acesso vem sendo assegurado, sofrendo ajustes recentes em seus dispositivos sobre a atenção das empresas quanto aos dados pessoais armazenados de seus clientes. Tais dispositivos sustentam-se no princípio da boa fé, sendo norteados por princípios que são básicos na proteção efetiva dos dados pessoais, devendo ser observados pelas instituições que manipulam dados guardados, a partir da sua finalidade, transparência, qualidade e segurança. Podem ser verificados, nesse sentido, requisitos que, em seu teor, tutelam a proteção dos dados pessoais em ambiente digital, inaugurando um outro olhar sobre essa tutela, quando se trata de violação. A legislação enumera e disciplina desde a privacidade liberdade de expressão, informação, bem como desenvolvimento livre, inviolabilidade íntima calcada nos direitos humanos e na dignidade da pessoa humana. Em conclusão, as evidências presentes na proteção do tratamento de dados pessoais, armazenados nas empresas, se estabelecem em lei para, no seu efeito propositivo, resguardar informações digitais e a privacidade dos cidadãos.

Palavras-chave: Empresas. Era digital. Proteção de dados.

ABSTRACT

This study, in its objective, sought to identify the guidelines regulated by law, which are part of the measures that must be considered by companies in the treatment of personal data in a

[1] Coordenador e Professor do Curso de Direito de Faculdade IDEAU – Getúlio Vargas. Mestre em Direito pela Faculdade Meridional – IMED. Especialista em Direito Civil e Processo Civil pela Universidade de Passo Fundo - UPF. Graduado em Ciências Jurídicas e Sociais pela UPF. E-mail: gustavowentz@ideau.com.br

[2] Aluna do Programa de Mestrado Interdisciplinar em Ciências Humanas – UFFS. Pós Graduada em Direito Previdenciário – UPF. Graduada em Direito – URI. Docente Faculdade Anglicana de Tapejara. Email: adv.advogados@bol.com.br Advogada inscrita na OAB/RS 69.693.

[3] Mestre em História – UPF. Pós-graduada em Direito do Trabalho e Seguridade Social - UPF; em Gestão Pública – UFSM; em Gestão Pública das Organizações de Saúde – UFSM. Graduada em Direito - URI. Docente da Faculdade IDEAU/Getúlio Vargas-RS. Email: lilianlang@ideau.com.br Advogada inscrita na OAB/RS 74282.

lawful manner that does not violate the privacy of citizens. It observes, first, that the regulations have been strengthened on a global level, driven by the consolidation of the internet in terms of everyone's access to shared information. In Brazilian regulations, such access has been ensured, with recent adjustments to its devices regarding the attention of companies regarding the personal data stored by their customers. Such devices are based on the principle of good faith, being guided by principles that are basic in the effective protection of personal data, and must be observed by the institutions that manipulate stored data, based on its purpose, transparency, quality and security. In this sense, requirements can be verified that, in their content, protect the protection of personal data in a digital environment, opening another look at this protection, when it comes to violation. The legislation lists and disciplines privacy, freedom of expression, information, as well as free development, intimate inviolability based on human rights and the dignity of the human person. In conclusion, the evidence present in the protection of the processing of personal data, stored in companies, is established by law to, in its purposeful effect, safeguard digital information and the privacy of citizens.

Keywords: Companies. Digital age. Data protection.

1 INTRODUÇÃO

A Lei n. 13.709, de 2018, com ajustes da Lei n. 13.853, de 2019, que vigora desde agosto do ano de 2020, estabelece robustas modificações na maneira como o ordenamento empresarial deve se postar frente ao tratamento e controle sobre os dados pessoais em seu fluxo de informações.

A atenção com as informações postadas nos dados pessoais resulta das transformações ocorridas na privacidade a partir do advento da denominada Quarta Revolução Industrial, em 1970, que informacionalizou a sociedade, respingando nas práticas empresariais que se sustentam por número bastante significativo de dados, oriundos do formato *online* (BOFF; FORTES; FREITAS, 2018).

No seu teor, a Lei n. 13.709 apresenta uma série de mecanismos protetivos, entre as quais, as que preveem multa de até 50 milhões de reais, aplicada pela Autoridade Nacional de Proteção de Dados (ANPD), quando se configurarem evidências de não observância da Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018).

A novel regulamentação estende sua importância, quer no intuito de tutelar a privacidade e proteção de informações pessoais *online* dos entes titulares, quer nas práticas

empresariais, quando demanda uma gama de requisitos, estabelecidos na LGPD, para que os dados informativos tenham o devido tratamento lícito.

Em alinhamento, este estudo traz como problema: como as medidas estabelecidas na Lei n. 13.709 de 2018, no que compete ao seu caráter protetivo no tratamento de dados pessoais, armazenados nas empresas, pode ser eficiente para resguardar informações utilizados em serviços *online*?

O assunto, em tela, justifica-se não só por seu caráter de contribuição no que tange a informações e elucidações à área acadêmica, como se apresenta de relevância em palco empresarial sobre a forma lícita de resguardar dados pessoais bem como pela égide da justiça, na função e atribuição dos órgãos competentes para que sejam postas em prática as medidas e diretrizes estabelecidas pela Lei 13.709, de 2018.

Em seu objetivo, busca identificar as diretrizes regulamentadas em lei, que fazem parte das medidas que devem ser consideradas pelas empresas no tratamento dos dados pessoais de forma lícita que não viole a privacidade dos cidadãos.

A opção foi pelo método dedutivo, que parte da generalização e se fundamenta na particularidade, embasado por amparo bibliográfico que inclui autores, leis e dados que versam sobre o tema em estudo.

2 A LEI N. 13.709/18 À LUZ DA PRINCIPIOLOGIA E O OLHAR DAS EMPRESAS

A novel Lei Geral de Proteção de Dados de 2018, já vigente, endossa posicionamentos para as empresas que possuem dados pessoais armazenados, obrigando-as a adaptações frente a um novo ordenamento legal para a preservação da privacidade das pessoas em outra contextualização.

A regulamentação sobre o uso de dados pessoais via lei específica vem se fortalecendo em cenário global a partir do momento em que a internet se consolidou e permitiu o acesso de todos de forma compartilhada quanto às informações. Em solo brasileiro, transitar pela internet se encontra garantido pela determinação da Lei n. 12.965 de 2014, quando evidencia em seu art. 7º[4] que ascender à internet é fundamental para que se exerça a cidadania do usuário.

[4] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] (BRASIL, Lei n. 12.965, 2014).

A Lei 13.709 de 2018, ajustada em alguns itens pela Lei n. 13.853 de 2019, estabelece em seu art. 6º[5], sobre a observância das empresas que armazenam dados pessoais, fundamentado no princípio da boa fé, sendo seguido por princípios basilares que sustentam a o olhar atento da lei na proteção efetiva dos dados pessoais.

Segundo expõe Mendes (2014), os princípios se desvelaram firmados em mecanismos internacionais e transnacionais, pela nova percepção de privacidade, associada à proteção dos dados pessoais, sendo embutidos na legislação do Brasil. Sendo essenciais aos cidadãos, tais princípios precisam ser considerados pelas instituições que lidam com dados que permanecem armazenados, podendo entre outros, serem basilares os princípios da finalidade, transparência, qualidade e também segurança de dados.

Nessa esteira, o princípio da finalidade, pela sua fundamentação, se estabelece por meio de uma via correlativa entre a utilização dos dados pessoais e o fim informado aos entes, por ocasião da realização da coleta. Isso pode, além de impor limites o acesso de outrem ao que foi coletado, determinar adequação e razoabilidade dos dados adquiridos. Na sua observância, o princípio da finalidade, nas instituições, ampara-se pelo fim dispensado ao "[...] tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas" (MENDES, 2014, p. 71).

[5] Art. 6º. As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, Lei n. 13.709, 2018).

No que compete ao princípio da transparência, o conhecimento público é preceito fundamental, justificado pela máxima da democracia de dados sigilosos sendo incompatíveis com estado democrático de direito. Além disso, em caráter transparente, os dados ficam longe de práticas abusivas de sua utilização. Em acordo com tal princípio, as instituições devem ser nominadas, bem como sua sede e conteúdo junto ao banco de dados, registradas publicamente em "[...] diários oficiais ou meios de grande circulação sob pena de ineficácia desse direito" (MENDES, 2014, p. 71).

Já, quanto ao princípio de qualidade, conforme ensina Silva (2015), há a exigência de informações qualificadas, sendo tratadas de forma leal e lícita e se mostrarem adequadas ao fim proposto, apresentando teor objetivo, com exatidão e atualização. Por isso, as empresas devem mostrar cautela com a manipulação dos dados. Segundo refere Mendes (2014), a atualização dos dados deve sempre se fazer presente, com dispositivos que possam assegurar os direitos de acessibilidade, retificação e pedidos de cancelamento.

Em sequência, na efetivação do princípio de segurança, impõem-se formas que evitem que os dados pessoas possam sofrer extravios, destruições, modificações e desvios, que não tiverem autorização de seus titulares. Nesse alinhamento, o princípio da responsabilização e prestação de contas se configura quando busca garantir "[...] a reparação adequada e integral dos danos materiais e morais causados ao indivíduo em razão da violação ao seu direito à privacidade" (MENDES, 2014, p. 72).

Veríssimo (2017), nesse sentido, cita os Programas de Integridade (*Compliance*) como uma relevante via para suprir os obstáculos desafiadores que compõem uma prática de adaptação, bem como os seus formatos estratégicos para reduzir riscos de reputação e de legalidade das empresas, e isso demanda organização tecnológica de segurança de informação governança normativa e contratual, aliadas à capacitação de equipes, para agirem de forma rápida.

Nesse sentido, torna-se importante considerar o programa a ser utilizado, podendo ser ajustado ao porte e ao riscos da empresa que terão pela frente. Formatos de integridade com procedimentos rigorosos mais simples que podem assegurar a observância ética e íntegra entre as microempresas e empresas de menor porte estão estabelecidos na Portaria Conjunta da Controladoria Geral da União (CGU) e do Ministério da Micro e Pequena Empresa n. 2279/2015. Isso deixa claro serem possíveis programas de adequação em caráter simples e de

forma garantida, com baixo custo às empresas. O cumprimento de normas torna-se, assim, mais complexo em situações cujas empresas apresentam grandes portes e consequentes grandes riscos. (VERÍSSIMO, 2017).

De acordo com art. 52, parágrafo II[6], da LGPD, quando se tratar de riscos e seu descumprimento, as penalidades comportam sérios efeitos, principalmente se houver publicização da infração, o que resulta em multa diária incidindo sobre o faturamento da empresa, em especial no Brasil, computando a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Conforme expõe Frazão (2018), o programa de ajuste não se apresenta de forma fácil, contudo, em não havendo a sua efetivação, os prejuízos podem ser inúmeros para as empresas, pois, ao mesmo tempo em que as adequações se mostrem preventivas, também são reativas. Assim, os programas de ajustamento podem ser considerados redutores de prejuízos e danos.

Veríssimo (2017), nesse cenário, traz indicadores de um Programa de Integridade, sob o viés de três aportes. Primeiramente, inserem-se o momento de verificação dos riscos, a definição de procedimentos preventivos e a montagem de uma organização de *compliance*. Após, em segundo tempo, inclui-se a implementação, quando é informado o detalhe do programa, com medidas para compor os processos de *compliance*. Já no que se refere ao terceiro tempo, instalam-se a consolidação e o aperfeiçoamento, via processo de análise de violações, critério de sanções, bem como verificação contínua, com práticas de aperfeiçoamento do programa.

Os riscos, conforme Veríssimo (2017), deve ser estruturados, de maneira que possam ser previstos e sequencialmente serem evitados ou reduzidos, com a finalidade de preservar a empresa de prováveis danos à sua imagem, caso ocorra vazamento das informações armazenadas. Nesse contexto, Barros refere que o risco se compõe "[...] de dois grandes componentes: a probabilidade de ocorrência e a magnitude de perda", sendo que esta última consiste em "impacto". Por sua vez, as ocorrências se configuram em eventos danosos em dado

[6] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
[...] II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; [...] (BRASIL, Lei n. 13.709, 2018).

tempo, impactando o sentido comprometido "[...] de uma das propriedades básicas da segurança de informação: confidencialidade, integridade e disponibilidade" (2015, p. 40).

Barros (2015) assinala, ainda, que podem ser apontados instrumentos para estarem em acordo com a LGPD, como a composição de normas 27000, em publicação pela *International Organization for Standardization* (ISO), que se destaca em robusto mecanismo protetivo de dados. Em seus ordenamentos, tais normas traçam requisitos para um sistemática de gestão de segurança da informação (SGSI), somada à operação, que é a ISO 2700121, e que se revela em um padrão internacional com reconhecimento e valia para que seja garantida a informação.

Em seguimento, próximo item faz uma abordagem sobre alguns artigos que estabelecem a privacidade e suas políticas de garantias, fundamentados na LGPD, de 2018, consagrando um novo olhar para assegurar que os dados pessoais não sejam violados e manipulados de forma ilícita.

3 DADOS PESSOAIS DIGITAIS E AS POLÍTICAS DE PRIVACIDADE: ALGUMAS CONSIDERAÇÕES

No que compete aos requisitos que buscam proteger os dados pessoais em ambiente digital, a LGPD, nas suas normativas, inaugura um novo olhar sobre esse material e a probabilidade sua violação, que deve estar protegida por lei.

Relata Fernandes que a Diretiva da União Europeia há algum tempo vem abraçando o tema sobre necessidade protetiva dos dados pessoais, deixando evidenciado em seu manifesto:

> A Diretiva 95/46/CE, do Parlamento Europeu e do Conselho da Europa, de 24 de outubro de 1995, veio a responder a esta necessidade, ao obrigar os Estados à adoção de legislação oferecendo garantias semelhantes em todo o espaço europeu, e ao regrar os procedimentos quanto aos fluxos de dados pessoais para países que não os da União Europeia, tendo este passado a ser classificado de modo diferenciado, consoante ofereçam, ou não, um nível de proteção adequado (2017, p. 364).

Em seara brasileira, a LGPD de 2018 tem apresentado uma gama de dispositivos que inserem a devida atenção com o destino dos dados pessoais armazenados. Nesse sentido, segundo expõe Frazão, há o entendimento de que "[...] o regime de proteção de dados não tem por finalidade apenas a de tutelar a privacidade dos usuários" (2018, p. 3).

Em observância da Lei 13.709/2018, o seu art. 1º[7] deixa clara a sua finalidade precípua, quando atenta para a real proteção dos direitos essenciais de liberdade e privacidade bem como pelo pleno desenvolvimento da personalidade dos cidadãos. Fica, assim, definido o objeto da lei.

Já o art. 2º[8] da lei enumera e disciplina uma gama de requisitos que amparam a sua aplicação e que implica a proteção efetiva do cidadão e seus dados pessoais. Aborda desde a privacidade liberdade de expressão, informação, entre outros, bem como desenvolvimento livre, inviolabilidade íntima calcada nos direitos humanos e na dignidade da pessoa humana.

Entende Frazão que ao enumerar o desenvolvimento livre da personalidade, assim como da cidadania e dignidade,

> [...] a lei certamente procura evitar muitas das destinações atuais que vêm sendo conferidas aos dados pessoais, os quais, processados por algoritmos, são capazes de fazer diagnósticos e classificações dos usuários que, por sua vez, podem ser utilizados para limitar suas possibilidades de vida. Mais do que isso, a partir de tais dados, as empresas podem discriminar usuários ou mesmo tentar manipular suas opiniões, crenças ou valores em vários âmbitos, inclusive o político (2018, p. 4).

Por sua vez, o art. 4º[9] estabelece sobre as situações, cuja LGPD não estende sua aplicação, expondo no inciso I, em caso de pessoa natural para fins exclusivamente particulares

[7] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019) (BRASIL, Lei n. 13.709, 2018).

[8] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V - o desenvolvimento econômico e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, Lei n. 13.709, 2018).

[9] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:
a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou

e não econômicos, e também para fins jornalísticos e artísticos, e de acadêmicos, a não ser em situações que estão determinadas nos arts. 7º[10].

Por sua vez, o inciso III, do art. 4º, traz a sua inaplicabilidade no que tange aos tratamento dos dados pessoais nos casos de fins únicos de segurança pública, defesa nacional, segurança do estado, e,

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
§ 2º É vedado o tratamento dos dados a que se refere o inciso III do caput deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do caput deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público (Redação dada pela Lei n. 13.853, de 2019) (BRASIL, Lei n. 13.709, 2018).

[10] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
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;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
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;
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);
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei n. 13.853, de 2019)
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.
§ 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.
§ 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.
§ 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.
§ 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. (Incluído pela Lei n. 13.853, de 2019) (BRASIL, Lei n. 13.709, 2018).

também, em ações investigativas atividades de investigação e de repressão de infrações penais. Ainda o inciso V refere sobre a não aplicação ao dados oriundos de fora do solo brasileiro, que não são objeto de comunicação, bem como sobre o uso compartilhado de dados com agentes de tratamento brasileiros, entre outras situações.

Nesse sentido, o art. 5º, inciso II[11], da LGDP descreve em seu teor o dado pessoal, observado como sensível quando se trata de informação pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, incluindo dados que dizem respeito à saúde ou à vida sexual, bem como genético ou biométrico, em vínculo a uma pessoa natural.

Em sua referência, associa-se o art. 6º da Lei n. 13.709, quando enumera os princípios que devem ser considerados na competência do tratamento de dados, deixando evidenciada a concomitância do princípio da boa fé. Nesse alinhamento são estabelecidos para fins da LGPD, os princípios que tangem à finalidade, adequação, necessidade, ao livre acesso, à qualidade dos dados, transparência, segurança; prevenção, a não discriminação, à responsabilização e prestação de contas.

Por sua vez, o art. 7º da LGPD enumera critérios nos quais se insere como podem ser tratados os dados pessoais. A atenção que deve ser considerada é a da permissão do titular, para a efetivação de qualquer tratamento, coleta, disponibilização dos dados pessoais, exceto os que se encontram estabelecidos neste artigo.

No que compete ao caráter privativo dos dados, a LGPD inclui como exigência a especificação sobre a finalidade dos dados a serem tratados com limitação mínima necessária de informação, bem com o prazo já definido, segundo expõe o art. 15, I e II[12]. Já quanto aos meios disponíveis para o titular ter livre acesso o art. 9[13] em seu *caput* deixa evidenciado o

[11] Art. 5º Para os fins desta Lei, considera-se:
[...] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, Lei n. 13.709, 2018).
[12] Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
II - fim do período de tratamento; [...] (BRASIL, Lei n. 13.709, 2018).
[13] 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:

formato claro, adequado e ostensivo dentre outras características que se inserem para o acolhimento do princípio.

Conforme assinalam Oliveira *et al.* (2019), é essencial disponibilizar ao titular dos dados as informações claras e precisas, e isso se revela em um amplo desafio para as empresas, em especial, àquelas que praticam a exploração de tais dados de forma comercial, uma vez que precisam justificar o tratamento dos dados embasadas pelas previsões legais dispostas no art. 7º da LGPD.

Nesse sentido, fica evidenciado que a ação política de privacidade deve cientificar o titular dos dados pessoais de que tais dados serão tratados seguindo os dispositivos inseridos na LGPD, em seu art. 7º e que somam dez hipóteses (OLIVEIRA *et al*. 2019).

Na compreensão de Cavalcanti e Santos, a hipótese do consentimento, expressa no artigo 7º, I, da Lei n. 13.709, mostra sua essencialidade "[...] na autodeterminação informativa, controle e liberdade do titular em relação aos seus dados, configurando-se elemento central para a proteção de dados pessoais" (2018, p. 358). No entanto, pode ser examinada como uma hipótese frágil, devido à probabilidade de ser revogada pelo titular, bem como ser observada como nula a anuência do titular em situação de abuso ou se for conseguido a partir de informações incompletas ou de conteúdo enganoso e que se fundamenta pelo art. 8º, § 5º[14] da LGPD.

Frazão (2018) destaca que a Lei n. 13.709, no teor do seu art 5º aponta vários conceitos sobre consentimento, sendo que em, em seu inciso XII[15], o texto expressa sobre um tipo de livre manifestação, que é informada se equívocos em concordância com o titular sobre a forma de tratar os seus dados pessoais, e que traz em seu bojo uma robusta feição principiológica no que tange à informação que se autodetermina, com sustentação no art. 2º, II.

Por sua vez o art. 8º, § 1º[16] também se soma às permissões legais, teorizando que o consentimento dos dados pessoais deve ocorrer em formato escrito ou outro meio que mostre a

[14] Art. 8º [...] § 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, Lei n. 13.709, 2018).
[15] Art. 5º [...] XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; [...] (BRASIL, Lei n. 13.709, 2018).
[16] 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.

anuência do titular. Cabe, ainda, a verificação regular desse consentimento pelo controlador do ônus da prova, sob a égide da lei, conforme estabelece o § 2º[17], do mesmo artigo.

Na sua qualificação, o consentimento se sustenta a partir da afirmação, segundo Frazão (2018), de que

> [...] a manifestação de vontade precisa ser (i) livre e inequívoca, (ii) formada mediante o conhecimento de todas as informações necessárias para tal, o que inclui a finalidade do tratamento de dados, e (iii) restrita às finalidades específicas e determinadas que foram informadas ao titular dos dados (2018, p. 2).

Em formato mais amplo, estende-se a qualificação do consentimento no que tange ao tratamento de dados pessoais também aos que se referem aos pessoais sensíveis, em seus critérios, conforme estabelece o art. 11, inciso I[18], sendo acompanhado pelo art. 14, § 1º[19], que aborda os menores de idade, cujo consentimento deve ocorrer a partir dos pais ou responsáveis.

A partir de tais observações, fica evidenciado que a regulamentação que trata dos dados pessoais digitais em seu caráter de proteção está assentada pela LGPD, traçando requisitos e critérios que precisam ser considerados para que tais dados, estando armazenados nas empresas, não sejam utilizados de forma alheia à vontade de seu titular, a não ser quando esse optar por consentimento.

4 CONSIDERAÇÕES FINAIS

Na busca de identificação sobre as diretrizes regulamentadas em lei, que fazem parte das medidas que devem ser consideradas pelas empresas no tratamento dos dados pessoais de forma lícita que não viole a privacidade dos entes, este estudo, inicialmente, observa que as considerações da lei vêm se fortalecendo em plano global, impulsionadas pela consolidação da

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. [...] (BRASIL, Lei n. 13.709, 2018).

[17] Art. 8º [...] § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei (BRASIL, Lei n. 13.709, 2018).

[18] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; (BRASIL, Lei n. 13.709, 2018).

[19] Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal (BRASIL. Lei n. 13.709, 2018).

internet no que compete ao acesso de todos sobre informações em via compartilhada. No cenário brasileiro, esse acesso tem sua garantia desde a Lei n. 12.965 de 2014, quando estabelece a sua importância para o exercício da cidadania do usuário.

Por sua vez, a Lei 13.709, de 2018, ajustada pela Lei 13.853, de 2019, estabelece sobre a atenção das empresas, na observância dados pessoais armazenados de seus clientes, que se fundamentam no princípio da boa fé, permeado por princípios que são básicos e sustentáculos na proteção efetiva de tais dados.

Esses princípios se sustentam em instrumentos internacionais e transnacionais, pela nova visão de privacidade, atribuída à proteção dos dados pessoais, e que estão consagrados na legislação brasileira. Na sua essencialidade, precisam ser observados pelas instituições que manipulam dados que se encontram armazenados, a partir da sua finalidade, transparência, qualidade e segurança.

Podem ser verificados, assim, requisitos que, em seu teor, tutelam a proteção dos dados pessoais em ambiente digital, a partir da nova legislação, inaugurando um outro olhar sobre esse material e quando se trata de violação. A Lei enumera e disciplina desde a privacidade liberdade de expressão, informação, bem como desenvolvimento livre, inviolabilidade íntima calcada nos direitos humanos e na dignidade da pessoa humana.

Ao concluir, fica evidenciado que a proteção do tratamento de dados pessoais, armazenados nas empresas, se encontra estabelecida na Lei n. 13.709 de 2018, com ajustes pela Lei 13.853, de 2019, para, no seu efeito propositivo, resguardar informações digitais e a privacidade dos cidadãos.

Nessa perspectiva, as considerações, que se mostram pertinentes e significativas, sugerem futuras análises e pesquisas no que compete ao cumprimento real das garantias da legislação pelas empresas.

REFERÊNCIAS

BOFF, S. O.; FORTES, V. B.; FREITAS, C. O. A. **Proteção de dados e privacidade:** do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei n. 13.853, de 2019) Vigência. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/ L13709.htm>. Acesso em: 12 mar. 2021.

BRASIL. **Lei n. 13.853, de 2019, de 8 de julho de 2019.** Altera a Lei n. 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: <http://www.planalto.gov.br › ccivil_03 › _ato2019-2022>. Acesso em: 12 mar. 2021.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br › Acesso em: 12 mar. 2021.

CAVALCANTI, N. P.; SANTOS, L. M. S. B. A lei geral de proteção de dados do Brasil na era do Big Data. *In:* **Tecnologia Jurídica & Direito Digital** - II Congresso Internacional de Direito, Governo e Tecnologia. 2018.

FERNANDES, D. A. Dados pessoais: uma nova commodity, ligados ao direito à intimidade e a dignidade da pessoa humana. **Revista Jurídica** – Unicuritiba. v. 4, n. 49, Curitiba, p. 360-392, 2017. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2298/1428>. Acesso em 15 mar. 2021.

FRAZÃO, A. **Nova LGPD**: a importância do consentimento para o tratamento dos dados pessoais. Disponível em: <https://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: 12 abr. 2021.

FRAZÃO, A. **Nova LGPD**: as demais hipóteses de tratamento de dados pessoais. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/ -19092018>. Acesso em: 10 abr. 2021.

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

OLIVEIRA, A. P.; ZANETTI, D. LIMA, F. S.; SAMPAIO, T. O. A lei geral de proteção de dados brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**, ano 4, n. 1, maio, 2019.

SILVA, F. Gestão de identidades e acessos. *In*: CABRAL, C.; CAPRINO, W. (Orgs.).**Trilhas em segurança da informação, caminhos e ideias para a proteção de dados**. Rio de Janeiro: Brasport, 2015.

VERÍSSIMO, C. **Compliance**: incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva, 2017.