Como citar esse artigo:

GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica. **Coletâneas de artigosjurídicos: em homenagem ao Professor José Laurindo de Souza Netto**. Viviane C. de S. K., Adriane G., José L. de S. N. 1.ed., Curitiba: Clássica Editora, 2020. ISBN 978-65-87965-03-1. pg 319-344.

LEI GERAL DE PROTEÇÃO DE DADOS: DIRETRIZES E IMPLICAÇÕES PARA UMA SOCIEDADE PANDÊMICA

GENERAL DATA PROTECTION LAW: GUIDELINES AND IMPLICATIONS FOR A PANDEMIC SOCIETY

Adriane Garcel
Sergio Fernando Moro
José Laurindo de Souza Netto
Karen Paiva Hippertt

Resumo:
O presente estudo investiga as diretrizes da Lei Geral de Proteção de Dados (LGPD). A problemática versa sobre as mudanças acarretadas pela lei, sua entrada parcial em vigor em 18 de setembro de 2020, em plena pandemia e as principais implicações para a sociedade. Para tanto, utilizou-se a metodologia hipotético-dedutiva, baseada na pesquisa bibliográfica em livros e artigos científicos publicados em revistas especializadas, bem como na legislação brasileira e jurisprudência sobre o tema. Um dos resultados do presente trabalho está na constatação de que a LGPD representa marco na autodeterminação informativa, bem como pilar do uso correto de dados e dos direitos fundamentais dos titulares que irá atingir milhões de empresas, inclusive, não brasileiras, impondo inúmeras adequações estruturais e culturais. Adicionalmente, conclui-se que grande parcela das empresas brasileiras não está preparada para as mudanças, muitas sequer conhecem a lei. Por fim, como resposta à problemática proposta, evidencia-se a urgência de adequação das empresas às novas diretrizes, independentemente da discussão em torno da data de início de vigência integral da lei, diante do árduo desafio que terão de enfrentar para se adequarem.

Palavras-chave: Lei Geral de Proteção de Dados. Diretrizes. Implicações. Vigência.

Abstract:
This study investigates the guidelines of the General Data Protection Law (LGPD). The problem concerns the changes brought about by the law, its partial entry into force on September 18, 2020, in the middle of a pandemic and the main implications for society. For that, we used the hypothetical-deductive methodology, based on bibliographic research in

books and scientific articles published in specialized magazines, as well as in Brazilian legislation and jurisprudence on the subject. One of the results of the present work is the verification that the LGPD represents a milestone in the informative self-determination, as well as a pillar of the correct use of data and the fundamental rights of the holders, which will reach millions of companies, including non-Brazilian ones, imposing innumerable structural adaptations and cultural. Additionally, it is concluded that a large portion of Brazilian companies are not prepared for the changes, many do not even know the law. Finally, in response to the proposed problem, there is an urgent need to adapt companies to the new guidelines, regardless of the discussion around the date when the law will come into full force, given the arduous challenge they will have to face in order to adapt.

Keywords: General Data Protection Law. Guidelines. Implications. Validity.

INTRODUÇÃO

Na era da Big Data a informação tornou-se representação do próprio poder. A vida das pessoas passou a ser diretamente influenciada pela produção, armazenamento e tratamento massivo de dados. Atualmente a indústria do banco de dados direciona, inclusive, a tomada de decisões empresariais e políticas.

Em que pese à circulação das informações privadas beneficie em grande medida os setores, particularmente, a indústria de dados pessoais, a preocupação com relação aos riscos à pessoa humana é crescente, considerando a influência que têm na capacidade de autodeterminadação, fundamentação das decisões, hábito de consumo, entendimento social, político, cultural e a forma com que os usuários lidam com as informações.

Destarte, apesar de não expressamente assegurado na Constituição Federal, à proteção de dados é direito fundamental, já que o desenvolvimento pleno da personalidade implica a salvaguarda de um amplo rol de garantias fundamentais constitucionalmente asseguradas, dentre elas, a autodeterminação informativa contemplada na proteção de dados.

Com amplo espectro, o direito engloba diversos elementos sensíveis à proteção da pessoa humana, integridade física e moral, privacidade, personalidade da pessoa, liberdade e igualdade, o que sinaliza sua fundamentalidade.

Resultado de amplo debate, a Lei Geral de Proteção de Dados (LGPD), inspirada na legislação europeia (RGPD), traça o que virá a ser o pilar do uso correto dos dados conferindo-lhes tratamento adequado com salvaguarda da autodeterminação do usuário, atendimento de interesses legítimos e dos padrões de transparência, verificação e responsabilidade.

Os impactos serão os mais expressivos alcançados por qualquer legislação anteriormente edita no país e, além disso, a lei irá atingir todos os setores da economia com aplicação extraterritorial; milhões de empresas serão impactadas, produto e serviços terão de se adaptar à nova legislação.

Especialmente, com a pandemia do COVID-19 em que a coleta, armazenamento e processamento de dados da população em larga escala tornaram-se essenciais para diminuição do vácuo no conhecimento, possibilitando respostas céleres e eficientes, a discussão em torno do tema toma especial relevo (ALMEIDA et.al., 2020).

Na contemporaneidade pós-pandemia, a Lei Geral de Proteção de Dados terá papel de destaque ao colocar limites à captação, acesso, compartilhamento e utilização dos dados, resguardando os direitos fundamentais dos titulares.

Ocorre que, a adaptação do mercado e setor público tem sido inexpressiva e, ainda, 41% dos empreendedores sequer sabem do que se trata a LGPD, de acordo com dados do Reclame Aqui, além disso, o processo de adaptação é complexo, sem falar no imbróglio criado em torno da data em que passará a vigorar a lei.

Assim, o que se busca com o presente estudo é investigar as diretrizes da Lei Geral de Proteção de Dados e as mudanças por ela acarretadas, sua entrada em vigor e principais implicações para a sociedade.

Para tanto, a exposição se desenvolverá em três capítulos, para além da introdução e conclusão. Apresentar-se-á, primeiramente, a proteção de dados enquanto direito fundamental.

Na sequência, analisar-se-ão os fundamentos e princípios da Lei Geral de Proteção de Dados, tratando, também, da problemática em torno da *vacatio legis*; e, por fim, as implicações para a sociedade e análise do panorama geral de adequação por parte das empresas. Como encerramento, serão apresentadas, de forma sintética, as principais conclusões derivadas da pesquisa.

Para a elaboração, será utilizado o método hipotético-dedutivo, combinado aos procedentes de pesquisa bibliográfica e documental.

1. A PROTEÇAO DE DADOS COMO DIREITO FUNDAMENTAL

Desde o século XIX, com o advento da era da digitação e das novas tecnologias, as realidades social e jurídica sofreram transformações que levaram a sociedade industrial ao que

se tem hoje por “sociedade da informação” ou “sociedade em rede”, a chamada era da Big Data.

A alcunha se refere à sociedade contemporânea regida pelo paradigma tecnológico da tecnologia da informação refletido nas tecnologias, meios de comunicação em massa, particularmente, a internet (HARTMANN et. al, 2014).

Na “sociedade em rede” a multiplicação da capacidade de produção de dados é tão expressiva que a vida das pessoas, produção e relacionamentos é diretamente influenciada, rompida a fronteira público- privado.

O massivo uso da informação passou, inclusive, a direcionar a tomada de decisões empresariais e políticas, por meio da “indústria de banco de dados” (SOLOVE, 2004, p.19), que atua na facilitação da circulação de dados comercializados ou transmitidos por cessão, na grande maioria das vezes, de forma invisível, sem o consentimento ou conhecimento do usuário.

Um traço marcante da era digital resta refletivo nos fenômenos da *surveillance* e *dataveillance*, que, respectivamente, consistem na capacidade de vigia permanente, direcionada e metódica dos dados dos usuários com o intuito de protegê-los, direcionar, controlar ou dirigir e a aptidão para armazenamento de uma infinidade de dados pessoais para análise, com inúmeros fins.

O estudo e desenvolvimento tecnológico da empresa Target por meio da análise dos dados captados é exemplo interessante do mecanismo da *surveilance*. Os dados captados por mineração (*data mining*) passaram a compor banco de dados que, até os dias atuais, viabiliza o direcionamento do marketing da empresa que passou a se voltar aos hábitos consumeristas identificados no padrão de informações e interesses captados com precisão (PEGORARO JR. et.al, 2017, p. 21).

Apesar de a circulação das informações privadas beneficiar em grande medida os setores, particularmente, as indústrias de dados pessoais, a preocupação com relação aosriscos à pessoa humana é crescente, na medida em que influencia diretamente na capacidade de autodeterminadação, fundamentação das decisões, hábito de consumo, entendimento social, político e cultural.

Com a informação tornando-se representação do próprio poder, a edição de leis regulamentando especificamente o tema passou a ser crescente (BEDENDO; PEGORARO JR., 2018).

O ano de 1890 foi marcado pela doutrina de Warren e Brandeis, tratada no artigo “The Right to Privacy” publicado na Havard Law Review, que traz a privacidade como o “o direito

de estar só" ou "direito de ser deixado em paz", desvinculado da tutela da propriedade (WARREN; BRANDEIS, 2013).

No Século XX, com a transformação dos fins do Estado e revolução tecnológica, o caráter negativo e individualista do direito à privacidade foi substituído por um cateter positivo relacionado ao eixo "pessoa-informação-circulação-controle" (DONEDA, 2006, p.23).

Na Década de 70, o direito à privacidade passou a ocupar posição central na proteção da pessoa humana, diante do reconhecimento de que os dados são projeção da personalidade.

Em 1948, o art. 5º da Declaração Americana de Direitos e Deveres do Homem, passou a prever o direito à proteção contra violações abusivas à vida particular e familiar. No mesmo ano, a Declaração Universal dos Direitos Humanos, incluiu em seu art. 12 a proteção da privacidade. Em 1969, a Convenção Americana de Direitos Humanos passa a prever, em seu artigo 11, que ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada.

Entretanto, a disciplina da proteção de dados só veio a surgir no ano de 1960, nos Estados Unidos. Na sequência, estendeu-se para a Europa, particularmente, na União Europeia, local dos debates preliminares que resultaram na edição do Regulamento Geral de Proteção de Dados Pessoais Europeu.

Para DOENDA (2011) a matéria da Proteção de Dados apenas foi impulsionada "a partir da aplicação de determinadas concepções do direito à privacidade e da proteção da pessoa em face do desenvolvimento tecnológico. A própria expressão "proteção de dados" não reflete fielmente o seu âmago, pois é resultado de um processo de desenvolvimento do qual participaram diversos interesses em jogo".

No Brasil, à Constituição de 1988 confere proteção específica ao direito à privacidade que foi erigido ao patamar de Direito Fundamental e inserido em inciso específico no rol do artigo 5°, os incisos X e XII, que traz a proteção à intimidade, a vida privada, a honra e a imagem das pessoas, assegurando direito à indenização face eventuais danos decorrentes de violação (SARTORI, 2016, p. 72). No âmbito infraconstitucional, passou a ser previsto como direito da personalidade no artigo 21 do Código Civil. Contudo, a Constituição deixou de tratar especificamente acerca do direito à proteção de dados, distinto do direito à privacidade aqui abordado.

O Direito à Privacidade é direito humano fundamental que proíbe a interferência do Estado na vida privada, exceto nas hipóteses previstas em lei; envolve a inviolabilidade da intimidade, vida privada, honra, imagem, casa e do sigilo das telecomunicações.

Por sua vez, o direito a proteção de dados impõe o funcionamento de mecanismos de segurança que protejam o indivíduo que tem seus dados coletados, processados, armazenados e utilizados.

Apesar das diferenças, a positivação do direito à privacidade no rol dos direitos fundamentais da Constituição Federal reflete a preocupação do constituinte com o tratamento de dados com proteção de uma série de garantias fundamentais, como o direito à autodeterminação de dados e informações.

Na realidade, os dois direitos estão quase que umbilicalmente ligados, conforme explica DONEDA (2011, p. 94):

> a informação pessoal está, quase como ato reflexo, ligada à privacidade por uma equação simples e básica que associa um maior grau de privacidade a menor difusão de informações pessoais e vice-versa. Esta equação nem de longe encera toda a complexa problemática em torno dessa relação, porem pode servir como ponto de partida para ilustrar como a proteção das informações pessoais passou a encontrar guarida em nosso ordenamento jurídico: como um desdobramento da tutela dodireito à privacidade.

A PEC 19/2019, aprovada em primeiro turno na câmara dos deputados, objetiva exatamente a inclusão dos dados pessoais disponíveis em meio digital no rol das garantias individuais previstas na Constituição Federal, nos moldes da legislação e jurisprudência europeias, contudo ainda aguarda votação em segundo turno.

Não obstante, o Supremo Tribunal Federal na ADI 6387/DF, em julgamento paradigmático, reconheceu a fundamentalidade do Direito à Proteção de Dados ressaltando que os efeitos negativos da vigilância representam retrocesso às conquistas histórias, como a liberdade da pessoa humana.

Para a corte, a Constituição Federal expressamente assegura o direito à autodeterminação informativa, por isso o uso de dados e informações pessoais deve ser controlado pelo próprio indivíduo, conforme expressamente positivado na LGPD (Lei nº 13. 709/2018) em seu art. 2º, I e II. Não obstante, o direito à autodeterminação informativa e à privacidade são desmembramentos dos direitos da personalidade e subsidiam a proteção não só da democracia, mas também de uma série de direitos fundamentais previstos no art. 3º, I e II; art. 4º, II; art. 5º, X e XII; art. 7º, XXVII; e art. 219 da CF.

COÊLHO (2020) traz importante recorte acerca do tema:

> Os dados são o ativo e o legado do século 21, da "Era da Informação". Esse novo giro histórico requer do Estado a adequada e efetiva proteção dos cidadãos, da sua privacidade e da autodeterminação em relação aos seus dados pessoais. Constitui dever de um Estado Social e Democrático de Direito, garantidor da dignidade humana e de sua autodeterminação no campo informacional, livrar-nos de horizontes distópicos como aqueles imaginadas pelo escritor George Orwell, em sua obra "1984" ou na série televisiva "Black Mirror". (...) **Novos dados de realidade exigem o reconhecimento de novos direitos e o alargamento das garantias jurídicas com vistas a tutelar, com a máxima efetividade, a autodeterminação das pessoas e, ao fim e ao cabo, o direito à dignidade humana**. **Na Era da Informação**, inegável que o direito ao **sigilo** dos dados pessoais e **à autodeterminação** sobre eles seja **constitutivo de um direito mais amplo da dignidade e da personalidade humanas.**

Com amplo espectro, o direito engloba diversos elementos sensíveis à proteção da pessoa humana, integridade física e moral, privacidade, personalidade da pessoa, liberdade e igualdade, o que sinaliza sua fundamentalidade.

Além disso, enquanto direito fundamental autônomo, possui dupla dimensão, subjetiva ligada à defesa do indivíduo e objetiva relacionada ao dever de proteção Estatal. O Estado terá dever negativo de deixar de interferi no direito e o dever positivo de agir criando medidas para sua proteção. A eficácia irradiante ou horizontal, também chamada de *Drittwirkung,* ainda, estende tais deveres ao setor privado (SARLET, Ingo Wolfgang, 2012).

Destarte, "O direito fundamental à proteção de dados regula uma ordem de informação e comunicação" que "busca equilibrar os variados interesses de usos e direitos de proteção, de defesa e de participação do indivíduo nos processos comunicativos" (MENDES, 2014, p. 175).

Assemelha-se em muito ao direito da autodeterminação informativa consolidado já há muito tempo enquanto direito fundamental na Alemanha, dado seu amplo espectro de proteção que, aliás, o diferencia o direito fundamental à privacidade que possui âmbito de proteção mais restrito (MARTINS, 2016, p. 56).

A respeito das peculiaridades deste direito, ressaltou o Min. Gilmar Mendes ao proferir voto na Ação Direta de Inconstitucionalidade 6.389/DF de Relatoria da Ministra Rosa Weber:

> a autonomia do direito fundamental em jogo na presente ADI exorbita, em essência, de sua mera equiparação com o conteúdo normativo da cláusula de proteção ao sigilo. A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no

reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa.

Destarte, o desenvolvimento pleno da personalidade implica a salvaguarda de amplo rol de garantias fundamentais constitucionalmente asseguradas, como é o caso da autodeterminação informativa contemplada no direito fundamental à proteção de dados.

O âmago do direito à proteção de dados reside na vedação à coleta, processamento e circulação de dados irrestrita sem o consentimento do usuário, que impõe a estruturação de um sistema de segurança para proteção, garantindo a autonomia, autocontrole e autodeterminação do titular.

Por sua vez, o titular do direito fundamental é toda pessoa que realize qualqueroperação de tratamento de dados pessoais, seja organizações públicas ou privadas, pessoas físicas ou jurídicas (art. 1º, LGPD).

Não obstante a isso, os dados abrangidos pela proteção são quaisquer dados que levem à identificação de uma pessoa, não havendo que se falar em dados pessoais insignificantes ou neutros.

De outra banda, a discussão em torno do tema do direito fundamental à proteção de dados se justifica mais do que nunca. Com a pandemia do COVID-19, a coleta, armazenamento e processamento de dados da população em larga escala tornou-se medida imprescindível para embasar as respostas rápidas e adequadas à salvaguarda da vida.

Os esforços mundiais para diminuição do vácuo no conhecimento para respostascéleres e eficientes quanto à pandemia exige a captação de dados de boa qualidade dos mais diversos segmentos da sociedade para que as autoridades, especialmente, governamentais e sanitárias, possam se articular a partir da avaliação dos riscos e cenários.

Os dados permitem a compreensão não só do padrão epistemológico do vírus, mas também a estruturação de padrões matemáticos que servem de suporte às decisões (ALMEIDA et.al., 2020).

Os aplicativos que captam dados de geolocalização e circulação de pessoas, por exemplo, tornaram-se recorrentes na pandemia,

Diante de todo contexto exposto, questionamentos acerca das espécies, proporção de dados realmente necessária a se captar, acesso, compartilhamento e utilização dos dados, além de questões éticas, legais e técnicas vão se delineando no contexto da pandemia e são tratados adequadamente pela Lei Geral de Proteção de Dados.

Somado a isso, o panorama global aponta para a propensão de que os dados passem a ser utilizados para verificar o cumprimento do isolamento e quarentena, probabilidade de contágio e gerenciamento de permissões para sair de casa (ALMEIDA et.al., 2020), para além dos já conhecidos traços da era que ficou conhecida como Big Data.

Neste cenário, a LGPD terá importante papel na regulamentação do uso de dados pessoais no país, salvaguardando os direitos fundamentais dos titulares.

Além do panorama traçado, o tema mostra-se essencial, já que as empresas terão de se adaptar o quanto antes às diretrizes trazidas pela Lei de Proteção de Dados.

2. FUNDAMENTOS E PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

O desenvolvimento do tratamento autônomo de proteção dos dados deu lugar a diversas leis que passaram a regulamentar o assunto com o fim de obter um modelo jurídico rico e complexo (DONEDA, 2011, p. 98).

A despeito disso, o direito fundamental autônomo a proteção de dados deriva, no Brasil, da constatação dos riscos que o tratamento inadequado dos dados traz à proteção da personalidade da pessoa humana, não decorre de reconhecimento expresso na Constituição Federal da fundamentalidade do direito, como exemplificado no tópico precedente.

Hodiernamente, a Lei Geral de Proteção de dados (Lei nº 13. 709/ 2018) regulamenta a proteção de dados em âmbito nacional no país, conciliando a proteção da pessoa, interesse público e incentivo ao desenvolvimento econômico e tecnológico ligados à circulação da informação.

Após anos de debates, a LGPD reflete aquilo que vem a ser a espinha dorsal das regulamentações existentes acerca da proteção de dados que tratam das questões principais com as quais o ordenamento irá ter que lidar.

Ao longo do artigo 2º, a LGPD expõe seus fundamentos, respeito à privacidade e autodeterminação informativa; liberdade de expressão, informação, comunicação e opinião; inviolabilidade da intimidade, da honra e imagem; desenvolvimento econômico e tecnológico; inovação, livre iniciativa, concorrência e defesa do consumidor; direitos humanos, o livre desenvolvimento da personalidade, dignidade e o exercício da cidadania.

Em síntese, ao proteger a inviolabilidade da intimidade, honra, imagem e vida privada, a LGPD vislumbra a salvaguarda da privacidade; ao contemplar o direito ao controle e

proteção de dados pessoais, tutela a autodeterminação informativa. Também, preserva a liberdade de expressão, informação, comunicação, livre opinião, a liberdade de iniciativa e livre concorrência, com a defesa do consumidor; tutela a democracia, os direitos mais sensíveis da personalidade da pessoa humana e sua dignidade (SERPRO, 2020).

Não obstante, seu maior objetivo encontra-se na garantia de que a pessoa se cientifique acerca de quais dados estão sendo acessados, coletados e armazenados, para qual fim e por quem, o que fica evidente a partir da análise dos princípios que regulamentam a proteção de dados no país dispostos no art. 6º da Lei — boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

O princípio da boa-fé institui padrão ético de conduta pautado nos ideais de honestidade, lealdade e lisura, de modo a garantir a legitima confiança e expectativa (SILVA; SANTOS, 2011, p. 128).

Somado a ele, o princípio da finalidade impõe que a utilização dos dados se dê nos exatos moldes que haviam sido elencados no momento do recolhimento, com finalidade legitima, em conformidade com as normas que regulamentam o tratamento de dados do início ao fim (GEDIEL; CORRÊA, 2008, p. 147).

O princípio em questão delimita a transmissão dos dados a terceiros e institui critérios para a tratativa de dados, propósitos legítimos, específicos, explícitos e informados ao usuário, impedindo finalidades genéricas e indeterminadas por meio da realização de um juízo de ponderação entre a “utilização de determinados dados para certa finalidade" (DONEDA, 2011, p. 100).

Somado a isso, a motivação deverá condizer com a informação solicitada, presentes a pertinência e adequação com relação finalidade informada, conforme traça o princípio da adequação. O tratamento, ainda, deverá se limitar ao mínimo indispensável ao atendimento das finalidades com dados apropriados, não excessivos e proporcionais à finalidade, nos moldes do princípio da necessidade (art. 6º, III, da LGPD).

O princípio da proporcionalidade no uso de dados para alcance dos fins os quais se almeja deverá ser, igualmente, atendido.

Também, os dados armazenados precisam condizer com a realidade, assim a coleta e tratamento devem ser feitos de modo adequado com cuidado, correção e devida atualização (DONEDA, 2011).

Não obstante, o princípio do livre acesso assegura, como o próprio nome já diz, o livre acesso do titular e consulta facilitados à totalidade de seus dados, particularmente, com

relação a forma e duração do tratamento. O dono dos dados terá acesso às informações armazenadas, facultada a cópia dos registros e viabilizado o controle dos dados, podendo, inclusive, os retificar, suprimir e complementar com novas informações (BEDENDO; JUNIOR, 2010, p. 11).

Além disso, o responsável deverá informar o titular dos dados indicando as informações relevantes para o tratamento de dados, até mesmo quanto às especificidades, tais como às relacionadas à forma, fim e tempo de armazenamento dos dados (GEDIEL; CORRÉA, 2008, p. 147), nos exatos termos do trazido pelo princípio da transparência (ou da publicidade). Não só, como também, a LGPD assegura exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade deseu tratamento, conforme o princípio da qualidade dos dados impõe.

Malgrado, o princípio da segurança física e lógica impõe a necessidade de utilização de medidas técnicas e administrativas eficientes à proteção dos dados. Trata-se da implementação e gerenciamento de um sistema eficiente e abrangente de governança e gestão de riscos de segurança da informação que leve em conta a complexidade da problemática da proteção de dados.

O princípio da prevenção impõe, ainda, ao responsável pelos dados, a obrigação de que essas medidas e politicas qualitativas se deem previamente de modo qualitativo com o fim de evitar eventuais danos oriundos do tratamento dos dados.

Outrossim, os dados pessoais não poderão ser usados com o fim de promover discriminação do titular dos dados de qualquer natureza, raça, sexo, cor, idade e quaisquer outras formas (art. 3º, III e IV).

Caso o uso acarrete prejuízo ou viole quaisquer regras do ordenamento jurídico,ensejará responsabilização civil, nos termos do princípio da responsabilização que exige ainda, o acompanhamento pelas autoridades competentes do processamento dos dados impondo sanções quando houver descumprimento da lei. Paralelamente, o princípio da prestação de contas trata da necessidade de comprovação da adoção das medidas adequadas.

Conforme destaca ALMEIDA (et al., 2020, p. 2490), a "conformidade com as leis gerais de proteção de dados, portanto, requer tecnologia, infraestrutura e pessoal especializado para que os dados sejam tratados de forma lícita, justa e responsável em relação aos titulares".

Os dados abrangidos pela LGPD são quaisquer dados que estejam relacionados à pessoa situada no Brasil quando da coleta, independentemente da nacionalidade, do meio aplicado, país-sede do operador ou localidade dos dados. Além disso, abarca todos os setores da economia, com aplicação transversal, multisetorial e extraterritorial.

O âmbito de proteção da lei é tão alargado que ao conceituar o que vem a ser dado pessoal a LGPD engloba qualquer informação relacionada à pessoa natural identificada ou identificável, seja dado sensível ou não.

A exceção do alcance da lei fica por conta do rol do art. 4 da LGPD, excepcionados os fins exclusivamente particulares e não econômicos e os exclusivamente jornalísticos, artísticos, acadêmicos, bem como os exclusivos de segurança pública, defesa nacional, segurança de Estado ou atividade de investigação e repressão de infrações penais, além dos dados advindos de fora do país e que não sejam objeto de transferência internacional, desde que o país de onde derivarem disponha de proteção adequada.

Evidencia-se, assim, que a Lei Geral de Proteção de Dados trata-se de marco para a regulamentação dos dados pessoais no Brasil.

Entretanto, apesar de instituir importantes princípios e direitos aos seus titulares a *vacatio legis*, que em 2018 era de dois anos, foi postergada para agosto de 2020 por meio da Medida Provisória 696/2019, convertida na Lei 13.853/2019.

Na sequência, a grave recessão causada pela pandemia do COVID-19 levou a edição do PL 1.179/2020 que estabelece regime jurídico emergencial, ficando decidida, em sede de primeira votação, postergação para janeiro de 2021, a exceção da *vacatio* das multas esanções que ficariam para agosto de 2021.

O imbróglio não parou por aí, a Medida Provisória 959/2020 que passou a vigorar na data de sua publicação, 29 de abril do ano corrente, adiou a vigência da lei para maio de 2021. Até 27 de agosto do ano corrente a Medida deverá ser convertida em lei para que não caduque.

Quando ao PL 1.179/2020, o Senado acabou por suprimir o dispositivo que prorrogava a vigência da Lei, ficando mantida a prorrogação apenas no que se refere às sanções.

Neste contexto, verifica-se cenário de insegurança com dois resultados possíveis: “sem a MP convertida em lei a LGPD entraria em vigor em 16 de agosto de 2020 (vigência que era prevista antes do início da pandemia) ou, com a conversão em lei da MP, a LGPD entraria em vigor em 3 de maio de 2021” (TUMELERO, 2020).

Além disso, até o presente momento o executivo não criou a Autoridade nacional de proteção de Dados (ANPD) que tem a finalidade de fiscalizar a aplicação da LGPD.

Especialmente, em situações emergenciais e de interesse público, como no caso da pandemia do COVID-19, os dados se mostram essenciais para a adoção de políticas de enfrentamento, tornando-se a LGPD importante marco regulatório cuja vigência não pode

mais ser postergada, dado os prejuízos aos direitos e garantias fundamentais que tutela, isso sem falar nos prejuízos econômicos.

3. IMPLICAÇÕES PARA A SOCIEDADE

Resultado de amplo debate, ao longo de oito anos, a Lei Geral de Proteção de Dados, inspirada na lei europeia (GDPR), trará uma série de benefícios quando passar a vigorar no país, não tão somente por unificar e harmonizar as normas existentes, mas pela flexibilização no tratamento em tempos de Big Data, por possibilitar a portabilidade dos dados e, particularmente, habilitar o Brasil ao processamento dos dados oriundos de outros países que já contavam com regras rígidas.

Longe de obstaculizar por completo o uso de dados que se fazem tão importantes à contemporaneidade, a lei traça o que virá a ser o pilar para o uso correto dos dados conferindo-lhes tratamento adequado dentro das bases legais, com salvaguarda da autodeterminação do usuário, atendimento de interesses legítimos e dos padrões de transparência, verificação e responsabilidade.

Os impactos serão os mais expressivos alcançados por qualquer legislação nacional, especialmente no âmbito econômico e comercial. Inclusive, este foi um dos fatores que levou à edição da lei.

Com aplicação extraterritorial que abrange o Brasil, a regulamentação europeia de proteção de dados, *General Data Protection Regulation* (GDPR), compele as empresas, incluindo as Brasileiras com filiais nos países da União Europeia, a se adaptarem, impondo elevadas multas, além de barrar a transferência internacional de dados aos países que não possuem legislação que assegure o tratamento adequado de dados.

Somado a isso, o intuito de o Brasil entrar na Cooperação e Desenvolvimento Econômico sendo obrigado, para tanto, a cumprir com as regras impostas pela OCDE de edição de uma lei geral de tratativa de dados robusta, foi um dos fatores que levou à aprovação da LGPD. O escândalo da *Cambridge Analytica,* nos Estados Unidos, que tinha o intuito de atuar no Brasil foi, também, outro motivo para aprovação.

A despeito disso, a causa principal foi à tentativa de alteração da Lei do Cadastro Positivo para dispensar o consentimento do consumidor na coleta, compartilhamento e utilização dos dados. Os riscos envolvidos na aprovação pura e simples do texto base

alterando a Lei do Cadastro positivo fizeram com que a aprovação ficasse condicionada a edição prévia de uma lei geral tratando da proteção de dados.

Destarte, a Lei Geral de Proteção de dados veio a somar ao Marco Civil da Internet, que até então trazia diretrizes básicas e genéricas acerca do tratamento de dados pessoais, introduzindo no ordenamento regras mais específicas e robustas.

A Lei Geral de Proteção de dados atingirá todos os setores da economia com aplicação extraterritorial, garantindo um maior controle dos dados pessoais em um contexto de maior segurança jurídica e cibersegurança, além de assegurar maior paridade de armas na concorrência diminuindo, também, os empecilhos ao desenvolvimento econômico do país.

Nos negócios, a LGPD irá impactar milhões de empresas brasileiras que trabalham com dados que passarão a ter de, obrigatoriamente, adaptar-se a nova legislação.

A comunicação digital, a forma com que o dado é analisado, a relação dos consumidores com o comércio, adaptação da forma com que se dá o marketing, adequação das empresas que oferecem solução de gestão de dados que terão de desenvolver novas ferramentas de transparência, controle, *compliance* e transparência, contratar profissionais especializados e editar novas regulamentações, além da necessidade de readequação dosprofissionais ativos e já inseridos no mercado da gestão de dados, serão algumas das interferências causadas pela lei (MAIA, 2019).

Com o início da vigência da lei, os titulares dos dados terão seus direitos ampliados e contarão com arcabouço completo para a proteção de sua privacidade e liberdade, bem como recursos disponíveis para os casos de violações de segurança que impliquem o vazamento e exposição de dados.

O acesso aos dados, retificação, cancelamento, exclusão, oposição ao tratamento, informação e explicação acerca do uso, são apenas alguns dos direitos que passarão a ter os titulares, com destaque para a possibilidade de portabilidade.

Destarte, a LGPG amplia a segurança jurídica “a empresas e consumidores diante de maior transparência na coleta e tratamento de dados coletados tanto em meios presenciais quanto em meios digitais” (FENALAW, 2018). As empresas não mais poderão “usar ou coletar informações pessoais sem consentimento (...)” (FENALAW, 2018).

Conforme destaca Patrícia Linhares “a LGPD trouxe uma garantia muito representativa para o cidadão. Sabe-se, hoje, que em diversos segmentos comerciais e econômicos as informações pessoais são utilizadas para algumas inteligências de dados que não estão acessíveis e nem são aparentes aos próprios titulares desses dados” (FUNCEF, 2020).

As instituições de ensino, também serão impactadas pela nova legislação. A despeito das ressalvas contidas no art.4º, art. 7º, IV e art. 11, II, c, deverão implementar programas adequados e políticas internas com normas baseadas na LGPD, além de treinar os funcionários e readequar documentos dentro de um sistema de *compliance*. Os antigos bancosde dados, por exemplo, deverão ser revisados.

A Lei de Proteção de Dados, ainda, exige que todas as empresas e organizações fixem prazo de armazenamento de dados que deverão ser categorizados, fiscalizados e não mais poderão ser armazenados indefinidamente. Além, da imposição da adoção de medidas técnicas e organizacionais adequadas. Inclusive, todos os colaboradores e terceiros abrangidos no processo relativo aos dados, como um todo, terão de assinar termo de confidencialidade específico.

Destarte, evidente a necessidade de mudança cultural nas organizações que terão a responsabilidade no tratamento dos dados alargada pela lei.

Ainda, as entidades controladoras que tratam os dados deverão necessariamente indicar pessoa natural, Data Protection Officer (DPO), que ficará encarregada de operar como intermediária entre o controlador, os titulares dos dados e a Autoridade Nacional, como também fiscalizar o cumprimento das regras e orientar funcionários e contratados.

Também, deverá ser produzido o chamado relatório de impacto à privacidade, *Data Protection Impact Assessment* (DPIA), com detalhamento adequado dos procedimentos que podem acarretar riscos, mapeamento destes e medidas a serem tomadas no intuito de mitigação. Da coleta à exclusão, todas as atividades de tratamento deverão ser registradas,com indicação dos dados que foram coletados, informações referentes ao armazenamento, sua duração, finalidade, segurança e autorização legal (*data mapping*), para tanto, com adoção de medidas adequadas de segurança.

Todos os produtos, serviços e modelos de negócios terão de ser pensados e se estruturar para salvaguardar os dados, adequando-se aos princípios e padrões de segurança impostos pela lei.

Igualmente, recomendada adoção de código de conduta e certificação quanto ao cumprimento dos padrões estabelecidos na LGPD e pelos setores da sociedade, estes últimos habilitados a definir seus próprios padrões desde que previamente autorizados pela Autoridade competente.

Não obstante, ocorrendo algum incidente envolvendo a segurança da informação, obrigatória à notificação da Autoridade Nacional competente pela empresa, em prazo

adequado. A depender da gravidade da situação, a ANDP poderá notificar os titulares e dar ampla publicidade ao caso, o que certamente abalará a imagem da empresa.

Ainda, a LGPD viabilizada a transferência internacional de dados, mesmo em países sem níveis de proteção adequados, desde que autorizada pelo titular mediante consentimento especifico, de modo prévio e separado. Também, autorizada à transferência por meio da garantia do cumprimento do disposto na LGPD a partir de selos, certificados e códigos de conduta expedidos e creditados pela Autoridade Nacional.

Com a lei, controlador e operador passarão a ter responsabilidade solidaria com relação ao tratamento inadequado dos dados e incidentes envolvendo as informações, apesar de a responsabilidade do operador poder ser restringida às obrigações ligadas à segurança e dispostas no contrato.

Por fim, a Lei Geral de Proteção de Dados prevê sanções para eventuais violações às balizas postas que variam desde advertência e multas até proibição do tratamento de dados (total ou parcial). As multas poderão ser fixadas em importe correspondente a 2% do faturamento no último exercício, até R$ 50.000.000,00 (cinquenta milhões de reais) porinfração, com possibilidade de fixação *astreinte* até que se cessem as violações.

Sob a ótica da sociedade, a LGPD representa importante passo na autodeterminação informativa, já que conscientiza a coletividade do uso dos seus dados pessoais lhes fazendo compreender que, na realidade, são eles os verdadeiros detentores dos próprios dados e do poder de escolha envolvendo essas informações (FUNCEF, 2020).

Trata-se de um grande avanço na segurança dos dados pessoais no país que efetivamente salvaguarda a segurança, controle e privacidade dos dados pessoais a partir de um arcabouço normativo completo com normas claras e detalhadas, não só balizando otratamento de dados, mas também dispondo acerca dos direitos dos usuários e medidas a serem tomadas diante de eventuais riscos.

Conforme destaca Fernando Santiago (2020), o início da vigência da lei constitui "marco para vida tanto das empresas, como dos entes públicos. Isto porque, os dados pessoais que antes eram tratados de forma quase artesanal pelas empresas, sem a devida atenção, passam agora ser tutelados pelo direito, razão pela qual devem ser manuseados com ascondições estritas prevista na lei".

Apesar do avanço, a adaptação do mercado e setor público tem sido inexpressiva, o que gera preocupações. É o que aponta pesquisa realizada pela ICTS Protiviti (2020) que apurou que 58% das pequenas empresas ainda não se adaptaram para cumprir a lei e o

Reclame Aqui (2019) que apurou que mais de 41% dos empreendedores sequer saber do que se trata a LGPD.

Até então, no setor privado, dois posicionamentos vêm sendo adotados: empresas que buscam se adequar e, outras, que fazem contas para verificar se não sairia mais lucrativo descumprir a lei; ainda, há aquelas que adotam postura passiva de tentar apenas evitar problemas sem olhar para o futuro.

Para Tony Debos (in ÉPOCA NEGÓCIOS, 2019), o processo de adaptação não é simples e o Brasil não está preparado para a nova legislação. A despeito disso, nos Estados Unidos e Europa, que ainda estão em processo de transição, a situação foi a mesma.

De fato, o processo de transição é árduo, para as pequenas e médias empresas a principal dificuldade diz respeito aos elevados custos envolvidos na adaptação, já para as empresas com modelos de negócio complexo são os dados sensíveis que preocupam, a incorporação dos princípios de proteção de dados às missões e valores da empresa e a abrangência das adequações são outros desafios que tem barrado a implementação das mudanças (KAFRUNI, 2020).

De qualquer forma, a adaptação é necessária e as empresas que se adequarem irão se tornar mais competitivas e abertas a negociar internacionalmente, além de não terem de arcar com os prejuízos oriundos do descumprimento da legislação que certamente serão mais custosos do que o investimento na transição para o novo modelo.

O problema é que a ausência de planejamento generalizado imporá a necessidade de adaptação às pressas de todo um setor público e privado, que não se antecipar às mudanças, quando da entrada em vigor da lei.

Além disso, a grave recessão causada pela pandemia do COVID-19, um dos fatores determinantes para o adiamento do início da vigência de parte da legislação, não pode mais ser tida como obstáculo ao início da vigência da lei diante dos impactos econômicos que uma nova prorrogação poderia representar, apesar da árdua tarefa que a adequação em tempo recorde em meio a grave recessão causada pela pandemia poderia representar (CORTEZ, 2020).

Destarte, as empresas precisam se antecipar com urgência aos novos parâmetros impostos pela LGPD sem contar com a data de vigência da lei.

CONCLUSÃO

Diante de um cenário global de utilização desenfreada de dados pessoais, particularmente, agravado em virtude da pandemia do COVID-19, a Lei Geral de Proteção de Dados foi passo imprescindível à salvaguarda dos direitos fundamentais dos titulares dos dados.

Longe de obstaculizar o uso de dados que se fazem tão importantes à contemporaneidade, a lei traça o que virá a ser o pilar para o uso correto dos dados conferindo-lhes tratamento adequado com salvaguarda da autodeterminação do usuário, atendimento dos interesses legítimos e dos padrões de transparência, verificação eresponsabilidade.

Resultado de amplo debate, a Lei Geral de Proteção de Dados possui aplicação transversal, multisetorial e extraterritorial, atingindo milhões de empresas, inclusive, as não brasileiras, que terão de se adequar às novas exigências que envolvem: a forma com que se dá a comunicação digital, o marketing, com que os dados são analisados e se dá a relação com consumidores e o comércio. A exceção do alcance da lei se dá apenas nas hipóteses rol do art. 4.

As alterações impulsionadas pela nova legislação envolvem a adoção de novas ferramentas de transparência, controle e *compliance*, conjuntamente com a contratação de profissionais especializados e adequação dos já inseridos no mercado (MAIA, 2019). A contratação de empresa terceirizada para realizar a transição seria, também, outra opção.

Inúmeras serão as adequações que implicam gastos elevados em meio a uma crise sem precedentes, por isso os dados apontam que as empresas brasileiras não estão se preparando para as mudanças. Muita, inclusive, tem feito cálculos para averiguar se não seria mais vantajoso arcar com as multas oriundas do descumprimento da lei.

Para as pequenas e médias empresas a principal dificuldade diz respeito aos elevados custos envolvidos na adaptação, já para as empresas com modelos de negócio complexo são os dados sensíveis que preocupam, a incorporação dos princípios de proteção de dados às missões e valores da empresa e a abrangência das adequações são outros desafios que tem barrado a implementação das mudanças.

A transição é complexa, já que inúmeras são as exigências da lei que impõe que as empresas passem a fixar prazos de armazenamento de dados, os quais deverão ser categorizados e fiscalizados; nomeiem um intermediário entre o controlador, os titulares dos dados e autoridade nacional que fiscaliza o cumprimento das regras, o chamado DPO; produzam relatórios de impacto de privacidade (DPIA), detalhando, inclusive, os procedimentos que podem acarretar risco, os mapeando e indicando medidas a serem

adotadas; registrem todas as atividades de tratamento com detalhamento (dados que foram coletados, informações de armazenamento, duração, finalidade, segurança, autorização legal e indicação da adoção de medidas adequadas de segurança); adotem de código de conduta e certificação que garanta o cumprimento da LGPD; e, em caso de incidente a autoridade competente deverá ser notificada.

Em síntese, toda a cultura e estruturação por de traz dos produtos, serviços e modelos de negócio terão de ser repensadas, trazendo maior segurança aos consumidores e empresas, com um tratamento de dados mais transparente.

Além disso, os titulares dos dados terão seus direitos ampliados e contarão com arcabouço completo para a proteção de sua privacidade e liberdade, bem como medidas em casos de violações de segurança. Acesso aos dados, retificação, cancelamento, exclusão, oposição ao tratamento, informação e explicação acerca do uso, são apenas alguns dos direitos que passarão a ter os titulares, com destaque para a possibilidade de portabilidade.

A LGPD, ainda, autoriza a transferência internacional de dados, mesmo em países sem os níveis de proteção adequados, mediante autorização específica do titular, de modo prévio e separado.

Outra mudança, diz respeito à responsabilidade do controlador e operador, com relação ao tratamento dos dados e incidentes envolvendo informações, que passará ser solidária, não obstante haja a possibilidade de limitar a responsabilidade do operador às obrigações contratuais e ligadas à segurança.

Não obstante, a lei prevê sanções para eventuais violações às balizas postas quevariam desde advertência e multas até proibição do tratamento de dados (total ou parcial).

Tratar-se, assim, de importante passo na autodeterminação informativa, uma vez que conscientiza a população acerca do uso dos dados pessoais e sua titularidade, contudo com árduo processo de transição diante da necessidade de investimento em tecnologia,infraestrutura, pessoal especializado e mudança de cultura.

Somado a isso, há todo um imbróglio criado em torno do prazo de *vacatio* legis, sobretudo em razão da crise do COVID-19.

O PL 1.179/2020, que estabelece regime jurídico emergencial postergando a data de vigência da lei, cujo prazo de *vacatio* era de dois anos, para janeiro de 2021, a exceção da *vacatio* das multas e sanções que ficariam para agosto de 2021, foi aprovado em primeira votação. Ato contínuo, o Senado acabou por suprimir o dispositivo que prorrogava a vigência da Lei, ficando mantida a prorrogação apenas no que se refere às sanções.

De outro vértice, a Medida Provisória 959/2020, que passou a vigorar na data de sua publicação, 29 de abril do ano corrente, adiou a vigência da lei para maio de 2021. Até 27 de agosto do ano corrente a Medida deverá ser convertida em lei, do contrário caducará.

Neste contexto, verifica-se cenário de insegurança em que a lei poderá entrar em vigor já em agosto do ano corrente, ou apenas em maio do ano que vem.

Apesar disso, a discussão acerca da data exata de vigência da lei torna-se, de certo modo, irrelevante diante do árduo desafio que as empresas terão para se alinharem ao novo regramento.

Se passar a vigorar agora, as empresas que não se adequaram terão desafio impensável pela frente. Por outro lado, caso passe a vigorar no próximo ano, a adequação prévia também se mostra de extrema urgência.

De qualquer forma, considerando o uso maciço de dados característico da era da Big Data e, agora, essencial para que se evite o agravamento da pandemia, somado à dilação já concedida e os impactos econômicos de eventual alargamento de prazo, verifica-se que a crise do COVID-19 não pode mais ser tida como fator que venha a impedir o início da vigência da lei que deve passar a vigorar o quanto antes.

REFERÊNCIAS

ALMEIDA, Bethania de Araujo et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciência & Saúde Coletiva**, v. 25, p. 2487-2492, 2020.

BARROSO, Luis. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente adequada do Código Civil e da Lei de Imprensa. Disponível em: https://www.migalhas.com.br/arquivo_artigo/art_03-10-01.htm. Acesso em: 09 set. 2020.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. Webinário A aplicação da Lei Geral de Dados Pessoais no cotidiano do Poder Judiciário e do STJ. Disponível em: https://www.youtube.com/watch?v=uhLLtb2AINM. Acesso em: 21 set. 2020

BEDENDO, Thaynara Zanchin; JUNIOR, Paulo Roberto Pegoraro. Lei Geral de Proteção de Dados Pessoais nas Relações do Comércio Eletrônico (LEI N. 13.709/2018). Disponível em: https://d1wqtxts1xzle7.cloudfront.net/63296745/LEI_GERAL_DE_PROTECAO_DE_DADOS_PESSOAIS_NAS_RELACOES_DO_COMERCIO_ELETRONICO20200513-98717-2hqhqj.pdf?1589377796=&response-content-disposition=inline%3B+filename%3DLei_Geral_de_Protecao_de_Dados_Pessoais.pdf&Expires=1598031953&Signature=boD2mn19Oye~gT3V3h1wKdFV2QJlhPfqb4DfNhhberdNER1rQ05AqyYZufHMjtkmaM0YvemmpjN4EGsj7A3gYv269JLtbNgu1qr3u6am~umZJYRAxVKr6bFfG0ftnccyoJptwp8IzbgSvU6VoG2nLqTcTW4u

RmEAbAP76rZMIZifKcj73oYR9MTbBmKy1LASG2qsy0GjAxoaJGxX57OzM5rSFK7tJnO
VULxANJOuaEqtMrpNLyS6T2lxbRU0QaVWLvgwPtQkGqcWhtJH65NMxLCM38exVCIa
dBj5vyMXWA1gjalTbKj~jtOP4x8VuyIxEgC7ijT9kBMRsuJKrY1Q__&Key-Pair-Id=APKA
JLOHF5GGSLRBV4ZA. Acesso em: 21 ago. 2020.

CARDOSO, Ana Paula. Pesquisa: 41,6% das empresas não sabem o que é LGPD**. Blog Reclame Aqui.** Disponível em: https://blog.reclameaqui.com.br/pesquisa-416-empresas-naosabem-que-e-lgpd/. Acesso em: 21 ago. 2020.

COÊLHO, Marcus Vinicius Furtado. O direito à proteção de dados e a tutela da autodeterminação informativa. **Consultor Jurídico**, 2020. Disponível em: https://www.co
njur.com.br/2020-jun-28/constituicao-direito-protecao-dados-tutela-autodeterminacao-infor
mativa. Acesso em: 21 ago. 2020.

CORTEZ, Frederico. O setor público está preparado para LGPD?. **Focus.jor**, 2020. Disponível em: https://www.focus.jor.br/o-setor-publico-esta-preparado-para-lgpd-por-frederico-cortez/. Acesso em: 21 ago. 2020.

DONEDA, Danilo. Um código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil, Rio de Janeiro**, v. 16, p. 117, 2003.

FENALAW/DIGITAL. LGPD e seus impactos na sociedade. **Fenalaw**, 31 ago. 2018. Disponível em: https://digital.fenalaw.com.br/legisla-o/lgpd-e-seus-impactos-na-sociedade. Acesso em: 21 ago. 2020.

FLAUTO, Fernando. Crowe, 2019. **Estamos preparados para a Lei Geral de Proteção de Dados?.** Disponível em: https://crowemacro.com.br/insight/insights-tecnologicos/estamos-preparados-para-a-lei-geral-de-protecao-de-dados/. Acesso em: 21 ago. 2020.

FUNCEF. Os impactos da LGPD nas nossas vidas. **Funcef.com.br**. Curitiba, 28 jan. 2020. Disponível em: https://www.funcef.com.br/portal/menuprincipal/comunicacao/os-impactos-da-lgpd-nas-nossasvidas.htm#:~:text=Quando%20a%20esmola%20%C3%A9%20demais,as%20consequ%C3%AAncias%20podem%20ser%20desastrosas.

GARCEL. Adriane; MORO. Sergio Fernando. Data Protection Law and its Interactions With The Anti-Money Laundering Law. VII Simpósio Internacional de Direito Consinter / Universidad de Computense de Madrid. 17 a 19 de novembro de 2020 - Revista Internacional CONSINTER de Direito. Disponível em: https://revistaconsinter.com/..

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola, p.146. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. **Revista da Faculdade de Direito UFPR**, v. 47, 2008.

GÊNESES IT CONSULTING. **Está preparado para a LGPD – Lei Geral de Proteção de Dados?**. Disponível em: https://geneses.com.br/lgpd-lei-geral-de-protecao-de-dados/. Acesso em: 21 ago. 2020.

HARTMANN, Ivar Alberto Martins et al. A sociedade-rede e o estado- rede. **Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação**, v. 1, n. 2, p. 2-47, 2015.

ICTS. 58% das pequenas empresas não estão preparadas para a LGPD**. icts.com.br**, 2020. Disponível em: https://icts.com.br/icts-news/58-das-pequenas-empresas-nao-estao-preparadas-para-a-lgpd. Acesso em: 21 ago. 2020.

JUNIOR, Paulo Roberto Pegoraro et al. Responsabilidade Civil e a surveillance: as commodities digitais e o risco da atividade**. In:** Revista Judiciária do Paraná/ Associação dos Magistrados do Paraná. — v.1, n.1—, (jan.2006) — .— Curitiba: AMAPAR, 2006.

_____. Liberdade de Expressão e Capacidade Comunicativa. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 12, n. 39, p. 145-183, 2018.

KAFRUNI, Simone. Mais da metade das empresas não está pronta para lei de proteção de dados. **Correio Brasiliense:** 17 fev. 2020. Disponível em: https://www.correiobraziliense.com.br/app/noticia/economia/2020/02/17/internas_economia,828562/mais-da-metade-das-empresas-nao-esta-pronta-para-lei-de-protecao-de-da.shtml#:~:text=Os%20brasileiros%20ter%C3%A3o%20um%20importante,o%20Brasil%20n%C3%A3o%20est%C3%A1%20preparado. Acesso em: 21 ago. 2020.

MAIA, Adriane. Os impactos da LGPD para os negócios. **E-commercebrasil**, 2019. Disponível em: https://www.ecommercebrasil.com.br/artigos/os-impactos-da-lgpd-para-os-negocios/. Acesso em: 21 ago. 2020.

MARTINS. Leonardo**. Tribunal Constitucional Federal Alemão: decisões anotadas sobre direitos fundamentais.** Volume 1: dignidade humana. Livre desenvolvimento da personalidade, direito fundamental à vida e à integridade física e igualdade. São Paulo: Konrad-Adenauer Stiftung – KAS. 2016. P. 56

MENDES, Laura Schertel; DONEDA, Danilo. Marco jurídico para a cidadania digital: uma análise do Projeto de Lei 5.276/2016. **Revista de Direito Civil Contemporâneo-RDCC (Journal of Contemporary Private Law)**, v. 9, p. 35-48, 2016.

MIZIARA, Raphael. LGPD: razões de sua existência e impactos nas relações de emprego. **Jota**, 15 mar 2020, 08: 32. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/lgpd-razoes-de-sua-existencia-e-impactos-nas-relacoes-de-emprego-15032020. Acesso em: 15 mar. 2020.

MOURA, Marcelo. O Brasil não está pronto para a Lei Geral de Proteção de dados. **Época Negócios**, 2 nov 2019, 6h00. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/11/o-brasil-nao-esta-pronto-para-lei-geral-de-protecao-de-dados.html. Acesso em: 21 ago. 2020.

MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados do Brasil – Análise**. Disponível em: file:///C:/Users/dell/Downloads/artigo-baptista-luz-pt-lei-geral-de-Protec%CC%A7a%CC%83o-de-dados-do-Brasil%20(5).pdf. Acesso em: 21 ago. 2020.

MORO, Sergio Fernando. Rumo a Nogales. In: Revista Crusoé, n.º 114, 03/07/2020, disponível em https://crusoe.com.br/edicoes/114/rumo-a-nogales/. Acesso em: 20 set. 20202

PEGORINI, Maria Fernanda Hosken et al. Lei Geral de Proteção de Dados: um resumo da LGPD (ATUALIZADO). **Legalcloud**, 2018. Disponível em: https://legalcloud.com.br/lei-geral-de-protecao-de-dados-resumo-lgpd/. Acesso em: 21 ago. 2020.

PEIXOTO, Andréa Stefani. Lei de Proteção de Dados: entenda em 13 pontos!. **Politize**, 2020. Disponível em: https://www.politize.com.br/lei-de-protecao-de-dados/. Acesso em: 21 ago. 2020.

REDE NACIONAL DE ENSINO E PESQUISA. **Qual o impacto da LGPD em instituições de ensino e pesquisa?.** Disponível em: https://www.rnp.br/noticias/qual-o-impacto-da-lgpd-em-instituicoes-de-ensino-e-pesquisa. Acesso em: 21 ago. 2020.

SARLET, Ingo Wolfgang. Neoconstitucionalismo e influência dos direitos fundamen tais no direito privado. civilistica. **In:** revista eletrônica de direito civil, v. 1, n. 1, p. 1-30, 2012.

SARTORI, Ellen Carina Mattias; BAHIA, Cláudio José Amaral. Big Brother is watching you: da distopia orwelliana ao direito fundamental à proteção de dados pessoais. **Revista de Direitos e Garantias Fundamentais**, v. 20, n. 3, p. 225-248, 2019.

SERPRO. **Objetivo e abrangência da LGPD**. Disponível em: https://www.serpro.go v.br/lgpd/menu/tratamento-dos-dados/objetivo-e-abrangencia-da-lgpd#:~:text=A%20 Lei%20Geral%20de%20Prote%C3%A7%C3%A3o,da%20personalidade%20de%20cada%20 indiv%C3%ADduo. Acesso em: 21 ago. 2020.

SILVA, Michael César; SANTOS, Wellington Fonseca. O direito do consumidor nas relações de consumo virtuais. **Revista da Faculdade Mineira de Direito**, v.15, n. 30, jul./dez. 2012 – ISSN 1808-9429. Disponível em: http://periodicos.pucminas.br/index.php/Direito/article/vi ew/P.2318-7999.2012v15n30p119. Acesso em: 25 mar. 2020.

SILVESTRE, Gilberto Fachetti; BORGES, Carolina Biazatti; BENEVIDES, Nauani Schades. The procedural protection of data de-indexing in internet search engines: the effectiveness in brazil of the so-called “right to be forgotten” against media companies. Revista Jurídica - UNICURITIBA, v. 1, n. 54, mar. 2019. p. 25 - 50

SUPERIOR TRIBUNAL DE JUSTIÇA. Webinário “A aplicação da Lei Geral de Dados Pessoais no cotidiano do Poder Judiciário e do STJ. Disponível em: https://www.youtube.com/watch?v=uhLLtb2AINM. Acesso em: 21 set. 2020

SOCIALGOODBRASIL**. Privacidade e proteção de dados pessoais: o impacto da Lei Geral de Proteção de Dados Pessoais na sociedade**. Disponível em: https://so cialgoodbrasil.org.br/2019/05/13/privacidade-e-protecao-de-dados-pessoais-o-impac to-da-lei-geral-de-protecao-de-dados-pessoais-na-sociedade/. Acesso em: 21 ago. 2020.

SOLOVE, Daniel**. The Digital Person. Technology and Privacy in the Information Age**. New York: New York University Press, 2004, p. 19.

SPIECKER, Indra. O direito à proteção de dados na internet em caso de colisão. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 12, n. 38, p. 17-33, 2018.

UNIÃO EUROPEIA. 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. Luxemburgo, out 1995.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **civilistica. com: revista eletrônica de direito civil**, v. 2, n. 3, p. 1-22, 2013.

ZANATTA, Rafael A.F. b A proteção dedados pessoais entre leis, códigos e programação: limites do marco civil da internet. **In:** DE LUCCA, Newton et al. Direito e Internet III: Marco Civil da Internet. São Paulo: Quartier Latin, 2015, p. 447- 470.