FUNDAMENTOS EM PROTECAO DE DADOS E PRIVACIDADE EM TEMPOS DE NOVO CORONAVIRUS (COVID-19)

Aparecida Angelica de Sousa Fraga, Advogada socia da empresa Sousa Fraga Assessoria Juridica e Empresarial, especialista em processo civil e civil, e direito empresarial, Trabalhista, conciliadora e mediadora no Tribunal de Justica do Rio de Janeiro.

RESUMO

Este artigo apresenta uma discussão teórica que parte das descobertas realizadas em uma pesquisa no aumento de Fake news nesse periodo de pandemia a que tem como objetivo investigar a ação de tutoria em ambientes virtuais de aprendizagem no âmbito a série de artigos sobre a LGPD, busca-se neste artigo analisar os fundamentos em Proteção de Dados e Privacidade, contextualizando com o momento atual - pandemia do novo coronavírus (COVID – 19). Tendo como base a epistemologia da complexidade à pesquisa que serve como base para este trabalho possibilita uma articulação entre as concepções relacionada à Lei Geral de Proteção de Dados Pessoais - LGPD - Lei nº 13.709 foi sancionada em 14 de agosto de 2018 após mais de oito anos de debate na sociedade civil, já vindo a sofrer constantes ameaças teve a prorrogação de seu prazo de vigência, como se os 24 (vinte e quatro) meses nela previstos não fossem suficientes para a adaptação das pessoas físicas e jurídicas para proporcionarem a proteção dos dados pessoais que estejam tratando ou que venham a tratar.

A LGPD dispõe sobre os direitos fundamentais de liberdade e de privacidade, bem como, assegura o livre desenvolvimento da personalidade da pessoa natural.

A LGPD se aplica a qualquer pessoa natural ou jurídica de direito público ou de direito privado que utilize dados pessoais - colete, armazene, compartilhe - inclusive nos meios

digitais. O âmbito de aplicação material abrange a maior parte de projetos e atividades de empresas. Sobre docência, tutoria e ação educativa virtual que evocam a emergente necessidade da complexidade na compreensão dos fenômenos da experiência humana que se manifestam nos processos de comunicação entre o Controlador e os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados. Emergência de um olhar complexo que surge principalmente no contexto atual da educação à distância, modalidade que tem aberto possibilidades para a divisão da ação educativa implicando fragmentações na docência, em virtude a pandemia surgiram adaptacao de aulas virtuais com as instituições de ensino.

O presente artigo propõe uma discussão teórica que tem como base as pesquisas realizadas a antiga Medida Provisória 869/2018, instituída ainda em dezembro do ano passado, surgiu com o propósito de alterar o marco regulatório do Brasil sobre proteção de dados, sendo, desde então, veiculado de forma incisiva pela mídia em geral, sobretudo por seu teor possuir grande efeito nas relações entre sujeitos de Direito.

Isso porque a medida (convertida na Lei 13.853/2019, sancionada em 8 de julho deste ano) prevê a criação da Autoridade Nacional de Proteção de Dados – ANPD, que altera sensivelmente a própria Lei Geral de Proteção de Dados (13.709/2018).

Palavras-chave: LGPD - Lei nº 13.709 foi sancionada em 14 de agosto de 2018, prorrogação do prazo de vigência da lei geral de proteção de dados pessoais – LGPD, situação de pandemia, direitos fundamentais de liberdade e de privacidade, ação preventiva, complexidade.

INTRODUÇÃO

A globalização, que também pode ser compreendida no berço da pós-modernidade como uma das grandes causas das transformações sociais nos últimos anos, é descrita por Warschauer (2006, p.34), como a nova economia global em que o capital, a produção, a administração, a mão de obra, os mercados, a tecnologia e as informações são organizados em uma relação que vai além das fronteiras nacionais, gerando redes transnacionais de empresas, implicando transformações sociais e uma educação virtual a conscientização e aplicabilidade da LGPD - Lei Geral de Proteção de Dados.

Segundo alguns teóricos, a sociedade já vive em uma realidade orientada e governada por algoritmos. Em muitas plataformas *on-line*, a navegação dos consumidores é direcionada para conteúdos selecionados pelos algoritmos,conforme as suas supostas predileções, porque quanto mais tempo o indivíduo gastar em um determinado site ou rede social, mais dinheiro é gerado para aquela plataforma eletrônica.

Por outro lado, algoritmos não são suficientemente transparentes ou bem compreendidos, além de selecionarem conteúdos de forma automatizada. Dessa forma, a vida na sociedade hiperconectada é permeada por decisões automatizadas, e vários dos tratamentos algoritmos automatizados são feitos por inteligências artificiais. Ocorre que cada vez mais foge do nosso controle saber como os algoritmos estão chegando àquelas conclusões em cada caso. Para pirar a situação, os algoritmos também estão ficando mais complexos, por causa das técnicas de "*machine learning*", "*deep learning*" e "*neural learning*". Atualmente, já existem algoritmos complexos que se auto programa, sem imputs lógicos dos seres humanos, propondo novas saídas para diversos problemas.

A esse respeito, as empresas de tecnologia devem assumir a responsabilidade de acompanhar a capacidade de autoconstrução dos algoritmos e auto evolução da inteligência artificial, principalmente tentando olhar para uma regulação "*by design*", pensando na privacidade durante toda a concepção daquela nova tecnologia. Portanto, uma vez identificados os potenciais desafios dessa nova realidade, é preciso identificar a resposta jurídica para esses problemas na atualidade. Nesse contexto, buscam-se modelos regulatórios para disciplinar a proteção dos dados pessoais, sem impedir que inovações legítimas beneficiem a sociedade .

O país encontra-se em um momento de particular efervescência em relação ao tema, já que a entrada em vigor da nossa Lei Geral de Proteção de Dados (LGPD), que estava prevista para agosto deste ano, poderá ser adiada para Janeiro de 2021 — conforme o *projeto de lei do Senado nº 1.179/2020.* Ainda assim, uma análise à luz da LGPD pode ser muito didática: afinal, é o regime jurídico que reflete a vontade soberana da população traduzida pelos seus representantes eleitos, é uma lei que representa a *culminação de um processo de anos de debat*e com a sociedade civil e carrega disposições específicas que permitem uma reflexão mais profunda sobre o tema.

No caso do atual coronavírus, podemos pensar em um cenário hipotético em que, após o período mais grave da curva de infecções, um governo pretenda implementar um regime controlado de circulação em cidades para promover a infecção paulatina e, consequentemente, a imunização controlada da população sem sobrecarregar o sistema de saúde. Para tanto, utilizam-se dados epidemiológicos e populacionais dos bairros, dados de movimentação obtidos de companhias telefônicas e *apps* de transporte de passageiros, além de dados coletados a partir de programas de desconto de medicamentos em uma parceria com farmácias locais.

A existência de um robusto sistema de proteção de dados fundado nos direitos do titular e em princípios e fundamentos cujas raízes últimas são os mandamentos constitucionais — de proteção à intimidade, de garantia da liberdade de informação e expressão, entre outros — demarcaria com clareza as linhas intransponíveis da arbitrariedade do Estado e da atividade das empresas. Seria o eixo em cima do qual construiríamos o difícil, porém necessário equilíbrio entre a proteção da saúde da população, a esfera íntima individual e a soberania sobre dados pessoais que, especialmente em nossa sociedade profundamente e ubiquamente conectada, compõem uma face real da própria personalidade.

Assim sendo, considerando a importância do tema, este artigo terá por objetivo a análise da perspectiva brasileira a respeito da proteção de dados pessoais, e sem mecanismos imediatos de fiscalização e resposta a erros graves e abusos, a proteção de dados está à deriva a LGPD. Em analise normativa que garanta o nível de proteção aludido não engessará ou impedirá o caráter autorregulatório da maioria das iniciativas tecnológicas. Pelo contrário,

incentivará a criatividade e a novidade, assim como a neutralidade da rede, na medida em que estabelecerá regras claras para todos os jogadores do mercado.

Sob este contexto, o artigo objetiva analisar o atual cenário legislativo brasileiro, investigando a necessidade de um marco legal específico a reger a matéria. O estudo de fundamentos em proteção de dados e privacidade em tempos de novo coronavirus voltado para a abordagem dos principais aspectos do Anteprojeto de Lei de Proteção de Dados Pessoais (ALPDP).

FUNDAMENTOS DA LGPD

O Brasil, na contramão a muitos de seus pares no cenário mundial, ainda não dispõe de proteção adequada para dados de natureza pessoal. Ainda que se considerem as proteções à intimidade e à privacidade estabelecidas pela Constituição Federal de 1988 (CF/1988), pelo Código Civil (CC), pela Lei de Acesso à Informação (Lei nº 12.527/11); e o amparo aos dados relativos a processos de consumo (nos ditames trazidos pelo Código de Defesa do Consumidor/CDC), ainda se está muito distante do nível de adequação garantido por legislações alienígenas, como as da Comunidade Europeia, do Canadá, da Argentina, do México, do Uruguai, do Peru, do Chile e dos Estados Unidos da América.

A Lei Geral de Proteção de Dados aprovada no Brasil (Lei 13.709/2018) registra de forma inequívoca a necessidade de interesse legítimo e autorização para coleta de dados, nos moldes do artigo 6º da lei:

"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.

Assim remetemos a ótica da LGPD?

Houve consentimento para a coleta e uso destes dados?

Quem está analisando softwares, permissões de acesso, possibilidades de cópia, transferência e backups dos dados armazenados na empresa?

Percebam que estamos muito distantes de comprar um software de segurança de dados, firewall e outros e resolver o problema.

Temos aqui a clássica dicotomia: Gestão ou tecnologia? A resposta ao meu sentir é: AMBOS, mas primeiro a gestão, depois a tecnologia.

A lei obrigará uma adaptação maior do que foi necessária quando tivemos o *compliance*, pois o *compliance* digital ainda hoje é pequeno perto de outros regramentos e porque não temos inserida na nossa cultura atual uma cultura digital e uma cultura básica

de proteção de dados.

Concordamos com quaisquer regras que os softwares nos imponham sem sequer pensar nos riscos envolvidos. Concordamos com qualquer um coletando nossos dados sem mesmo nos informar a finalidade de uso e onde serão armazenados, etc. Exemplo típico: Portaria de prédio. Porque coletar minha identidade, foto, CPF, endereço, BIOMETRIA (!), se bastava informar a sala onde estou indo se posso ou não subir (se fui ou não convidado). Onde ficam estes dados? Já perceberam que de tempos em tempos eles perdem nossos dados e pedem tudo de novo? E se estes dados vazarem? De quem era a responsabilidade de coleta, guarda e uso dos mesmos?

Notório que para adaptar a LGPD as empresas temos que ter times multidisciplinares. Os advogados precisam trabalhar com engenheiros, com pessoal de TI, com pessoal de compliance, com equipes que pensem mais do que apenas uma lei ou um dado, estamos lidando com um ecossistema inteiro, com consequências diretas ou indiretas a toda a empresa, muito além das multas da lei.

E ainda bem que vivemos num universo digital, posto que esta coleta, autorização e guarda pode ser obtida num clique de concordância eletrônica, desde que para tanto tenhamos alguns elos digitais de segurança.

A visão de que, graças às novas tecnologias, o mundo tem se transformado em uma grande rede é amplamente detalhada por Castells (1999), que revelou uma sociedade organizada em rede, fortemente influenciada pelos artefatos tecnológicos, especialmente a internet, gerando transformações econômicas e sociais. Porém, ainda que haja cada vez mais artefatos tecnológicos, a sociedade em rede apresenta uma contradição entre desenvolvimento econômico e desigualdade, como também descreve Warschauer (2006, p.53).

No artigo 2º da LGPD são indicados os fundamentos para a proteção de dados e a privacidade. Destaca-se que a proteção de direitos fundamentais é evidente no artigo citado e também em dispositivos presentes na Constituição Federal de 1988, como o artigo 5º.

A lei foi escrita em base de 7 fundamentos. São eles que delimitam o que é legal e o que é ilegal no que tange à proteção de dados, permeando os princípios e as bases legais na LGPD são:

O respeito à privacidade;
A autodeterminação informativa;
A liberdade de expressão, de informação, de comunicação e de opinião;
A inviolabilidade da intimidade, da honra, da imagem;
O desenvolvimento econômico e tecnológico e a inovação;
A livre iniciativa, a livre concorrência e defesa do consumidor;

Os direitos humanos, o livre desenvolvimento da personalidade, da dignidade e o exercício da cidadania pelas pessoas naturais.

A proteção à privacidade; à inviolabilidade da intimidade, da honra e da imagem encontra-se disposta no art. 5º, X, da CF/88. A liberdade de expressão está prevista no art. 5º, IX, da CF/88.

Dispõe o inciso X do referido artigo da CF, que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano

material ou moral decorrente de sua violação". Essa proteção geral dada no âmbito da privacidade é alvo de diversas interpretações e não se trata de um texto específico sobre a proteção de dados.

Uma menção direta da CF sobre proteção de dados se dá no inciso XII do já mencionado Art. 5º. Neste, determina-se a inviolabilidade do sigilo de comunicações, de dados e comunicações telefônicas, salvo por ordem judicial para fins de investigação criminal e instrução processual penal. Este mandamento constitucional foi regulado pela Lei Federal nº 9.296/96 que, em seu Art. 1º, parágrafo único, afirma que a proteção dada aos sistemas de telefonia também se aplica à interceptação de fluxo de comunicações em sistemas de informática e telemática. Todavia, o texto legal, ao utilizar a palavra "fluxo de comunicações", trouxe consigo divergência doutrinária e jurisprudencial em face da diferença entre dados estáticos e dados "em movimento". Contudo, pelo fato da Lei nº Federal 9.472/97, conhecida como Lei Geral de Telecomunicações (LGT), conceituar telecomunicação como transmissão, emissão ou recepção de informações de qualquer natureza, apenas o fluxo de comunicações estaria protegido pelo inciso XII da CF/88 e pelo Art. 1º da Lei nº 9.296/962.

Isso não significa que o Poder Judiciário brasileiro está completamente ausente de discussões sobre o assunto. Por exemplo, as cortes brasileiras têm ampliado o conceito de espaço público em diversos casos, ao mesmo tempo em que têm aplicado limitações à liberdade de expressão e garantido o direito à privacidade. Em um destes, relativo a dano moral, a súmula foi relata como segue:

> RESPONSABILIDADE CIVIL – DANO MORAL – Colocação de fotos em comunidade virtual – Cerceamento de defesa inocorrente – Preliminares rejeitadas – Exposição indevida da pessoa não configurada – Canal de comunicação mantido entre moradores do condomínio onde residem as partes – Retratação do dia a dia e eventos ocorridos no residencial – Inexistência de comentários relacionados às fotos, de modo a emprestar conotação espúria visando denegrir ou difamar – Dinâmica dos fatos que não denotam intenção de atingir a honra ou personalidade – Reconvenção – Inexistência

> do alegado excesso na ação ou abuso de poder da parte, ao exercer seu legítimo direito de ação – Decisão que analisou a questão de forma sucinta e coesa, não havendo falar em sentença 'citra petita' – Recursos desprovidos.

Por meio da leitura da súmula do acórdão acima transcrita, consegue-se evidenciar que as cortes pátrias estão atentas a algumas das noviças questões que a utilização da internet trouxe, especificamente acerca do uso e da divulgação de informações pessoais.

No escopo do referido inciso constitucional, o Código Civil em seu Art. 21 estabelece que o judiciário, a pedido do ofendido, pode adotar providências para cessar as ofensas, uma vez que a "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

Entretanto, o entendimento sobre a confidencialidade de dados estáticos tem mudado, e a estes é imposto o véu da proteção dada à privacidade. Neste gênero é possível incluir, por exemplo, meros dados cadastrais em posse de empresas como registros eletrônicos de comunicação, tais como os endereços de Protocolo de Internet (IP). O Anteprojeto de Lei de Proteção de Dados Pessoais (ALPDP) pretende colocar um fim a essa divergência, conceituando dados pessoais e afirmando que estes somente podem ser fornecidos mediante ordem judicial. A referida proteção também é garantida pelo Projeto de Lei nº 2.126/2011, conhecido como "Marco Civil da Internet" que, caso aprovado com a redação atual, estipulará que tais dados somente podem ser fornecidos mediante ordem judicial. Neste, há uma abordagem explícita ao tema, como segue:

O acesso à Internet é essencial ao exercício da cidadania e ao usuário são assegurados os seguintes direitos:

I – à inviolabilidade da intimidade e da vida privada, assegurado o direito à sua proteção e à indenização pelo dano material ou moral decorrente de sua violação;

II – à inviolabilidade e ao sigilo de suas comunicações pela Internet, salvo por

ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

Neste particular, o texto do Código de Defesa do Consumidor (CDC) já explicita uma proteção extensa a dados relativos às relações de consumo. A Seção VI do CDC trata especificamente sobre bancos de dados e cadastro de consumidores garantindo, no seu Art. 43, que "o consumidor, sem prejuízo do disposto no Art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes". O mesmo artigo garante em seus parágrafos que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele" e que "o consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção".

Em consonância com o Art. 43 do CDC, a Portaria número 05 de 2002 do Ministério da Justiça alargou o rol de cláusulas abusivas do Art. 51 do CDC, considerando:

Art. 1º [...] abusiva, nos contratos de fornecimento de produtos e serviços, a cláusula que:

I – autorize o envio do nome do consumidor, e/ou seus garantes, a bancos de dados e cadastros de consumidores, sem comprovada notificação prévia;

II – imponha ao consumidor, nos contratos de adesão, a obrigação de manifestar-se contra a transferência, onerosa ou não, para terceiros, dos dados cadastrais confiados ao fornecedor;

III – autorize o fornecedor a investigar a vida privada do consumidor;

É importante frisar o inciso III desta Portaria, que considera cláusula abusiva aquela que autoriza ao fornecedor a investigar a vida privada do consumidor. Esta orientação é frequentemente desrespeitada, em especial quando se utilizam meios eletrônicos, pois a coleta de dados e a transferência destes para terceiros é quase uníssona, mesmo que explicitada nos "termos de uso" dos serviços (quando existentes).

O Art. 43, § 4º, do CDC considera os bancos de dados de consumidores algo de caráter público. Desta forma, em uma interpretação integrativa da lei, o acesso aos bancos de dados de registros pessoais das relações de consumo é igualmente assegurado por meio de habeas data.

A Lei Federal nº 9.507/97, que regulou o direito ao habeas data determina em seu Art. 1º, parágrafo único que se considera "[...] de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações". Desta forma, será concedido o habeas data:

Art. 7º (...)

I – para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público;

II – para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

III – para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro, mas justificável e que esteja sob pendência judicial ou amigável.

O inciso XXXIII do Art. 5º da CF afirma que "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado". Este inciso foi regulamentado pela Lei Federal nº 12.527/11, que estabeleceu procedimento específico para que o cidadão requisite dados que estejam em posse da Administração Pública, além de classificar os documentos do Estado em níveis diferentes de sigilo, em consonância com o Decreto nº 5.301/04. Tais graus de sigilo variam desde o ultrassecreto, que somente pode ser acessado após vinte cinco anos, até o reservado, que se torna público após cinco anos.

Segundo a professora e Doutora em Direito Regina Ruaro (2015), a autodeterminação informativa constitui um desdobramento do direito à privacidade e pode ser chamada de direito à privacidade informacional.

Danilo Doneda, advogado e professor Doutor em Direito Civil, entende que a autodeterminação informativa tem status de direito fundamental enquanto direito de personalidade, o que garante ao indivíduo o poder de controlar as suas informações.

Esse cenário revela as contradições sociais, culturais e econômicas que envolvem o contexto mundial em que há as implicações destacadas pelas visões de pós- modernidade, hipermodernidade e modernidade líquida. Nesse sentido, Bauman (2007), ao revelar uma configuração social a partir de tempos "líquidos", também enfatiza a questão da sociedade ser organizada em rede, a partir da contradição e da complementaridade entre conexão e desconexão no tecido social:

> A sociedade é cada vez mais vista e tratada como uma "rede" em vez de uma "estrutura" (para não falar em totalidade sólida): ela é percebida e encarada como uma matriz de conexões e desconexões aleatórias e de um volume essencialmente infinito e de permutações possíveis (BAUMAN, 2007, p.9).

Nas definições aqui apresentadas a respeito do momento e das condições sociais na qual este artigo se insere, a contradição, o conflito, a incerteza, a liquidez e as transformações dinâmicas se transformam, de certa maneira, nas únicas certezas para a condição humana vista na perspectiva de Morin (2009).

O respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, de comunicação e de opinião e à inviolabilidade da intimidade, da honra e da imagem faz com que as operações de tratamento de dados pessoais devam ser realizadas com o consentimento do titular, ressalvadas as situações em que o consentimento pode ser dispensado.

Salienta-se que o consentimento deve ser livre e inequívoco e o indivíduo deve ter acesso às informações pertinentes ao tratamento de seus dados pessoais – finalidade do tratamento, forma e duração do tratamento, identificação do controlador, informações acerca do uso compartilhado de dados pelo controlador e a finalidade.

Percebe-se que a LGPD veio para auxiliar o desenvolvimento econômico e tecnológico, uma vez que o uso crescente das Tecnologias traz muitos benefícios, mas também nos torna muito vulneráveis, sendo assim, devem ser buscadas políticas de segurança da informação e de proteção dos dados pessoais.

A LGPD objetiva trazer mais segurança para os cidadãos, os consumidores, as empresas, as organizações públicas e garantir a manutenção do Estado Democrático de Direito e cria uma regulamentação para o uso, proteção e transferência de dados pessoais no Brasil, nos âmbitos privado e público, e estabelece de modo claro quem são as figuras envolvidas e quais são suas atribuições, responsabilidades e penalidades no âmbito civil – que podem chegar à multa de 50 milhões de reais por incidente.

A lei está baseada nos direitos fundamentais de liberdade e de privacidade, como a livre iniciativa e o desenvolvimento econômico e tecnológico do país.

Dentre seus princípios, tem especial relevância o da transparência para o uso de dados pessoais e a respectiva responsabilização, o da adequação, ou seja, a compatibilização do uso dos dados pessoais com as finalidades informadas, da proteção do usuário em toda arquitetura do negócio (privacy by design), da finalidade, segundo o qual os dados só devem ser utilizados para as finalidades específicas para as quais foram coletados e previamente informados aos seus titulares, e também do princípio da necessidade, que significa limitar o uso dos dados ao mínimo necessário para que se possa atingir a finalidade pretendida, do qual surge ainda a indispensável exclusão imediata de dados, depois de atingida tal finalidade.

A regulamentação define como dado pessoal qualquer informação que identifique diretamente ou torne identificável uma pessoa natural e tratamento, como toda operação realizada com dados pessoais, tais como a coleta, utilização, acesso, transmissão, processamento, arquivamento, armazenamento, transferência etc.

Qualquer operação de tratamento de dados pessoais realizada no território nacional, por pessoa natural ou pessoa jurídica de direito público ou privado, cujos titulares estejam localizados no Brasil, ou que tenha por finalidade a oferta de produtos ou serviços no Brasil, estão sujeitos á LGPD, que passa a exigir o consentimento expresso do usuário para esta operação.

As únicas exceções à aplicação da lei são as hipóteses de tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos, além daqueles realizados exclusivamente para fins (i) jornalístico, artístico ou acadêmico (neste caso, não se dispensa o consentimento), (ii) de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais ou (iii) dados em trânsito, ou seja, aqueles que não têm como destinos Agentes de Tratamento no Brasil.

A lei criou os chamados Agentes de Tratamento de dados pessoais – nas figuras do Controlador e do Operador – que podem ser uma pessoa natural ou jurídica, de direito público ou privado. Ao primeiro (controlador) competem as decisões referentes ao tratamento de dados pessoais, enquanto ao segundo (operador), a realização do tratamento em nome do primeiro.

Foi definida também a figura do Encarregado, que também na condição de pessoa natural ou jurídica, de direito público ou privado, atuará como canal de comunicação entre o Controlador e os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

A criação da ANPD, órgão da administração pública indireta que ficará responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, aliás, foi vetada pelo Poder Executivo, pois implicaria em inconstitucionalidade do processo legislativo por trazer vício de iniciativa (a criação teria que partir do Executivo Federal). Mas o presidente já sinalizou que concorda no mérito com a criação do órgão, e que enviará um projeto de lei para essa finalidade.

Os direitos dos usuários receberam capítulo próprio no texto legal, valendo destacar o direito de acesso, que lhes garante a possibilidade de obtenção, mediante requisição, junto aos controladores, de todos os dados pessoais que estão sendo tratados, e como consequência disso, os direitos de retificação e atualização, haja vista a obrigação dos agentes de mantê-los sempre corretos e atualizados.

No que tange ao consentimento, a lei traz vários requisitos para sua validade. As informações sobre o tratamento de dados (finalidades, forma e duração, identificação do controlador e seus dados de contato, informações sobre uso compartilhado, responsabilidades dos agentes que farão o tratamento), devem ser de fácil acesso ao usuário. De igual modo, o procedimento de retirada ou revogação do consentimento e a mudança de finalidade (finalidade não compatível com a original) devem ser gratuitos e facilitados.

O consentimento deve ocorrer por manifestação livre, informada e inequívoca do titular, expressando sua concordância com o tratamento de seus dados pessoais para uma finalidade determinada, não sendo admitidas autorizações genéricas, sendo vedado o tratamento, caso a autorização tenha sido obtida mediante vício de consentimento.

Por fim, pode-se dizer que a LGPD se assemelha ao GDPR europeu, que é pautado em direitos fundamentais e objetiva proteger e garantir privacidade, liberdade, segurança, entre outros.

Os recentes escândalos de vazamento de dados da rede social Facebook – o mais famoso com o fornecimento de informações de milhares de usuários para a empresa britânica de big data e marketing político Cambridge Analytica – levaram diversos países a apressarem leis de proteção de informações pessoais.

Depois de a União Europeia publicar, em maio, seu Regulamento Geral de Proteção de Dados da União Europeia (GDPR), o Senado Federal rapidamente aprovou, no dia 10 de julho de 2018, o PLC 53/18 consolidando-se assim como a Lei Geral de Proteção de Dados brasileira (LGPD).

Diante dessa realidade, não há espaço para que se mantenha, sem crítica, o pensamento tradicional e simplificador para o desenvolvimento do conhecimento e, nessa

linha, os avanços trazidos pela revolução digital são, sem sombra de dúvida, positivos. Hoje, conseguimos informações do nosso interesse em segundos, seja através do computador, do tablet ou do celular, sendo esse apenas um lado da moeda: várias são as notícias de violações os direitos no mundo virtual, que trazem prejuízos não apenas de ordem material, mas também moral, tanto para pessoas naturais quanto jurídicas da própria educação dos sujeitos. No âmbito da educação virtual, a proposta que nos leva a repensar estruturas, processos, e as denominadas *fake news*, a publicação indiscriminada de fatos e fotos que violam a tão importante privacidade, transações fraudulenta se os abusos da liberdade de expressão representam o lado deletério da internet. Assim, já era o momento de se ter uma lei com vista à proteção de direitos fundamentais que nos são tão caros no presente, vem como uma reforma do pensamento que nesse contexto incerto, líquido e marcado por profundas contradições, emerge como uma esperança e se apresenta como a via da complexidade (MORIN, 2003, 2008, 2009).

Por uma série de razões, entre elas relativas à autorização de despesas por meio do poder legislativo, a medida não possuía em seu dispositivo original a previsão de constituição da referida autoridade.

Outra impactante divergência entre os textos legislativos foi que a MP 869 propôs ainda excetuar a vedação de transferência de dados da Administração Pública a entidades privadas, pela indicação de um Encarregado de Proteção de Dados, o que foi revisto pela Lei 13.853/2019, que revogou essa possibilidade.

Entre os benefícios trazidos pela Lei 13.853/2019, é válido mencionar a abrangência que cerceia a LGPD, passando de lei federal para lei nacional, de maneira a fazer com que os Estados, Distrito Federal e municípios, por possuírem capacidade legislativa residual, fiquem com um estreito espaço para legislar acerca de temas que a LGPD não mencionar.

Outra inovação da Lei 13.853/2019 faz alusão às sanções, uma vez que ela flexibilizou as penalidades nos casos de acesso ou vazamentos não autorizados de dados, caso haja conciliação entre o controlador e o titular de dados. Não obstante, na hipótese dessa eventual composição ser infrutífera, o controlador permanece sujeito a sanções elencadas pelo art. 52 da Lei 13.709.

Além disso, segundo a antiga MP 869, era facultativo à ANPD requisitar aos envolvidos no manejo de dados a emissão de relatórios de impacto à proteção de informações pessoais. Contudo, tal faculdade foi revista pela Lei 13.853/2019, e então houve um restabelecimento do texto original da legislação.

Não se limitando a isso, se tornou obrigatório pelo Poder Público o uso

compartilhado de informações com a iniciativa privada à comunicação do titular do dado. A ANPD é uma medida extremamente desejável e salutar para a manutenção de um Estado Democrático de Direito.

Diante de todo o exposto, a antiga MP 869, além de propor um modelo controverso alusivo à ANPD, ainda realizou pontuais ajustes estratégicos na LGPD que poderiam representar um comprometimento de sua eficácia, se não fosse novamente à atuação do Legislativo, restabelecendo algumas garantias quanto ao sentido do texto original aprovado.

Restam agora a vigilância e a atuação decisiva da sociedade em geral para garantir a atuação imparcial da ANPD, incluindo interesses do Poder Público e da esfera privada, no sentido de assegurar que todas as atribuições designadas à ANPD estejam em plena vigor, para assim fazer jus aos benefícios galgados pela lei.

Fonte: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm.

PRORROGAÇÃO DA ENTRADA EM VIGOR DA LGPD E OS REFLEXOS DO COVID – 19

Em tempos de educação virtual, o pensamento simplificador permite discursos de simplificação e fragmentação dos processos educativos virtuais, tornando-se pandemia a necessidade da LGPD – Lei Geral de Proteção de Dados Pessoais - lei 13.709, de 2018 - já vinha sofrendo constantes ameaças de prorrogação de seu prazo de vigência, como se os 24 (vinte e quatro) meses nela previstos não fossem suficientes para a adaptação das pessoas físicas e jurídicas para proporcionarem a proteção dos dados pessoais que estejam tratando ou que venham a tratar.

Não obstante a prorrogação fomentada pela Lei 13.853/2019, que alterou de 18 para 24 meses o lapso para entrada em vigor de grande parte dos dispositivos relativos à

regulamentação do manejo de tratamento de dados, algumas dessas previsões legislativas, sobretudo aquelas referentes à criação da ANPD, passaram a ter vigência imediata, seguindo exemplo dos sistemas legislativos relacionados ao tema, como a GDPR.

A situação de pandemia reforçou esse entendimento, quando na verdade deveria ser justamente o contrário, pois nunca, em todo o mundo, os dados pessoais ficaram tão expostos, haja vista que o trabalho remoto, somado a ampla utilização da nuvem e as reuniões virtuais aumentam exponencialmente a possibilidade de incidentes com dados pessoais. Veja-se o exemplo do vazamento de dados pessoais ocorrido na plataforma Zoom.us, cujos dados tratados, ao que parece, estão à venda na darkweb.

Mas, infelizmente, o Brasil está indo no caminho da prorrogação do prazo de vigência da LGPD. O Senado Federal aprovou, no dia 3 de abril (sexta-feira), o PL 1.179/20 que dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de direito privado, no período da pandemia causado pela covid-19, cujo ponto principal do PL é a intenção de postergar a entrada em vigor LGPD, prevista para agosto deste ano.

No âmbito empresarial diversas medidas já vêm sendo adotadas pelo Governo a fim de minimizar os impactos econômicos da pandemia. Nesta seara, o PL 1.179/20, sugeriu prorrogar a vigência da LGPD por mais 18 (dezoito) meses, sob a justificativa de "não onerar as empresas em face das enormes dificuldades técnicas econômicas advindas da pandemia".

Nessa perspectiva, há que se debruçar em reflexões sobre a LGPD e suas concepções para além do sujeito que, como uma peça de quebra-cabeça, deve se encaixar somente em uma dimensão da ação educativa virtual. A condição humana noutro bordo, não há como negar o impacto econômico trazido pela pandemia do covid-19, resultante na paralisação quase que nacional do comércio para perpetuar a quarentena, ocasião em que se torna necessária à atuação do Estado com alternativas para mitigar os efeitos da crise de saúde pública e desonerar empresas, em especial as mais vulneráveis, e também para visar à manutenção dos empregos, rendas e atividades em geral.

A prorrogação da LGPD revela-se ser uma faca de dois gumes, de um lado desafoga as empresas que ainda sequer iniciaram medidas necessárias para se adequarem aos procedimentos nela requeridos, e de outro lado, promove insegurança no cenário do mercado internacional.

Tentando estabelecer uma relação entre a divisão do trabalho e ação dos sujeitos do fazer educativo a partir de Tardif e Levasseur (2011) e as orientações legais (BRASIL, 2010), é possível realizar uma aproximação entre a ação que os *teachers aides* desenvolvem com a ação prescrita para os professores-tutores virtuais, como iniciativa de iniciar-se um equilibrio nesse momento de pandemia. Assim com advento de ações na pandemia, veio tambem a MEDIDA PROVISÓRIA Nº 959, DE 29 DE ABRIL DE 2020, in verbis:·.

> Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais - LGPD.

A prorrogação da LGPD afetar diretamente o desenvolvimento econômico do Brasil, justamente nesse momento de crise, podendo ser até maior do que apontam os estudos recentes de que praticamente não haverá crescimento do PIB no calendário de 2020.

Além disso, há que ser considerada uma possível imagem negativa a prorrogação da vigência da LGPD, sujeitando o Brasil às eventuais perdas de oportunidades relacionadas a transações que envolvem dados pessoais sensíveis de nível internacional, como investimentos estrangeiros.

É manifesto o interesse do Brasil em ingressar na OCDE (Organização para a Cooperação e Desenvolvimento Econômico), na medida em que essa participação implica em credibilidade internacional e, consequentemente, atrai investimentos possibilitando o desenvolvimento econômico.

No entanto, para ingressar na OCDE é necessário cumprir diversos requisitos técnicos e político-diplomáticos, dentre eles possuir uma legislação de proteção de dados e uma autoridade independente e capaz de fiscalizar o seu cumprimento. Para a OCDE, ter uma lei de proteção de dados significa que o país garante a proteção mínima a partir de princípios como transparência, finalidade, necessidade, entre outros. Por esta razão, é de notável interesse do Brasil aproveitar o suporte dos EUA, e adote medidas necessárias que visem acelerar o atendimento aos requisitos exigidos pela OCDE para sua aceitação no grupo econômico internacional.

Frisa-se que conforme informações do ICO (Information Commissioner's Office - Autoridade independente do Reino Unido criada para defender os direitos de informação e

dados de privacidade dos indivíduos), frente à pandemia do covid-19 tornou-se necessário o uso de rastreamento de celulares visando analisar minuciosamente a expansão do vírus para poder agir de forma preventiva, sendo que neste caso, como já há uma regularização no Reino Unida o Estado já está responsabilizado por este tratamento de dados privados.

Em detrimento a prorrogacao e os empactos em virtude da pandemia, cresceu ocorrencia do numero crescente de *fake news*, temos que mencionar que foi Sancionada, com nove vetos, lei que cria Autoridade Nacional de Proteção de Dados, sendo necessario que seja avaliado que estejam em pleno vigor a LGPD, para assim fazer jus aos benefícios galgados pela lei, in verbis:

> O Diário Oficial da União publicou nesta terça-feira (9) a Lei 13.853/19, que cria a Autoridade Nacional de Proteção de Dados (ANPD), órgão federal que vai editar normas e fiscalizar procedimentos sobre proteção de dados pessoais. A nova lei tem origem na Medida Provisória 869/18 e foi sancionada pelo presidente Jair Bolsonaro com nove vetos.

Editada no final do ano passado pelo então presidente Michel Temer, a MP 869/18 altera a Lei Geral de Proteção de Dados Pessoais (LGPD, 13.709/18), norma que regulamentou a forma como as organizações (empresas, bancos, órgãos públicos e outros) utilizam os dados pessoais.

CONSIDERAÇÕES COMPLEXAS

A prorrogação da entrada em vigor da LGPD tem sido alvo de questionamentos por parte de advogados e de juristas, que têm percebido uma postura de adiamento por partes de autoridades e de organizações. Independente da pandemia, já havia projeto anterior com o intuito de prorrogar a data de vigência da lei.

Para advogada e pesquisadora Patrícia Peck Pinheiro (2020) a Autoridade Nacional de Proteção de Dados - ANPD - já deveria ter sido constituída e empossada em 2019.

Como demonstrado em artigo anterior "Aspectos sobre a Lei nº 13.853 de 2018", publicado na página, Instituto de Direito Real, a ANPD é importantíssima para a implementação da LGPD, já que é o órgão competente para fiscalizar e regulamentar os critérios da LGPD.

Embora haja grande postergação para a entrada em vigor da LGPD, mais cedo ou mais tarde as empresas precisarão se adequar às disposições da LGPD.

Conforme indicado a proteção de dados pessoais e a garantia da privacidade estão atreladas a diversos direitos fundamentais. Estamos enfrentando uma situação muito grave e devem sim, ser pensadas alternativas para auxiliar no combate a COVID-19.

A utilização dos dados pessoais pode ser útil para auxiliar nas pesquisas científicas e na elaboração de políticas públicas de controle do vírus. Ressalta-se que deve ser respeitada a finalidade, deve haver transparência e exclusão dos dados após o uso.

Segundo Danilo Doneda (2020) a legislação de proteção de dados pessoais na proteção de liberdades individuais e coletivas torna-se muito importante no momento atual, em razão do risco de se utilizarem os dados para interesses não relacionados com o combate à doença.

Assim, verifica-se a necessidade e urgência da entrada em vigor da LGPD e da criação efetiva da Autoridade Nacional de Proteção de Dados.

Interessantes reflexões com grandes debates sobre a Lei Geral de Proteção de Dados, não é mesmo?

Não podemos fazer afirmações irrefutáveis sobre a Lei Geral de Proteção de Dados, uma vez que sequer está em vigor no Brasil e porque quando assim estiver teremos muitas interpretações jurisprudenciais sobre o tema, entretanto, temos que perceber e analisar o que já acontece com a lei em vigor Europeia (quiçá, como exemplo) para que nosso trabalho e análise fiquem mais compromissados com a verdade, aproveitando a experiência que os demais já passaram.

REFERÊNCIAS

- BRASIL. Medida Provisória 959 de 2020. Constituicão da Republica Federativa do Brasil. Brasilia, DF: Senado Federal. Disponivél em: http://www.planalto.gov.br/ccivil_03/_ato2019-022/2020/Mpv/mpv959.htm.
- ROCHA, Gustavo/ Especialista em Marketing (Consultoria GustavoRocha.com), Um Pouco Mais Sobre Compliance Digital E A Lei Geral De Proteção De Dados – LGPD, doutrina Gestão e marketing.
- BRASIL. Constituição da República Federativa do Brasil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 5 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 20 jun. 2013.
- BRASIL. Lei complementar nº 105, de 10 de janeiro de 2001. Dispõe sobre o sigilo

das operações de instituições financeiras e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 11 jan. 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp105.htm>. Acesso em: 20 jun. 2013.

- BRASIL. Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 30 out. 1984. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L7232.htm>. Acesso em: 20 jun. 2013.
- BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 12 set. 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 20 jun. 2013.
- BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do Art. 5° da Constituição Federal. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 25 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9296.htm>. Acesso em: 20 jun. 2013.
- BRASIL. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 17 jul. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9472.htm>. Acesso em: 20 jun. 2013.
- BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 13 nov. 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L9507.htm>. Acesso em: 20 jun. 2013.
- BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm>. Acesso em: 20 jun. 2013.
- BRASIL. Lei nº 11.419, de 19 de dezembro de 2006. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 20 dez. 2006. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11419.htm>. Acesso em: 20 jun. 2013.

- BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do Art. 5º, no inciso II do § 3º do Art. 37 e no § 2º do Art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm>. Acesso em: 20 jun. 2013.
- BRASIL. Medida Provisória nº 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 27 ago. 2001. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm>. Acesso em: 20 jun. 2013.
- BRASIL. Projeto de Lei nº 2.126, de 2011. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, [em tramitação]. Disponível em: <http://www.planalto.gov.br/ccivil_03/Projetos/PL/2011/msg326-24ago2011.htm>.