REPATS - Revista de Estudos e Pesquisas Avançadas do Terceiro Setor

V.8, N.1 JAN/JUL (2021)

A LGPD E SUA APLICAÇÃO ÀS ENTIDADES DO TERCEIRO SETOR

THE "LGPD" AND IT'S APPLICATION TO THE THIRD SECTOR ENTITIES

José Eduardo Sabo Paes [*]

Vera Wolff Bava [**]

RESUMO: A Lei Federal nº 13.709/2018, denominada de Lei Geral de Proteção de Dados (LGPD) entrou em vigência no Brasil e impõe uma nova dinâmica para entidades públicas, privadas e também as entidades sociais de todo o Brasil, principalmente quanto a proteção de dados das pessoas envolvidas nas atividades que são desenvolvidas pelas organizações. Esta pesquisa demonstra, por meio de revisão bibliográfica e análise prospectiva da aplicabilidade da LGPD ao Terceiro Setor. Trata-se de um estudo aplicado, buscando direcionar a efetivação deste novo diploma normativo.
Palavras chave: LGPD, Terceiro Setor, Proteção de Dados.

ABSTRACT: In Brazil, Federal Law No. 13,709 / 2018, called the General Data Protection Law (LGPD) came into force in Brazil and imposes a new dynamic for public and private entities and also social entities from all over Brazil, especially regarding protection data of the people involved in the activities that are developed by the organizations. This research demonstrates, through bibliographic review and prospective analysis of the applicability of LGPD to the Third Sector. It is an applied study, seeking to direct the implementation of this new normative diploma.
Keywords: LGPD, Third Sector, Data Protection.

[*] Pós Doutor em Democracia e Direitos Humanos pelo Ius Gentium Conimbrigae/Centro de Direitos Humanos (IGC) - Coimbra, Portugal. Procurador de Justiça do Ministério Público do Distrito Federal. Procurador Distrital dos Direitos do Cidadão do MPDFT. Professor da Universidade Católica de Brasília.

[**] Advogada graduada pela USP. Procuradora do Estado de São Paulo aposentada. Foi Corregedora Geral da Administração e Ouvidora Geral do Estado. Atua como consultora nas áreas de compliance, proteção de dados, integridade e ouvidoria.

INTRODUÇÃO

A Lei Federal nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados (LGPD), com o objetivo de proteger o direito à privacidade e o livre desenvolvimento da personalidade da pessoa natural, disciplina o tratamento de dados pessoais (que, nos termos da própria norma, são quaisquer informações relacionadas à pessoa natural e viva, identificada ou identificável), por pessoa natural ou jurídica, de direito público ou privado, independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados.

A LGPD entrou em vigor em setembro de 2020 e, portanto, todas as organizações do Terceiro Setor, Associações, Fundações e outras que, independentemente de seu porte, lidam com dados pessoais de seus colaboradores, de terceiros e de seu público em geral, devem estar preparadas para cumprir referida Lei e agir preventiva e continuamente para manter, de forma adequada, esse escorreito tratamento.

Referida Lei é fruto da pressão da sociedade moderna que, cada vez mais consciente das questões envolvendo o tratamento de dados pessoais, passou a exigir das instituições públicas e privadas maior transparência e segurança no que concerne à forma como seus dados são tratados, bem como maior poder de decisão sobre o seu uso e compartilhamento (DE SALVIO; RODENFISH; LADEIRA, 2019).

As regras contidas na LGPD, na verdade, não são totalmente inéditas. A Lei foi inspirada na GDPR – *General Data Protection Regulation* 2016/679, norma que regula o tratamento de dados pessoais na União Europeia e que tem como base o art. 8º da Carta Europeia de Direitos Humanos, como bem lembra Ruaro e Glitz (2019)[1], o qual reconhece o direito fundamental a proteção de dados, direito este elevado a categoria de direito fundamental autônomo, separado, inclusive, do direito à intimidade, que está previsto no art. 7º.

[1] RUARO, Regina Linden. GLITZ, Gabriela Pandolfo Coelho. Panorama Geral da Lei Geral de Proteção de Dados Pessoais no Brasil e a inspiração no Regulamento Geral de Proteção de Dados Pessoais Europeu. REPATS, Brasília, V.6, nº 2, p 340-356, Jul-Dez, 2019.

Assim, a visão trazida pela RGPD reforça que o tratamento de dados pessoais deve servir à humanidade, porém tal direito não é um direito absoluto e, portanto, deve ser considerado em relação a sua função com a sociedade e manter sempre o equilíbrio com os demais direitos fundamentais, baseado no princípio da proporcionalidade (MAÑAS, 2016, p. 57).

Portanto, é bom esclarecer que a proteção de dados pessoais e da privacidade no Brasil já tinha guarida em relevantes diplomas normativos, como a própria Constituição Federal de 1988, o Código de Defesa do Consumidor, o Código Civil, a Lei de Acesso à Informação, o Marco Civil da Internet e Lei do Cadastro Positivo.

Importante também dizer que a LGPD estabelece os limites de sua abrangência: conforme artigo 3º, e bem resumidamente, qualquer operação de tratamento de dados que seja realizada no território nacional, ou em que os dados pessoais objeto do tratamento tenham sido coletados no território nacional. A Lei também arrola expressamente os tratamentos de dados pessoais que não estão submetidos às suas regras (por exemplo, o realizado por pessoa natural para fins exclusivamente não econômicos, ou os jornalísticos, artísticos, acadêmicos, de segurança pública, defesa nacional, dentre outros previstos no seu artigo 4º).

É sabido que a maior parte das instituições ainda não logrou êxito no intento de implantação da LGPD, não por descaso ou incompreensão da importância da referida norma jurídica, mas por diversos fatores, dentre eles, o entendimento de sua exata dimensão, a dificuldade de mapear os riscos existentes nas suas atividades, o receio de que esta implementação implique em aumento de gastos, ou mesmo pelo simples fato de não saber como fazer para que tais regras virem uma prática no dia a dia da organização.

A adoção de tais medidas preventivas e protetivas, entretanto, além de fazer com que as instituições não incorram nas pesadas sanções impostas pela LGPD (que começarão a valer a partir de agosto de 2021), podem ser de grande valia para estas, no que concerne à sua reputação, confiança do mercado e credibilidade perante seus usuários, públicos interno, externo, consumidores e parceiros de negócios.

Muito comum ouvirmos hoje em dia que a proteção de dados pessoais é valor e não um gasto. Além de fazer com que a entidade deixe de estar exposta a riscos desnecessários, ela agrega valor às organizações, à imagem destas perante a sociedade, denotando comprometimento e seriedade da cultura organizacional. Para estar em conformidade com a LGPD, portanto, necessário conhecê-la a fundo, investir em sua implementação através, principalmente, do trabalho em equipe multidisciplinar, eventualmente, contando com assessoramento técnico externo, para, enfim, conseguir torná-la uma realidade, ou seja, efetiva no aspecto prático.

Até porque a LGPD não foi criada para limitar a atuação de todos aqueles que são responsáveis pela gestão de dados, e sim para promover a inovação, bem como a expansão segura dessas atividades, tendo sempre como missão a proteção e a promoção dos direitos fundamentais, resguardando a intimidade e a privacidade, essenciais para a efetiva tutela dos dados privados dos cidadãos.

Passemos, então, à abordagem sobre conceitos, princípios, agentes e hipóteses de tratamento de dados pessoais previstos pela LGPD, para então chegarmos à aplicação da Lei no dia a dia das organizações do Terceiro Setor, que é o objetivo maior deste item.

Lembrando sempre que o *compliance*, as boas práticas de governança, o gerenciamento de riscos, o plano emergencial para incidente de vazamento de dados e de forma especial o mapeamento de dados, são indispensáveis para a garantia da segurança e a proteção das informações, e são algumas das mais variadas técnicas de adequação a LGPD, e que adiante também serão tratados.

2. CONCEITOS, PRINCÍPIOS DA LEI FEDERAL 13.709/2018 E OS SEUS BENEFICIÁRIOS DIRETOS (TITULARES DE DADOS PESSOAIS)

Nos termos do artigo 5º da LGPD, considera-se **dado pessoal** toda e qualquer informação, em suporte eletrônico ou físico, relacionada à pessoa natural viva, identificada ou

identificável. Ou seja, dado pessoal não se resume a nome, e-mail, endereço, telefone, número de RG ou CPF, mas a toda e qualquer informação que, individualmente considerada, ou em conjunto com outras, possa levar à identificação de alguém.

Já **dado pessoal sensível** é aquele que pode levar à discriminação de alguém, como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. A LGPD cuida ainda, e de forma especial, do tratamento de dados pessoais de crianças e adolescentes, reforçando a proteção da privacidade que o Estatuto da Criança e do Adolescente já proporciona a estes indivíduos.

Sendo assim, titular será sempre a pessoa natural a quem se refiram os dados pessoais que são objeto de tratamento.

Por outro lado, a LGPD considera **tratamento** toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Assim, e resumidamente, pode-se dizer que o ciclo de vida básico dos dados pessoais (com exceção daqueles previstos no artigo 4º, aos quais a LGPD não se aplica) são: criação, armazenamento, uso, compartilhamento, arquivamento e eliminação. A diferença entre armazenamento e arquivamento está na necessidade de manuseio dos dados no dia a dia. Enquanto os dados armazenados têm que estar facilmente acessíveis, os arquivados não são mais utilizados e permanecerão no arquivo morto até que possam ser definitivamente eliminados.

Por sua vez, são exemplos de atividades envolvendo dados pessoais a identificação de pessoas para atender demandas, recepção de informações de atendimento ao público, consolidação de informações resultantes de manifestações de canais de acesso, programa de

fidelização de clientes, armazenamento de imagens coletadas com câmeras de vigilância, armazenamento de dados pessoais em rede local, *data centers*, ou na "nuvem", dentre outros.

Colocados estes principais conceitos, segue-se que, de acordo com o artigo 6º, as atividades de tratamento de dados pessoais deverão observar os seguintes princípios: a) **Finalidade** (propósitos legítimos, específicos e informados aos titulares de dados); b) **Adequação** (compatibilidade do tratamento com as finalidades informadas aos seus titulares); c) **Necessidade** (limitação do tratamento ao mínimo necessário para a realização das suas finalidades); d) **Livre acesso** (garantia aos titulares de consulta facilitada e gratuita sobre a forma e a duração do tratamento de seus dados); e) **Qualidade dos dados** (exatidão, clareza, relevância e atualização dos dados); f) **Transparência** (garantia aos titulares de dados de informações precisas sobre a realização do tratamento em si, bem como os respectivos agentes de tratamento); g) **Segurança** (utilização de medidas técnicas e administrativas para proteção dos dados pessoais); h) **Prevenção** (adoção de medidas para prevenir a ocorrência de incidentes com os dados pessoais e possíveis danos); i) **Não discriminação** (impossibilidade de realização do tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos); j) **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, assim como da eficácia dessas medidas).

Além de obedecer a estes princípios e demais normas regulamentares, os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de modo a atender aos requisitos de segurança, bem como aos padrões de boas práticas e de governança (artigos 49 e 50, da LGPD).

Sabe-se que a promoção de boas práticas de governança requer o desenvolvimento de um Programa de *Compliance*. E *compliance* é, antes de tudo, "estar de acordo", ou seja, significa desenvolver cada aspecto das respectivas atividades em consonância com os mais diversos regulamentos a que se submete uma entidade do Terceiro Setor.

Ademais, o *compliance* objetiva reduzir os riscos da atividade se voltando para a concretização da missão, das finalidades e da atividade da entidade.

Desse modo, o *compliance*, como aponta Tatiana Kolly (Rodrigues, 2021)[2], se caracteriza como método responsável pela manutenção e controle dos riscos legais, com procedimentos especificamente direcionados a garantir a conformidade dos regulamentos legais nacionais e internacionais, além dos regramentos internos.

Em suma, essa prática se aplica a todos os tipos de instituições e envolve uma conduta essencial no mercado atual, visto a exigência de condutas legais cada vez mais rígidas e punitivas, dada a relevância dos direitos tutelados, em especial da LGPD.

Verifica-se assim a importância dada pela lei ao *compliance*, sendo sua implementação essencial para o desenvolvimento da empresa, da transparência, da ética e da sociedade, servindo assim como instrumento efetivo de construção e consolidação da LGPD.

2.1 Governança

Governança corporativa é o conjunto de processos, costumes e leis que norteiam a forma como uma organização é administrada. Boas práticas de governança tendem a estabelecer um ambiente de confiança entre os stakeholders[3] em seus relacionamentos negociais, zelando por um capital que não tem preço: a reputação institucional.

Principalmente no Terceiro Setor, reputação institucional é sinônimo de credibilidade, pois facilita a obtenção de "licença social" para a instituição atuar, atrai investidores

[2] RODRIGUES, Tatiana Kolly Wasilewski. Lei Geral de Proteção de Dados (LGPD) e Data Mapping (Mapeamento de Dados): desafios, perspectivas e como se adequar à nova lei na prática. In: TEIXEIRA, Tarcisio (coord.). Empresas e Implementação da LGPD – Lei Geral de Proteção de Dados. Salvador: Editora JusPodivm, 2021. p. 62-63.

[3] Stakeholders ou partes interessadas são indivíduos ou entidades que assuem algum tipo de risco, direto ou indireto, em face da organização. São eles, além dos associados ou empregados, mantenedores, clientes, fornecedores, credores, governo e comunidade.

Recebido em: 03 jan. 2021 - Aceito 30 jan. 2021
E-mail: repats.editorial@gmail.com

comprometidos com negócios sustentáveis e permite o despertar de um propósito institucional que se reflete em seu corpo funcional. Ou seja, adotar práticas de governança corporativa é muito mais do que uma opção ou modismo, é uma necessidade atual, no cenário mundial de demandas socioambientais inadiáveis e riscos crescentes.

Em sintonia com as boas práticas de governança, o conceito de *Compliance* também evoluiu nos últimos anos. O termo de origem inglesa, comumente traduzido como o dever de estar em conformidade com atos, normas e leis, amplia seu escopo de significado incorporando mecanismos específicos de prevenção, detecção e remediação dos atos lesivos previstos na Lei nº 12.846/2013 (BRASIL, 2015b).

Para implementar a cultura de *Compliance* dentro de uma organização é necessário entender que a iniciativa precisa estar baseada no apoio inequívoco da Alta Administração, sendo imprescindível discutir, implementar e reforçar comportamentos que impactam a cultura organizacional da entidade e de suas lideranças.[4]

A evolução e a rápida transformação do ambiente de negócios, marcadas por crises, ameaças cibernéticas, grandes escândalos decorrentes de fraude e corrupção, bem como inovações disruptivas, vêm forçando as organizações a ampliarem o foco em governança e em *compliance*.

Boa governança tem como uma de suas dimensões fundamentais a *accountability*. Paulo Nogueira da Costa, inclusive, expôs a respeito das dimensões do princípio da *accountability* no campo da gestão, salientando ser ela fundamental no quadro de combate à corrupção e na promoção da transparência da vida pública[5], até porque prestação de contas é essencial para qualquer organização pública ou privada.

Não sem razão, a LGPD prevê de modo claro, em seu artigo 50 e seguintes, as boas práticas e condutas de governança, que visam adequar as atividades das organizações controladora de dados ao que dispõe os direitos por ela tutelados.

[4] KPMG – Pesquisa Maturidade do Compliance no Brasil, 4ª edição, 2019.
[5] COSTA, Paulo Nogueira da. O Tribunal de Contas e a Boa Governança. 2ª edição. Petrony Editora, junho de 2017. pp. 240-242.

O referido dispositivo permite que as corporações que exercem atividades econômicas que envolvem tratamento de dados criem regras de boas práticas e de governança, desde que estabeleçam, por exemplo, condições de organização, regimes de funcionamento, procedimentos, normas de segurança e de padrões técnicos, mecanismos internos de supervisão e de mitigação de riscos, e outros aspectos relacionados ao tratamento das informações sensíveis[6].

3. AGENTES DE TRATAMENTO DE DADOS PESSOAIS: O CONTROLADOR, O OPERADOR, O ENCARREGADO E A AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS - ANPD

A LGPD estabelece duas figuras cruciais no processo de tratamento de dados pessoais: o **Controlador** e o **Operador**.

O **Controlador** é a pessoa natural ou jurídica, de direito público ou privado, a quem compete, na organização, as decisões sobre o tratamento de dados pessoais. É ele quem controla e determina os motivos, bem como a forma desse tratamento. Já o **Operador**, que também pode ser pessoa natural ou jurídica, de direito público ou privado, é aquele que realiza o tratamento em nome do controlador e atendendo às instruções que recebe deste último.

Sem a definição destas duas figuras, a organização não estará em conformidade com a LGPD, além de ficar suscetível às sanções impostas pela Lei, porquanto a equipe fica incapaz de dar respostas às várias questões que o assunto traz. Por outro lado, se estes agentes são definidos e se eles arcarem corretamente com suas responsabilidades, as operações de tratamento de dados estarão em conformidade com a LGPD e a organização pode, inclusive, ter sua pena atenuada em casos de incidentes ou vazamentos de dados.

[6] PLUGAR. Conheça as boas práticas de governança e sanção da LGPD. 30 de maio de 2019. Disponível em: https://www.plugar.com.br/conheca-as-boas-praticas-de-governanca-e-sancao-da-lgpd/. Acesso em 09 de maio de 2021.

Além do controlador e do operador, a LGPD também traz as figuras da **Autoridade Nacional de Proteção de Dados - ANPD**, que é o órgão colegiado da Administração Pública federal responsável por zelar, implementar e fiscalizar o cumprimento da LGPD, bem como o **Encarregado** de dados, que é pessoa indicada pelo Controlador, para atuar como canal de comunicação entre este último, os titulares de dados e a ANPD.

A Lei não diz se o Encarregado pode ou deve ser pessoa física ou jurídica, utilizando apenas a palavra "pessoa". Também não obriga a que ele seja funcionário da organização, podendo ser terceirizado. Não há, ademais, vedação à possibilidade de o papel do Encarregado ser exercido por um colegiado. Neste caso, porém, deve ser escolhido um de seus integrantes para a necessária divulgação pública, pois a Lei exige, no parágrafo 1º, de seu artigo 4º, que "[...] *a identidade e as informações de contato do encarregado* [...]" sejam amplamente divulgadas nos sites e canais de comunicação da organização, devendo constar também, por via de consequência, dos seus contratos e instrumentos de parceria.

As atividades e responsabilidades[7] do Controlador, Operador e Encarregado de dados pessoais são estabelecidas pela LGPD ao longo de seu texto, em especial nos artigos 37 a 51.

A responsabilidade civil na LGPD não surge apenas da violação do microssistema jurídico de proteção de dados. É preciso interpretar o art. 42, *caput* em conjunto com o art. 44, parágrafo único, que assim dispõe: "Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano". O art. 46, por sua vez, estabelece que os agentes de tratamento deverão adotar medidas de segurança, técnicas e

[7] A responsabilidade civil está regulamentada na Seção III do Capítulo VI da LGPD, intitulada de "Da Responsabilidade e do Ressarcimento de Danos". É importante ressaltar que tais normas não serão aplicáveis em todos os casos envolvendo responsabilidade civil, podendo, dependendo da relação jurídica, ceder espaço a normas específicas, como o Código de Defesa do Consumidor, o que, inclusive, é expressamente reconhecido pela LGPD em seu art. 45: "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente".
A responsabilidade surge do exercício da atividade de proteção de dados que viole a "legislação de proteção de dados". Por essa expressão, o legislador reconhece que a proteção de dados é um microssistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural.

Recebido em: 03 jan. 2021 - Aceito 30 jan. 2021
E-mail: repats.editorial@gmail.com

administrativas visando a proteção de dados pessoais. Tais normas podem ser editadas, inclusive, pela ANPD. (CAPANEMA, Walter Aranha, 2020).[8]

4. BASES LEGAIS OU HIPÓTESES DE TRATAMENTO LEGÍTIMO E LÍCITO DE DADOS PESSOAIS

A LGPD, em seu artigo 7º, estabelece que o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses (também chamadas de bases legais):

1) mediante o fornecimento de consentimento (expresso) do titular;

2) para cumprimento de obrigação legal ou regulatória pelo controlador;

3) pela Administração Pública, para realização de políticas públicas;

4) para a realização de estudos por órgãos de pesquisa (desde que não tenham fins econômicos);

5) quando necessário para a execução de contrato;

6) para o exercício regular de direitos em processos judicias, administrativos ou arbitrais;

7) para proteção da vida, ou incolumidade física do titular ou de terceiro;

8) para tutela da saúde;

9) para atender aos interesses legítimos do controlador ou de terceiro (exceto nos casos de prevalecerem os direitos e liberdades fundamentais do titular, que exijam a proteção de dados pessoais), sempre devidamente justificado em Relatório de Impacto);

10) para a proteção do crédito.

[8] CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020. p. 165.

Depreende-se da leitura destes dispositivos que, para a LGPD, o tratamento de dados pessoais somente poderá se dar caso a situação concreta se enquadre em uma, ou mais de uma, destas dez hipóteses ou bases legais (JIMENE, 2019).

De todas elas, o consentimento (dado de forma livre, expressa, inequívoca e para a finalidade determinada) é, sem dúvida, o mais seguro para legitimar o tratamento de dados. Porém, como ele pode ser revogado a qualquer momento pelo titular (conforme parágrafo 5º, do artigo 8º), deve ser usado apenas em último caso, ou seja, desde que a situação concreta não possa ser enquadrada em nenhuma das nove outras hipóteses. Disto decorre também que, caso o tratamento de dados não se enquadre em nenhuma das dez bases legais acima descritas, ele não poderá ocorrer.

5. PASSOS PARA A IMPLANTAÇÃO DA LGPD NAS ORGANIZAÇÕES.

Já ficou clara a importância e a premência de que a LGPD seja implementada em todas e quaisquer pessoas naturais ou jurídicas, de direito público ou privado, que lidem com dados pessoais. Desta obrigação não podem fugir, portanto, as organizações do Terceiro Setor. Sendo assim, são indicados a seguir alguns passos bastante importantes para esta finalidade.

Antes de mais nada, é necessário que a alta liderança da instituição tenha consciência da importância da implantação da LGPD, engajando-se nesse mister, para com isto estimular diretores, funcionários e demais colaboradores na empreitada de implantação de programa de governança em privacidade.

Frise-se ser também fundamental nestes primeiros passos, além do comprometimento das altas lideranças, que haja o efetivo engajamento de representantes das áreas afetas (em especial, departamentos jurídico, de *compliance*, controladoria, marketing, atendimento ao cliente, vendas, recursos humanos, dentre outros), no trabalho de conscientização dos demais funcionários, colaboradores e também do público externo (incluindo usuários dos serviços,

espectadores, alunos, consumidores, enfim, o público externo da entidade). Ideal é que todos sejam estimulados ao conhecimento da LGPD e ao respeito às suas normas garantidoras e protetivas de direitos. Isto pode se dar através de *workshops*, treinamentos, palestras, debates, cursos de formação, vídeos, *posts* na *Intranet*, participação na elaboração de guias de boas práticas, enfim, de ampla e clara comunicação entre todos os envolvidos.

De fato, como asseveram Paes e Grazzioli (2018), "[...] a eficácia de um novo modelo comportamental está intrinsecamente ligada a um processo de conscientização pessoal quanto à sua necessidade e importância. Apenas com a internalização desse novo modelo por parte de cada colaborador é que o conjunto de regras estabelecido deixa de ser um texto normativo e passa a ser um legítimo instrumento de integridade."

A seguir, devem ser definidos quais são os agentes de tratamento de dados, Controlador e Operador, da organização, bem como nomeado, pelo Controlador, o Encarregado de dados pessoais que, como já dito, é o responsável pela interlocução da organização com a ANPD e com os titulares de dados, devendo atender às demandas destes últimos com a agilidade que a Lei prevê (os titulares têm o direito de pedir acesso, atualização, correção ou eliminação de seus dados). Cabe também ao encarregado orientar os funcionários e terceirizados quanto às boas práticas de proteção de dados pessoais, trabalho este que pode ser feito em conjunto com representantes das áreas afetas da instituição, bem como acompanhar a edição de novas orientações ou regulamentações pela ANPD e o surgimento de melhores práticas no mercado.

Tem sido frequente, na doutrina e nos manuais de melhores práticas, a recomendação de que, a depender do porte da organização, sejam criados Comitês de Privacidade ou de Segurança da Informação, integrados por representantes das diversas áreas, para mapeamento tanto do tratamento de dados em todo o seu ciclo (da coleta à eliminação), como dos riscos aos quais a entidade está sujeita.

Contando ou não, a entidade, com o auxílio de tais Comitês para esta tarefa, é necessário realizar-se um inventário de dados pessoais e das atividades de seu processamento

para responder questões básicas desse levantamento inicial. A organização coleta dados pessoais? Quais os propósitos da solicitação? São coletados somente os dados necessários? Quais os meios em que tais dados se encontram (físicos ou digitais)? Onde eles ficam armazenados? Quem tem acesso a eles? Há trânsito interno e externo? Qual o fluxo das informações? Onde são arquivados e por quanto tempo isto é necessário?

Na sequência, deve ser feita a identificação, dentre as informações gerenciadas pela Instituição, de quais são dados pessoais, quais são dados pessoais sensíveis e quais, eventualmente, são dados de crianças e adolescentes.

Segue-se a estes diagnósticos iniciais o mapeamento dos riscos na proteção de dados pessoais, inclusive riscos de terceiros (parceiros da organização). A partir dele é que podem ser elaboradas e adotadas normas de governança para tratamento de dados pessoais e medidas preventivas de segurança da informação e mitigatórias de riscos, além da construção de planos de contingência para tratar incidentes de segurança com agilidade e transparência.

Importante comentar aqui que, conforme nos explica Zanoni (2021), esses incidentes não se resumem a invasões, roubo de dados ou ataques de hackers, mas a toda e qualquer destruição, perda ou divulgação acidental ou ilegal de dados pessoais, lembrando que o suporte pode ser eletrônico ou físico. Para tais situações, além das devidas responsabilizações e sanções, a LGPD prevê, em seu artigo 48, notificações necessárias aos titulares dos dados e à Autoridade Nacional de Proteção de Dados.

O levantamento inicial e o mapeamento de riscos, como se viu, são imprescindíveis para se chegar à fase de verificação do grau de adequação atual da organização à LGPD e ao diagnóstico das necessidades de eventual obtenção de consentimento dos titulares dos dados, alteração ou adaptação de documentos (contratos, formulários, cadastros, dentre outros), processos e procedimentos, redação ou atualização das principais normas internas da organização (Códigos de Ética, de Conduta, Procedimentos Operacionais), inserindo-se nestas as políticas de privacidade, proteção de dados, tempo de guarda segurança da informação, dentre outras ligadas à nova legislação.

Por óbvio, importantíssimo dizer que as políticas de privacidade de dados, além de ser redigidas em linguagem simples, clara e direta, devem ser bastante divulgadas dentre os colaboradores, terceirizados e o público externo que, em última análise, são os potenciais titulares dos dados coletados pela organização.

Integradas, assim, as políticas de privacidade e proteção de dados ao Programa de *Compliance* da organização, é recomendável seja mantido um cronograma de revisão e atualização periódica das mencionadas normas internas, o que certamente envolverá um trabalho conjunto do Encarregado de Proteção de Dados com a área de *compliance* (ZANONI, 2021).

Como pondera Paes (2020), "[...] quando se trabalha com a ideia de *compliance*, deve-se ter em mente que um programa só agrega valor à organização e produz resultados concretos, portanto, mensuráveis, se for efetivo no aspecto prático."

Enfim, para ficarem de acordo com a LGPD, as organizações necessitam adequar seus programas de *compliance*, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, de fluxos e procedimentos e, acima de tudo de mudança de cultura (PINHEIRO, 2020).

CONCLUSÕES

Do exposto, pode-se concluir que:

As entidades do Terceiro Setor, assim como todas as pessoas naturais ou jurídicas, públicas ou privadas, com ou sem fins lucrativos, que lidam com dados pessoais, têm que se adequar à LGPD;

Para tanto, além do conhecimento mais aprofundado do texto da Lei, são necessários alguns passos, a começar pelo compromisso e engajamento da alta administração, a fim de

que os demais colaboradores e terceirizados também possam ser estimulados a encarar a empreitada de implantação da LGPD;

Necessárias também as definições das figuras do Controlador, do Operador e, a partir destes, a indicação do Encarregado de dados, que irá trabalhar, em conjunto com as áreas afetas ao assunto, não somente na implantação da LGPD na organização, mas também no seu curso, sendo sua principal atividade o canal de comunicação entre o Controlador, os titulares de dados pessoais e a ANPD;

Imprescindível o trabalho em equipe multidisciplinar para o levantamento e registro das operações de tratamento de dados pessoais realizados na organização, mapeamento de riscos e adoção de medidas mitigatórias destes;

Aos levantamentos apontados, seguem-se a adoção de providências para adaptação de contratos, documentos, procedimentos e normas internas à LGPD;

Integradas, destarte, as políticas de privacidade e proteção de dados ao Programa de *Compliance*, recomendável que seja mantido o cronograma de atualização das normas internas da organização, bem como um monitoramento contínuo das operações de dados pessoais, com periodicidade para revisão de políticas, procedimentos e avisos de privacidade;

Enfim, implementar a LGPD significa uma mudança cultural nas organizações e, como se sabe, toda mudança cultural envolve empenho, esforço e, sobretudo, disposição de aceitar e incorporar as novidades. Porém, se a perspectiva for no sentido de que estas inovações trarão todos os benefícios já mencionados, a tarefa fica mais atraente e facilitada. Além do mais, como também se viu, um programa só agregará valor à organização se for efetivo no aspecto prático. Por isso, mãos à obra!

Recebido em: 03 jan. 2021 - Aceito 30 jan. 2021
E-mail: repats.editorial@gmail.com

REFERÊNCIAS

BRANCHER, Paulo Marcos Rodrigues; BEPPU, Ana Claudia (Coord.). *Proteção de Dados Pessoais no Brasil – Uma nova visão a partir da Lei n. 13.709/2018*. Belo Horizonte: Forum, 2019.

BRASIL. Tribunal de Contas da União. Manual de gestão de riscos do TCU / Tribunal de Contas da União. – Brasília : TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2018.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 163-170, Janeiro-Março/2020.

CORTEZ, Frederico. *A LGPD nos centros educacionais privados, por Frederico Cortez*. Disponível em: www.focus.jor.br. Acesso em 22.02.2021.

COSTA, Paulo Nogueira da. O Tribunal de Contas e a Boa Governança. 2ª edição. Petrony Editora, junho de 2017. pp. 240-242.

GRAZZIOLI, Airton; PAES, José Eduardo Sabo. *Compliance no Terceiro Setor – Controle e Integridade nas Organizações da Sociedade Civil.* São Paulo: Elevação, 2018.

JIMENE, Camila do Vale. *Proteção de Dados Pessoais* – Curso *on line* da LEC – Legal Ethics Compiance – outubro de 2019 – Disponível em: www.lecnews.com. Acesso em 23.02.2020.

PAES, José Eduardo Sabo. *Fundações, Associações e Entidades de Interesse Social – Aspectos jurídicos, administrativos, contábeis trabalhistas e tributários*. 10 ed. Rio de Janeiro: Forense, 2020.

PINHEIRO, Patrícia Peck. *Proteção de dados pessoais: comentarios à Lei n. 13709/2018 (LGPD)*. 2 ed. São Paulo: Saraiva, 2020.

PIZZOLANTE, Francisco Eduardo O. Pires e Albuquerque. *Habeas Data e Banco de Dados: Privacidade, Personalidade e Cidadania no Brasil Atual*. Rio de Janeiro: Lumen Juris, 2002.

RODRIGUES, Tatiana Kolly Wasilewski. Lei Geral de Proteção de Dados (LGPD) e Data Mapping (Mapeamento de Dados): desafios, perspectivas e como se adequar à nova lei na prática. In: TEIXEIRA, Tarcisio (coord.). Empresas e Implementação da LGPD – Lei Geral de Proteção de Dados. Salvador: Editora JusPodivm, 2021. p. 62-63.

RUARO, Regina Linden. GLITZ, Gabriela Pandolfo Coelho. *Panorama Geral da Lei Geral de Proteção de Dados Pessoais no Brasil e a inspiração no Regulamento Geral de Proteção de Dados Pessoais Europeu*. REPATS, Brasília, V.6, nº 2, p 340-356, Jul-Dez, 2019.

ZANONI, Fernando Henrique. *LGPD na Prática: 13 passos para se adequar à nova regulamentação.* Disponível em: www.codigoconduta.com Acesso em: 22 fev. 2021.