LEI GERAL DE PROTEÇÃO DE DADOS SOB A PERSPECTIVA DAS ENTIDAES SINDICAIS. ADEQUAÇÕES NECESSÁRIAS.

Sanções administrativas somente poderão ser aplicadas a partir de 1º de agosto de 2021.

A Lei n. 13.709, de 14 de agosto de 2018, chamada de Lei Geral de Proteção de Dados - LGPD, foi editada tendo como objetivo **"proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"**.

Sua vigência é progressiva, dividida em três etapas, sendo a primeira em 28 de dezembro de 2018, quanto aos artigos que tratam da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados (CNPD), a segunda, em 18 de setembro de 2020, que trata da maioria dos artigos, e a terceira, em 01 de agosto de 2021, quanto aos artigos que tratam das sanções administrativas.

Os fundamentos da lei são realmente relevantes, sendo eles, **respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor, e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício de cidadania pelas pessoas naturais**.

A partir deste escopo, foi elaborada uma lei relativamente extensa, que em seus sessenta artigos e respectivas subdivisões, apresenta definições, conceitua dados sensíveis e constitui segmentos (como crianças, por exemplo), delimita sua aplicação, trata dos direitos dos titulares de dados, estabelece obrigações às pessoas detentoras de dados pessoais e ao Poder Público, bem como prevê sanções ao seu descumprimento.

Como ainda há margem para regulamentação, algumas exigências poderão ser relativizadas, de acordo com o tipo de organização, seu tamanho e quantidade de dados pessoais gerenciados.

Mesmo assim, esse texto procura destacar aspectos da lei sob a perspectiva das entidades sindicais, apontando algumas sugestões objetivas, visando indicar um caminho para adequações necessárias considerando o cenário atual de regulamentação, pois as entidades sindicais e associações de classe, por coletarem dados cadastrais dos seus filiados e dependentes, estão sujeitas aos ditames da lei.

Neste sentido, é relevante salientar algumas das conceituações trazidas pela norma, que são fundamentais para a sua adequada compreensão:

- **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;
- **dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, **filiação a sindicato** ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **controlador**: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **operador**: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

- **encarregado**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- **tratamento**: toda operação realizada dom dados pessoais, como as que se referem a coleta, produção, recepção, classificação, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
- **consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Ainda, neste exercício inicial de compreensão da lei, é importante citar e detalhar alguns de seus princípios, tais como o da **finalidade**, que orienta a realização do tratamento de dados para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; **adequação**, que exige compatibilidade do tratamento com as finalidades informadas ao titular; **necessidade**, que limita o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades.

Existem outros princípios, inscritos no art. 6º da lei, mas partindo destes que foram destacados, já se pode constatar, com muita clareza, a importância dada para a questão da informação ao titular dos dados, sendo que a finalidade que inicialmente deu causa a coleta de tais dados não pode ser desvirtuada ou alterada sem prévio e expresso consentimento.

Informação explícita e clara e consentimento expresso são, portanto, pontos fundantes, dispensados apenas quando os dados foram tornados manifestamente públicos pelo titular ou nos casos excepcionais previstos na lei.

O **consentimento**, como dito, deve ser **prévio e expresso**, ou seja, por escrito ou através de outro meio que demonstre a manifestação de vontade pelo titular, bem como **deve conter a finalidade**, **vedadas as autorizações genéricas**, sendo atribuído ônus ao controlador de comprovar que o consentimento foi obtido em conformidade com a lei.

Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular deverá ser informado com destaque sobre esse fato, devendo ser esclarecido sobre os meios pelos quais poderá exercer os seus direitos. Também **quanto ao tratamento de dados sensíveis, como é o caso de filiação sindical, por exemplo, deve haver autorização específica e destacada, para finalidades específicas.**

Desta forma, a título de exemplo, **o compartilhamento de dados cadastrais de filiados e seus dependentes com fornecedores de planos de saúde ou outros serviços, deverá, necessariamente, contar com autorização específica para tal finalidade, uma vez que se estará tratando dado pessoal sensível, qual seja, a filiação sindical.**

O envio de material informativo ou publicitário também deve ser previamente autorizado, de forma explícita, atendendo aos princípios da lei.

Os **dados pessoais sensíveis**, como a informação sobre filiação sindical, podem ser tratado **sem consentimento do titular** em casos determinados, **se for indispensável**, entre outras hipóteses, **para cumprimento de obrigação legal** ou regulatória pelo controlador, **tratamento compartilhado de dados necessários à execução, pela**

administração pública, de políticas públicas previstas em leis ou regulamentos, **exercício regular de direitos**, inclusive em contrato e **em processo judicial, administrativo e arbitral**, **proteção da vida ou da incolumidade física do titular** ou de terceiro.

Os dados pessoais de crianças e adolescentes devem ter tratamento específico, resguardado o seu melhor interesse, sendo exigido o consentimento específico e em destaque por pelo menos um dos pais ou responsável legal.

Assim, será necessário obter as autorizações, tal como determina a lei, ou adequar as autorizações existentes, **atentando para o fato de que as autorizações genéricas não serão válidas.**

Há que se atentar, ainda, para o período de manutenção dos dados, bem assim quanto ao exaurimento da finalidade a que se destinavam, caso em que os dados deverão ser eliminados.

Os **direitos do titular de dados** estão em um capítulo à parte na lei, sendo fundamental conhece-los integralmente, motivo pelo qual se transcreve o art. 18:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019) Vigência
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

Como se vê, os direitos estão alinhados com a capacidade do titular de dispor sobre os seus dados pessoais, com base nos princípios basilares da lei.

Para atender todos esses requisitos, a lei prevê que os controladores deverão **indicar um encarregado pelo tratamento de dados pessoais**, devendo a identidade e as informações de contato deste serem divulgadas publicamente. Dentre as atividades do encarregado, estão a de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, bem como orientar funcionários e os contratados a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Este ponto ainda poderá ser complementado pela ANPD, que poderá prever, inclusive, hipóteses de dispensa da necessidade de indicação do encarregado, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Como não há certeza quanto a este aspecto, o indicado é organizar uma forma de atender tal requisito, até mesmo porque se trata de uma medida adequada, considerando as muitas exigências que devem ser conhecidas e respeitadas pelas organizações.

Observe-se, que a lei prevê a possibilidade de responsabilização, inclusive solidária, do controlador ou operador que causar dano patrimonial, moral, individual ou coletivo, em violação à legislação de regência da matéria.

Quanto às **sanções administrativas**, estão previstas advertência, multa simples, multa diária, publicização da infração, bloqueio dos dados pessoais a que se refere a infração até a sua regularização, eliminação dos dados pessoais, suspensão ou até proibição parcial ou total do exercício de atividades relacionadas a tratamentos de dados.

Ressalva importante neste ponto é de que **não poderá haver sanções sem procedimento administrativo**, que garanta oportunidade ampla de defesa, **e estas somente podem começar a ser aplicadas a partir de 01 de agosto de 2021**.

No quesito da **segurança e boas práticas**, fica estabelecida a obrigação de adoção de **medidas de segurança, técnicas e administrativas, capazes de proteger os dados pessoais de acessos não autorizados**, bem como de qualquer forma de tratamento inadequado ou ilícito, devendo ser comunicado o titular e a autoridade nacional qualquer ocorrência de segurança que possa acarretar risco ou dano relevante aos titulares.

Sendo assim, é relevante que as entidades, por serem detentoras de dados pessoais de seus filiados, bem como de seus dependentes e pensionistas, adotem medidas práticas para a proteção dessas informações, cabendo sugerir alguns passos de ordem prática, neste sentido:

1. Mapear em quais ocasiões ou situações acontece a captação de dados pessoais;
2. Identificar as bases em que existem registros com dados pessoais, ou seja, se estão em meio eletrônico e/ou físico, em qual ou quais computadores, em qual ou quais arquivos físicos;
3. Mapear quais dados foram captados (que tipo), se existem dados sensíveis, se existem dados de crianças;
4. Avaliar os riscos, considerando os locais em que estão os dados e se esses locais estão sujeitos ao acesso indevido ou não autorizado (por exemplo, se estão em arquivo físico, se existe chave, se estão em arquivo eletrônico, se existe limitação ao acesso, como senha);
5. Observar se os dados disponíveis estão coerentes com a finalidade a que se destinam e, se existem dados desnecessários ou incoerentes com as finalidades, avaliar eliminação;
6. Estabelecer requisitos de segurança e revisar todas as rotinas, desde a captação dos dados, armazenamento e disponibilização (para fornecedores, por exemplo);
7. Elaborar materiais para treinamento da equipe e, em especial, para os que manipulam os dados pessoais, para que conheçam os limites de uso e as necessidades de preservação e cuidados com os dados pessoais;
8. Definir as responsabilidades, ou seja, quem é o controlador, quem é o operador e quem é o encarregado, e o que incumbe a cada um;
9. Editar as normas internas ou revisar as normas já existentes para prever as regras de proteção, os responsáveis e operacionalizar o papel de cada ator no processo de proteção e tratamento de dados (controlador, operador e encarregado);

10. Aditar ou formular contratos com fornecedores de serviços ou terceirizados que recebam acesso aos dados pessoais tratados pela entidade, para definir as suas responsabilidades, nos termos da lei e sob as penas desta;
11. Editar documentos para obter as autorizações necessárias quando da captação de dados, visando atender os requisitos legais (tais como informação, finalidade, necessidade, etc.).

A lista acima não pretende ser exauriente, mas indica encaminhamentos práticos, administrativos e técnicos, visando cumprir a lei e, em última análise, preservar os dados pessoais sob custodia das entidades.

Como, na maioria dos casos, os dados pessoais estão alocados em ambientes eletrônicos, é importante avaliar o acesso de qualquer pessoa aos dados pessoais, verificando, inclusive, o acesso que o fornecedor de suporte técnico de informática possui, assim como deve-se verificar se há proteção contra hackers, se há backup e onde ele fica armazenado, se existem meios de cópia dos dados e quem pode efetuá-la, entre outras medidas.

O fornecedor de suporte de informática, seja ele funcionário ou terceirizado, poderá ser um auxiliar importante na criação dos mecanismos de segurança, sendo que, ele mesmo, caso tenha acesso aos dados pessoais, deve firmar compromisso de não utilização e de preservação da privacidade, nos termos da lei e sob as penas desta.

Reforça-se, ao fim, que o objetivo da lei é, em síntese, o respeito ao direito fundamental de liberdade e privacidade, de modo que todas as ações adotadas devem ser dirigidas para esse fim, sendo fundamental a **formalização adequada das autorizações, devendo ser adotado meio idôneo, podendo ser físico ou eletrônico, desde que a organização possa comprovar a existência de autorização sempre que se fizer necessário**.

Na dúvida quanto ao procedimento mais correto, deve-se sempre ter em mente o objetivo e os princípios da lei, adotando-se a alternativa que melhor atenda tais premissas.

Para encerrar, salienta-se que este assunto precisará ser adequadamente acompanhado pelas organizações, uma vez que a Autoridade Nacional de Proteção de Dados irá apresentar regulamentações, assim como deverá orientar todos os envolvidos quanto ao cumprimento dos preceitos trazidos pela lei.