



ATUALIZAÇÕES

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

ALTERAÇÕES TRAZIDAS
PELA LEI Nº 13.853/2019

TOZZINIFREIRE
ADVOCADOS

ATUALIZAÇÕES DA LEI GERAL DE PROTEÇÃO DE DADOS

LEI Nº 13.853/2019

INTRODUÇÃO

No dia 28 de dezembro de 2018 foi publicada a Medida Provisória (MP) nº 869, que tinha o objetivo de alterar alguns pontos da Lei Geral de Proteção de Dados do Brasil (LGPD), originalmente promulgada em 14 de agosto de 2018.

A principal mudança trazida pela MP foi a inclusão dos artigos relacionados à criação da Autoridade Nacional de Proteção de Dados (ANPD), vetada na versão original da LGPD. Em 09 de julho de 2019 foi publicada a sanção presidencial da Lei nº 13.853/2019, como resultado da conversão da referida MP, que, além das mudanças supramencionadas, também trouxe vetos do presidente da República com relação a alguns dispositivos.

Preparamos a cartilha abaixo para indicar as principais mudanças decorrentes da publicação da MP, os vetos presidenciais, e um panorama da versão final da LGPD, levando todos os pontos acima em consideração.



NOVIDADES NA LGPD

Interesse nacional

Agora todas as disposições contidas na Lei Geral de Proteção de Dados são de **interesse nacional**, portanto, devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Definição do Encarregado

A definição do Encarregado sofreu uma alteração, porque agora se considera a pessoa indicada pelo controlador **e operador** para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Além disso, deixa de ser necessário que o Encarregado seja uma pessoa física.

Tratamento de dados pessoais concernentes à Administração Pública

Em nenhum caso os dados pessoais pertencentes à Administração Pública poderão ser tratados por pessoa de direito privado, exceto por pessoas jurídicas que

possuam capital integralmente constituído pelo Poder Público.

A redação original não dispunha de nenhuma exceção para esse tipo de tratamento de dados pessoais.

Tutela da saúde

Com a nova redação, o tratamento de dados pessoais e o tratamento de dados pessoais sensíveis poderá ser realizado para a tutela da saúde, se realizado, exclusivamente, **por profissionais de saúde, serviços de saúde ou autoridade sanitária**. Na redação original essa previsão apenas permitia o tratamento se realizado por profissionais da área da saúde ou por entidades sanitárias. Além disso, está vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com finalidade de obter vantagem econômica, exceto nas hipóteses relativas a: (i) prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício de interesses dos titulares de dados; (ii) permissão da portabilidade de dados quando solicitada pelo titular; e (iii) transações financeiras e administrativas resultantes do uso e da prestação dos serviços.

Também está vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Nova finalidade para tratamento de dados de acesso público

O novo texto prevê que o tratamento posterior dos dados pessoais cujo acesso é público poderá ser realizado para **novas finalidades**, desde que observados os propósitos

legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos na LGPD.

Portabilidade

O titular dos dados pessoais tem direito de obter do controlador a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a **regulamentação dada pela Autoridade Nacional de Proteção de Dados (ANPD)**, observando os segredos comercial e industrial.

Direitos dos titulares e agentes de tratamento

Apesar de os direitos dos titulares continuarem iguais, o responsável pelo tratamento, após receber solicitação de um titular, deverá comunicar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados, a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, **exceto** nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

Revisão de decisões automatizadas

A nova redação prevê que o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Na redação original era prevista a revisão **apenas** por pessoa natural. Agora, o artigo é silente quanto a quem deverá realizar a revisão, abrindo margem para pessoas jurídicas e outros sistemas automatizados.

Vedação de compartilhamento de dados pessoais pelo Poder Público

Agora o Poder Público não poderá transferir a entidades privadas dados pessoais, exceto na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, **desde que vedado o tratamento para outras finalidades.**

Conciliação entre controlador e titular

Os vazamentos individuais ou os acessos não autorizados poderão ser objeto de **conciliação direta** entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades cabíveis.



CRIAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Conforme mencionado anteriormente, a principal mudança trazida é a criação da Autoridade Nacional de Proteção de Dados (ANPD), um órgão da administração pública federal, integrante da Presidência da República. A ANPD possui natureza jurídica transitória com possibilidade de transformação em ente da Administração Pública Federal indireta após os dois primeiros anos de vigência.

Este órgão será composto por um Conselho Diretor, Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei.

Será competente à ANPD zelar pela proteção dos dados pessoais e pela observância dos segredos comercial e industrial, elaborar di-

retrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, apreciar petições, promover conhecimento das normas e políticas sobre proteção de dados pessoais à população, promover e elaborar estudos sobre o tema, indicar prazos e editar normas diferenciadas para empresas de pequeno porte, microempresas e startups, entre várias outras. Além disso, a ANPD será exclusivamente competente para aplicar sanções no que se refere a proteção de dados pessoais, pois possui autonomia técnica e decisória.

Constituirão receitas da ANPD os recursos provenientes de acordos, convênios ou contratos celebrados com entidades, organismos ou empresas, públicos ou privados, nacionais ou internacionais, e os valores apurados na venda de publicações, material técnico, dados e informações, entre outros. A arrecadação das multas aplicadas pela ANPD será destinada ao Fundo de Defesa de Direitos Difusos.

O Conselho Nacional de Proteção de Dados Pessoais e Privacidade será composto por 23 representantes e contribuirá para a criação da Política Nacional da Proteção de Dados Pessoais e da Privacidade, para a elaboração de relatórios anuais de avaliação de execução da referida Política, para a disseminação do conhecimento sobre a proteção de dados pessoais e da privacidade à população, além de sugerir ações a serem realizadas pela ANPD.



VETOS

Vale ressaltar que o presidente da República apresentou alguns vetos no momento da sanção presidencial, estando os principais elencados abaixo:

Revisão de decisões automatizadas por pessoa natural

Foi vetado o dispositivo que obrigava que a revisão de decisões tomadas unicamente com base em tratamento automatizado

fosse realizada por pessoa natural. Com este veto, essa revisão poderá ser realizada através de um sistema automatizado.

Proibição de o poder público compartilhar dados pessoais

Também foi vetado o dispositivo que proibia o poder público de compartilhar, com outros órgãos públicos ou com pessoas jurídicas de direito privado, dados pessoais pertencentes aos requerentes de acesso à informação (conforme a Lei de Acesso à Informação).

As razões do veto se dão pela ocorrência de insegurança jurídica. É argumentado que o compartilhamento de informações relacionadas à pessoa natural, que não deve ser confundido com a quebra do sigilo ou com o acesso público, é medida recorrente e essencial para o regular exercício de diversas atividades e políticas públicas.

Qualificação do encarregado

Também foram vetados alguns dispositivos que traziam regras específicas para a função do encarregado, a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre controlador, titular de dados e a ANPD.

O texto da PL aprovado pelo Senado previa que o encarregado deveria ser detentor de conhecimento jurídico e regulatório. Após os vetos, tais exigências foram excluídas, tornando a qualificação do encarregado mais flexível.

Cobrança por serviços prestados

Foi vetado o dispositivo que autorizava a autoridade a cobrar taxas por serviços prestados. A justificativa do veto se dá por conta da natureza jurídica transitória da Administração ANPD, pois não é cabível a cobrança de serviços prestados para constituição de sua receita, de for-

ma que a ANPD deve arcar, com recursos próprios consignados no Orçamento Geral da União, com os custos inerentes à execução de suas atividades-fim, sem a cobrança de taxas para o desempenho de suas competências, até sua transformação em autarquia.

Sanções administrativas aplicadas pela ANPD

Os últimos vetos são referentes ao rol de sanções administrativas que seriam aplicadas pela ANPD, anteriormente aprovado pelo Congresso. Tais punições previam a suspensão parcial do funcionamento do banco de dados pelo período máximo de seis meses, prorrogável por igual período; a suspensão do exercício da atividade de tratamento dos dados pessoais pelo período máximo de seis meses, prorrogável por igual período; bem como a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Os referidos dispositivos foram vetados, pois causam insegurança aos responsáveis por essas informações, bem como impossibilitariam a utilização e o tratamento de bancos de dados essenciais a diversas atividades privadas.



DISPOSIÇÕES DA LGPD INALTERADAS

Permanecem inalteradas e em vigor todas as disposições já previstas na redação original da LGPD não mencionadas acima, bem como as seções que tratam sobre (i) tratamento de dados pessoais de crianças e de adolescentes; (ii) término do tratamento de dados; (iii) transferência internacional de dados; (iv) obrigações do controlador e do operador pelo tratamento de dados pessoais; (v) responsabilidade e ressarcimento de danos; (vi) segurança e sigilo de dados; e (vii) boas práticas e governança.

Definições importantes

- **Dados pessoais:** informações relacionadas a pessoas naturais identificadas ou identificáveis.
- **Dados pessoais sensíveis:** informações que tratam da 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 à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Dados anonimizados:** dados relativos a titulares que não possam ser identificados, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
- **Titular:** pessoa física a quem se referem os dados pessoais.
- **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).

Direitos dos titulares

A LGPD garante uma série de direitos e garantias aos titulares de dados pessoais, que podem ser exercidos a requerimento do titular ou de seu representante legal:

- Direito à informação
- Direito de acesso
- Direito de retificação
- Direito de eliminação dos dados
- Direito de oposição
- Direito de portabilidade
- Direito de revisão de decisões automatizadas (sofreu alterações)

Bases legais para o tratamento

De acordo com a LGPD, os dados pessoais só podem ser tratados se for realizado o enquadramento em uma das hipóteses legais, conforme abaixo:

- Consentimento do titular
- Cumprimento de obrigação legal ou regulatória
- Execução de políticas públicas pela administração pública
- Realização de estudos por órgãos de pesquisa
- Execução de contrato ou procedimentos preliminares

- Exercício regular de direitos em processo judicial, administrativo ou arbitral
- Proteção da vida ou da incolumidade física
- Tutela da saúde
- Interesse legítimo do controlador
- Proteção do crédito

O tratamento de dados pessoais de crianças deverá ser realizado em seu melhor interesse, mediante consentimento específico e em destaque dado por pelo menos um de seus responsáveis legais. São obrigações adicionais: (i) o emprego de linguagem simples, clara e acessível; e (ii) o controlador manter públicas as informações sobre os tipos de dados coletados, bem como a forma de sua utilização e de exercício dos direitos que a LGPD confere ao titular. A lei ainda impõe aos controladores o dever de requerer o mínimo necessário de informações para a participação de crianças em jogos, aplicações de internet e outras atividades.

O **término do tratamento** ocorrerá quando: (i) o período do tratamento chegar ao fim; (ii) ocorrer uma manifestação do titular dos dados solicitando o término do tratamento; (iii) houver determinação legal nesse sentido; ou (iv) for verificado que a finalidade que fundamentou o tratamento foi alcançada, ou que os dados pessoais coletados perderam a sua pertinência para a finalidade pretendida.

Responsabilidade

A regra geral da LGPD é que controlador ou operador que, no exercício da atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou

coletivo, violando assim a legislação de proteção de dados, fica obrigado a repará-lo.

A lei é clara quanto à relação entre controlador e operador, determinando que o controlador deve dar instruções claras, completas, específicas e auditáveis ao operador, e que esse deverá segui-las estritamente. Nesse sentido, o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações legais de proteção de dados ou não seguir as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador.

Se dois ou mais controladores estiverem diretamente envolvidos no tratamento de dados pessoais que causou danos ao titular, todos respondem solidariamente. No entanto, o agente de tratamento que reparar o dano ao titular possui direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Dentre as excludentes de responsabilidade, vale indicar que os agentes de tratamento não serão responsabilizados quando conseguirem provar que:

- Não realizaram o tratamento de dados pessoais que lhes foi imputado;
- Realizaram o tratamento de dados pessoais que lhes foi imputado, mas não houve violação à legislação de proteção de dados; ou
- O dano decorreu de culpa exclusiva do titular dos dados ou de terceiro.

A LGPD também indica que as regras de responsabilização do direito do consumidor devem ser aplicadas nos casos em que há violação do direito do titular no âmbito das relações de consumo. Sendo assim, há responsabilização objetiva e solidária entre controlador e operador.

Transferência internacional de dados

Existem nove hipóteses em que a transferência internacional de dados é permitida:

- Fornecimento pelo titular de seu consentimento específico e em destaque em relação à transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente essa de outras finalidades;
- Quando a transferência for para países ou organismos internacionais que proporcionem um grau de proteção de dados pessoais compatível ao da legislação brasileira;
- Quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma, por exemplo, de cláusulas contratuais específicas para determinada transferência¹;
- Quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência;
- Quando a transferência for necessária para a proteção da vida do titular ou de terceiro;
- Quando a autoridade nacional autorizar a transferência;
- Quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; ou
- Quando a transferência for necessária para a execução de política pública.

O nível de proteção de dados do país estrangeiro deverá ser avaliado pela autoridade nacional, que considerará: (i) a legislação em vigor no país de destino; (ii) a natureza dos dados; (iii) o cumprimento de princípios gerais de proteção de dados pessoais; (iv) a adoção de medidas de segurança previstas em regulamento; (v) a existência de garantias judiciais e institucionais para a proteção de dados pessoais; e (vi) outras circunstâncias específicas relativas à transferência.

Vazamentos

Violação de dados é definida como o “acesso não autorizado e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento ilícito ou inadequado”.

Os agentes de tratamento de dados devem adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais contra o acesso não autorizado e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Incidentes deverão ser comunicados à ANPD e ao titular em prazo razoável. A comunicação deverá conter uma série de informações, incluindo: (i) descrição da natureza dos dados afetados; (ii) lista dos titulares envolvidos; (iii) quais eram as medidas técnicas e de segurança utilizadas para a proteção dos dados; (iv) os riscos relacionados ao incidente; e (v) quais as medidas adotadas para reverter ou mitigar o prejuízo causado pelo incidente.

Após ser notificada, a autoridade poderá determinar a adoção de providências como divulgar amplamente o fato em meios de comunicação e/ou a outros órgãos reguladores.

¹ Também são aceitas: i) cláusulas-padrão contratuais; ii) normas corporativas globais; e iii) selos, certificados e códigos de conduta regularmente emitidos.

Sanções

Além da responsabilidade de indenizar o titular que teve seus direitos violados, a LGPD prevê sanções de caráter administrativo. Seguem as principais sanções impostas aos sujeitos de tratamento:

- Advertência, com indicativo de prazo para a adoção de medidas corretivas;
- Multa de até 2% do faturamento da empresa ou do grupo no Brasil, limitada, no total, a R\$ 50 milhões por infração;
- Divulgação da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização; e
- Eliminação dos dados pessoais correspondentes à infração.

As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de acordo com as peculiaridades do caso concreto e considerados os seguintes critérios:

- A gravidade e a natureza das infrações e dos direitos pessoais afetados;
- A boa-fé do infrator;
- A vantagem auferida ou pretendida pelo infrator;
- A condição econômica do infrator;
- A reincidência;
- O grau do dano;
- A cooperação do infrator;

- A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;
- A adoção de política de boas práticas e governança;
- A pronta adoção de medidas corretivas; e
- A proporcionalidade entre a gravidade da infração e a intensidade da sanção.



PRÓXIMOS PASSOS

Segue abaixo o passo a passo para garantir a conformidade da sua empresa com a LGPD:

- Identificar e auditar (se necessário) terceiros que tratam dados pessoais em nome da empresa – os contratos celebrados com esses terceiros também devem ser revisados;
- Revisar as infraestruturas técnicas relacionadas com a segurança dos dados pessoais;
- Indicar o Encarregado (a LGPD não prevê a necessidade de registrar o Encarregado na Autoridade Nacional, mas prevê que a identidade e as informações de contato do Encarregado devem ser divulgadas publicamente, de maneira clara e objetiva, preferencialmente no site da empresa);
- Revisar contratos com clientes, fornecedores, parceiros e empregados, que tenham relação com o tratamento de dados pessoais;

- Identificar as normas aplicáveis à empresa (gerais e específicas do setor) – isso é importante para fins de mapeamento de dados e atribuição de bases legais;
- Criar uma equipe multidisciplinar dentro da empresa com a participação de representantes das áreas envolvidas no projeto de adequação à LGPD (por exemplo, RH, marketing, vendas, pesquisa etc.);
- Fazer mapeamento de dados – este é um passo importante para identificar as práticas da empresa em relação aos dados pessoais, bem como para identificar possíveis riscos e procedimentos que precisem ser ajustados;
- Revisar as políticas da empresa, de forma a adequar-se aos procedimentos previstos na LGPD;
- Revisar ou criar formulários de consentimento, conforme necessário;
- Preparar Relatórios de Impacto para as atividades de processamento de dados pessoais baseadas em interesses legítimos – de acordo com a LGPD, a ANPD também pode determinar que o controlador prepare o relatório em relação com outras atividades de processamento de dados, inclusive relacionadas a dados sensíveis;
- Instituir obrigatoriedade na participação dos empregados em treinamentos e distribuir material de conscientização. ■

CYBERSECURITY & DATA PRIVACY

A capacidade da tecnologia atual em trabalhar dados potencializa o desempenho de empresas de todos os setores. Tais dados digitais carregam informações estratégicas a seus negócios e, por isso, a proteção dos sistemas de tecnologia da informação e de suas informações é um dos maiores desafios no mundo dos negócios.

Sempre antecipando tendências, TozziniFreire Advogados conta com uma equipe especializada para oferecer, entre outros, os seguintes trabalhos: desenvolver estratégias abrangentes para a mitigação de riscos legais associados à utilização, divulgação e armazenamento de informações e dados; orientar sobre veiculação on-line de materiais publicitários e comerciais; orientar quanto à conformidade com as leis, regulamentos e melhores práticas, envolvendo a privacidade, a segurança das informações e a responsabilidade de provedores na internet; orientar na condução de auditorias de privacidade e segurança; revisar e elaborar políticas de privacidade e termos de uso de websites, em caráter preventivo; redigir contratos de compra e venda e troca de bases de dados, bem como orientar sobre a guarda e transmissão de dados; atuar, nas esferas cível e criminal, em disputas relacionadas a potenciais falhas de segurança da informação, inclusive adotando medidas judiciais de urgência para a proteção de dados maliciosamente divulgados na Internet, bem como em disputas relacionadas com órgãos de defesa do consumidor envolvendo relações de consumo realizadas em meios digitais.

Nossos profissionais têm atuação reconhecida por renomados guias e rankings internacionais como *Chambers and Partners*, *Latin Lawyer 250* e *Legal 500* e forte interação com os diferentes grupos de prática ou de setor de indústria do escritório, fornecendo um apoio completo para qualquer desdobramento dos casos – um apoio que só uma banca full-service do nosso porte consegue oferecer.

Nossa equipe se coloca à disposição para assessorá-los em qualquer questão que se mostre necessária.

CONTATOS



**MARCELA
W. EJNISMAN**

Sócia | Cybersecurity & Data Privacy
mejnisman@tozzinfreire.com.br



**CARLA DO COUTO
HELLU BATTILANA**

Sócia | Cybersecurity & Data Privacy
ccouto@tozzinfreire.com.br