LEFOSSE
ADVOGADOS

15 de agosto de 2018

Promulgada a Lei nº 13.709/2018, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais ("**LGPD**") foi promulgada no último dia 14 de agosto, estabelecendo um marco legal para a proteção da privacidade e dos dados pessoais no Brasil. A nova Lei prevê proteção específica à privacidade e aos dados pessoais dos cidadãos, determinando como as empresas, organizações e poder público deverão coletar, usar, processar e armazenar esses dados no desempenho de suas atividades.

Assim como a ***General Data Protection Regulation* – GDPR**, que entrou em vigor na União Europeia em 25 de maio deste ano e inspirou a redação da nova Lei, a LGPD representa uma mudança radical sobre a forma como a privacidade é tratada no Brasil. Isso porque a LGPD **confere** às pessoas físicas, chamadas de **titulares de dados, maior controle e autonomia sobre seus dados pessoais**, os quais somente poderão ser coletados, usados, processados e armazenados nos estritos limites das normas previstas na nova Lei, as quais estão em linha com os mais avançados padrões internacionais sobre o tema.

A LGPD **entrará em vigor após 18 meses** de sua promulgação, o que ocorrerá somente em **2020**, de modo que as empresas e organizações públicas e privadas terão um prazo razoável para se adequarem às novas regras.

Em resumo, a LGPD traz as seguintes inovações:

- Estabelece **10 hipóteses legais que autorizam o tratamento de dados**, tais como o **consentimento** do titular, **interesses legítimos** do controlador (i.e., aquele a quem compete as decisões referentes ao tratamento de dados pessoais), para o cumprimento de **obrigação legal ou regulatória**, quando necessário para a **execução de um contrato**, dentre outras hipóteses;
- Critérios mais rígidos para o tratamento de **dados pessoais sensíveis**, definidos como sobre origem racial ou étnica, a convicção religiosa, a opinião política, a 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;
- Estabelece **princípios** que deverão nortear as atividades de tratamento, tais como o da **finalidade**, que estabelece que os dados pessoais somente poderão ser tratados para propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de maneira incompatível com essas finalidades;
- **Direitos dos titulares de dados** deverão ser observados, tais como o **direito de acesso aos dados**, de **retificação**, **cancelamento** ou **exclusão** dos dados, **direito de oposição** ao tratamento com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento da Lei, **direito de revogar o consentimento** fornecido, os **direitos de informação e de explicação** sobre a utilização de seus dados, direito à **portabilidade** dos dados pessoais, dentre outros;

- Estabelece regras específicas para o **tratamento de dados pessoais de crianças e adolescentes**;
- Estabelece critérios bastante rígidos para a **transferência internacional de dados pessoais**;
- Cria a figura do "**Encarregado de Proteção de Dados**" (ou ***Data Protection Officer* – DPO**), que deverá ser nomeado pelas empresas, em determinadas circunstâncias, para ser o responsável por garantir a conformidade com a LGPD e com os atos administrativos da autoridade de proteção de dados. Pode ser um diretor, um gerente, um funcionário, ou até mesmo um escritório terceirizado, bastando que tenha autonomia para exercer suas funções;
- Estabelece um regime de **responsabilização do controlador e operador de dados pessoais**, o que exigirá uma definição muito clara, nos contratos firmados entre ambos, sobre as atividades a serem desempenhadas por cada um deles;
- Impõe a adoção **de medidas de segurança 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 qualquer forma de tratamento inadequado ou ilícito;
- Impõe uma obrigação de ***privacy by design*** ao estabelecer que as **medidas de segurança** visando à proteção de dados pessoais deverão ser observadas **desde a fase de concepção** do produto ou do serviço **até sua execução**.
- Incentiva os controladores e operadores a formular **regras de boas práticas e de governança** relacionados ao tratamento de dados;
- Estabelece a **obrigatoriedade de comunicação**, em prazo razoável, à autoridade de proteção de dados e aos titulares de dados, sobre a ocorrência de **incidentes de segurança da informação** que possam acarretar **risco ou dano relevante** aos titulares de dados pessoais;
- Previsão de **sanções administrativas** a serem impostas aos agentes de tratamento por eventuais infrações às normas da LGPD, incluindo **multa** de até **2% do faturamento da empresa, grupo ou conglomerado no Brasil** no seu último exercício, excluídos os tributos, **limitadas**, no total a **R$ 50.000.000,00** por infração.

A redação original do Projeto de Lei aprovado pelo Senado previa a criação da **Autoridade Nacional de Proteção de Dados Pessoais (ANPD)**, que seria autarquia federal vinculada ao **Ministério da Justiça**, que terá a incumbência de f**iscalizar a aplicação da LGPD.** Entretanto, esse dispositivo foi vetado pela Presidência da República, sob a justificativa de que havia um vício de iniciativa no processo legislativo. Entretanto, a autoridade deverá ser criada por meio de Projeto

de Lei de iniciativa do Poder Executivo, o que deverá ocorrer bem antes da entrada em vigor da LDPG.

A LGPD trará impactos bastante significativos na economia, resultando em profundas transformações nos modelos de negócios existentes de todas as entidades que atuam com tratamento de dados pessoais. A Lei deverá impactar atividades de instituições financeiras, hotéis, agências de turismo, hospitais, planos de saúde, farmácias, restaurantes, varejistas, universidades, provedores de serviços de internet, prestadores de serviços de telecomunicações, empresas de tecnologia, provedores de serviços de computação em nuvem, agências de publicidade, escritórios de advocacia, órgãos públicos e dentre outras.

Além disso, a nova Lei também afetará diretamente as relações entre fornecedores de produtos e serviços e seus clientes, relações de consumo, relações entre empregadores e seus empregados, dentre outras relações que impliquem coleta e tratamento de dados, tanto no ambiente online como offline.

A seguir nossas breves considerações sobre a LGPD:

Escopo de aplicação da lei

A LGPD se aplica a **qualquer operação de tratamento de dados pessoais** realizada por **pessoa física ou jurídica de direito público ou privado**, que (i) **seja realizada no Brasil**; (ii) tenha por **objetivo a oferta ou fornecimento de bens ou serviços** ou o **tratamento de dados pessoais** de **indivíduos localizados no território nacional**; **ou** (iii) envolva **dados pessoais coletados no Brasil**, independentemente do meio, do país de sede da pessoa jurídica ou do país onde estejam localizados os dados.

Assim com a GDPR, a LGPD também tem, portanto, aplicação extraterritorial, isto é, aplica-se mesmo a empresas estrangeiras, bastando que tenha filial ou subsidiária no Brasil, ofereça bens ou serviços no mercado nacional, ou colete dados pessoais de indivíduos localizados no país.

A LGPD não será aplicável ao tratamento de dados pessoais:

- realizado por pessoa natural para fins particulares;
- para fins jornalísticos, artísticos ou acadêmicos;
- para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (neste último caso, deverá haver legislação específica); ou
- provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado com agentes de tratamento brasileiros ou objeto de transferência de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Conceito de dados pessoais

"**Dado pessoal**" é definido pela LGPD como **qualquer informação relacionada à pessoa natural identificada ou identificável (chamado de "titular de dados")**. Desse modo, uma pessoa poderá ser considerada identificável se puder ser identificada, direta ou indiretamente, especialmente por referência a um identificador, como um nome, um número de identidade, CPF, dados de localização, identificadores eletrônicos como o número de IP, bem como elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa.

Conceito de "dados pessoais sensíveis"

A LGPD define "**dado pessoal sensível**" como dado pessoal sobre **origem racial ou étnica**, **a convicção religiosa**, **a opinião política**, **a 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**.

Vale destacar que os dados pessoais sensíveis são objeto de requisitos ainda mais rígidos para a seu tratamento.

Dados anonimizados

Dado anonimizado é definido como como **dado relativo a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento**. Por meio de um processo de anonimização, um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. Desse modo, dados anonimizados estão fora do escopo de aplicação da LGPD.

Tratamento de dados

A LGPD define **tratamento de dados** como **qualquer 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.

Em suma, qualquer atividade realizada utilizando-se dados pessoais está abrangida nesse conceito, fazendo incidir a aplicação da LGPD.

Agentes de tratamento

São considerados **agentes de tratamento**, isto é, aqueles que efetivamente coletam e utilizam os dados pessoais, como sendo (i) **o controlador**, isto é, a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, e o (ii) **operador de dados**, definido como a pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Normalmente, o controlador contrata um operador para que este realize o tratamento dos dados. Por exemplo, uma empresa pode contratar um prestador de serviços para realizar o tratamento de dados de seus funcionários. Neste caso, a parte contratante (empregador), será considerada o controlador, enquanto a prestadora dos serviços será a operadora dos dados. De qualquer modo, não raro uma mesma entidade pode exercer as duas funções, sendo controladora e operadora dos dados.

Princípios

A LGPD elenca um rol de princípios que deverão nortear as atividades de tratamento de dados, quais sejam:

- **Finalidade**: os dados pessoais somente poderão ser tratados para propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de maneira incompatível com essas finalidades;
- **Adequação**: o tratamento dos dados deve ser compatível com as finalidades informadas ao titular;
- **Necessidade**: o tratamento dos dados deve ser limitado ao mínimo necessário para a realização de suas finalidades;
- **Livre acesso**: os titulares poderão consultar de maneira facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade dos seus dados pessoais;
- **Qualidade dos dados**: aos titulares de dados serão garantidas a exatidão, clareza, relevância e atualização dos dados, em conformidade com a necessidade e finalidade do tratamento;
- **Transparência**: garantia aos titulares de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (respeitados os segredos comerciais e industriais);
- **Segurança**: utilização de medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de incidentes ou ilicitudes que levem à destruição, perda, alteração, comunicação ou difusão dos dados;
- **Prevenção**: adoção de medidas preventivas contra a ocorrência de eventuais danos decorrentes do tratamento de dados;
- **Não discriminação**: proibição de tratamento de dados para fins discriminatórios, ilícitos ou abusivos;
- **Responsabilização e prestação de contas (*accountability*)**: o agente de tratamento deverá demonstrar a adoção de medidas eficazes e capazes de comprovar a observância

e o cumprimento das normas de proteção de dados pessoais, inclusive da eficácia das medidas.

Requisitos legais para o tratamento de dados

A LGPD elenca 10 requisitos legais pelos quais os dados pessoais poderão ser tratados:

- Mediante o **consentimento** do titular de dados pessoais;
- Para o **cumprimento de obrigação legal ou regulatória** do controlador;
- Pela **Administração Púbica**, para tratamento de dados necessários à **implementação de políticas públicas**;
- Para a realização de **estudos por órgãos de pesquisa**, sendo garantida a anonimização;
- Quando necessário para a **execução de contrato**;
- **Como uma forma de exercício regular de direitos** em processo judicial, administrativo ou arbitral;
- Para a **proteção da vida ou incolumidade física**;
- Para a **tutela da saúde**, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- **Interesses legítimos** do controlador ou de terceiros, exceto no caso de prevalecerem direitos fundamentais do titular dos dados pessoais;
- **Proteção do crédito**, nos termos da legislação aplicável.

Ainda que alguns dos requisitos legais acima descritos possam parecer subjetivos, devendo, portanto, ser objeto de regulamentação, destacamos abaixo as hipóteses de (i) consentimento do titular e de (ii) interesses legítimos do controlador ou de terceiros, que, a nosso ver, deverão gerar maior discussão e dúvidas para fundamentar operações de tratamento de dados.

De qualquer modo, seja qual for a base legal para o tratamento de dados, esta decisão deve ser devidamente registrada e documentada pelo controlador e operador de dados.

Consentimento

O consentimento é definido pela LGPD como a **manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada**.

O consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular dos dados. No caso de consentimento por escrito, este deverá constar de **cláusulas destacadas das demais cláusulas do contrato**. O **consentimento deverá referir-se**

a finalidades determinadas e serão **nulas as autorizações genéricas**. Desse modo, em caso de mudança da finalidade para o tratamento de dados pessoais não compatível com o consentimento originalmente fornecido, o controlador deverá informar previamente o titular dos dados sobre a alteração, o que na prática corresponde à obtenção de novo consentimento.

O **consentimento poderá ser revogado a qualquer tempo**, mediante manifestação expressa do titular de dados, por meio de procedimento gratuito e facilitado.

No caso de **dados pessoais sensíveis**, o **consentimento** deverá ser fornecido de maneira **específica e destacada, para finalidades específicas**, sendo dispensável apenas em hipóteses restritas previstas na LGPD.

Na prática, os novos requisitos para o fornecimento de consentimento representam o fim dos longos e ambíguos termos de serviços e políticas de privacidade que conferem poderes quase absolutos aos agentes que coletam dados pessoais para fins genéricos e indefinidos, que podem ser até prejudiciais aos titulares dos dados.

Interesses legítimos do controlador

De acordo com a LGPD, o **legítimo interesse do controlador** somente poderá fundamentar tratamento de dados pessoais para **finalidades legítimas**, consideradas a partir de **situações concretas**, tais como apoio e promoção de atividades do controlador, proteção em relação ao titular de dados, do exercício regular de seus direitos ou a prestação de serviços que o beneficiem. Dessa forma, quando houver hipóteses claras em que o tratamento de dados é necessário para atender a interesses legítimos do controlador, o consentimento do titular poderá ser dispensado.

O tema dos interesses legítimos do controlador como fundamento para o tratamento de dados pessoais tem gerado bastante discussão na Europa, já que esta hipótese também está prevista na GDPR e não há clareza sobre quais as situações práticas em que o interesse legítimo do controlador poderá ser invocado para legitimar operações de tratamento de dados. Por exemplo, uma empresa ou organização poderia ter interesse legítimo quando o tratamento for efetuado no âmbito da relação com um cliente, quando realizar o tratamento de dados pessoais para fins de marketing direto, para prevenir fraudes, ou mesmo para garantir a segurança da rede e da informação nos seus sistemas de tecnologia da informação e comunicação.

Seja qual for o fundamento para o tratamento de dados com base no interesse legítimo do controlador, será necessário **ponderar os interesses do controlador e os direitos do titular dos dados**, nos termos da LGPD. Na prática, ainda que existam claras justificativas para o tratamento com base no legítimo interesse do controlador, o titular deverá ser sempre informado sobre esse fato e seus direitos e liberdades não poderão ser impactos adversamente. Caso contrário, o controlador não poderá valer-se do interesse legítimo como justificativa para o tratamento dos dados.

De qualquer modo, o legítimo interesse deverá constituir importante fundamento legal para o tratamento de dados por empresas de tecnologia que atuam em inovação orientada em dados, como *data mining*, *data analytics*, inteligência artificial, *machine learning*, bem assim para instituições financeiras, seguradoras, operadoras de telecomunicações, empresas que atuam na área da saúde, dentre outras.

Direitos dos titulares

A LGPD deixa claro que toda a pessoa natural tem assegurada a titularidade de seus dados pessoais, garantindo-se os direitos fundamentais de liberdade, de intimidade e de privacidade. Dentre os direitos assegurados pela LGPD, destacam-se o **direito de acesso aos dados**; de **retificação**, **cancelamento** ou **exclusão** dos dados; **direito de oposição** ao tratamento; **direito de revogar o consentimento fornecido**; bem como os **direitos de informação** e de **explicação** sobre a utilização de seus dados.

A LGPD também prevê o **direito à portabilidade** de dados pessoais a outro fornecedor de serviço ou produto, mediante solicitação expressa do titular. Por exemplo, o titular de dados pode solicitar que um provedor de *streaming*, como o *Spotify*, forneça seus dados pessoais para um serviço de *streaming* concorrente.

Importante ressaltar, nesse contexto, que a autoridade de proteção de dados poderá determinar padrões de interoperabilidade para fins de portabilidade e livre acesso aos dados.

Destaca-se também o **direito do titular de solicitar a revisão, por pessoa física, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais**, inclusive aquelas **decisões** destinadas a definir o seu **perfil pessoal**, **profissional**, de **consumo**, de **crédito** ou os **aspectos de sua personalidade**. O controlador deverá fornecer ao titular dos dados, quando este solicitar, **informações claras e adequadas** a respeito dos **critérios** e dos **procedimentos** utilizados **para a decisão automatizada**. Esse "direito de revisão humana", ou de "explicação" de decisões automatizadas, deverá impactar as empresas que utilizam meios tecnológicos automatizados para avaliar aplicações de crédito, recrutamento e seleção, seguros, disponibilidade de serviços de telecomunicações, dentre outros.

Crianças e adolescentes

A LGPD estabelece regras específicas para o **tratamento de dados de crianças e adolescentes**, que deverá ser realizado mediante **consentimento específico e em destaque dado por pelo menos um de seus pais ou de seu responsável legal**, salvo nos casos em que seja necessário coletar dados para contatar os pais ou responsável legal.

Transferência internacional de dados pessoais

A LGPD prevê diversas hipóteses em que a transferência internacional de dados poderá ser realizada, com destaque para:

- Transferência realizada **para países** ou **organizações internacionais que proporcionem grau de proteção de dados pessoais adequado** ao previsto na LGPD;
- Quando o **controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados** previstos na LGPD por meio de **cláusulas contratuais específicas para uma transferência**, **cláusulas-padrão**, **normas corporativas globais**, **selos**, **certificados** e **códigos de conduta**, regularmente emitidos pela autoridade de proteção de dados;
- Quando a transferência for **necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e de persecução**;
- Quando o titular tiver fornecido o seu **consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação**, distinguindo claramente esta de outras finalidades.

Tratamento de dados pelo poder público

A LGPD estabelece que o tratamento de dados pelo poder público deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

- Sejam informadas as hipóteses em que realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades;
- Seja indicado um Encarregado de Proteção de Dados quando realizarem operações de tratamento de dados pessoais.

Ademais, a Lei ainda prevê que **as empresas públicas e as sociedades de economia mista que atuem em regime de concorrência, explorando atividade econômica, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado**. Já as estatais que atuem na implementação de políticas públicas terão o mesmo tratamento dispensado aos órgãos e às entidades do poder público.

Com relação ao compartilhamento de dados pelo Poder Público, a LGPD estabelece que os dados devem ser mantidos em formato interoperável e estruturado para uso compartilhado. O compartilhamento deve atender a finalidades específicas de execução de políticas públicas e

atribuição legal pelos órgãos e pelas entidades públicas. Por outro lado, **é vedado ao Poder Público transferir a entidades privadas dados pessoais, exceto**:

- em casos de execução descentralizada de atividade pública que exija a transferência, observado o disposto na Lei de Acesso à Informação;
- nos casos em que os dados forem acessíveis publicamente.

Em regra, caso ocorra o compartilhamento de dados entre órgãos públicos e entidades privadas, fora das hipóteses indicadas acima, ou caso não se configure uma das hipóteses de dispensa de consentimento previstas na Lei, será obrigatório comunicar a autoridade de proteção de dados sobre referido compartilhamento e obter consentimento prévio do titular.

Relatórios de impacto

Os agentes de tratamento devem manter **registro de todas as operações de tratamento de dados** pessoais que realizarem, especialmente quando baseado no legítimo interesse. Nesse contexto, a LGPD estabelece que a autoridade de proteção de dados poderá determinar ao controlador que elabore **relatório de impacto à proteção de dados pessoais**, documentação contendo a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Esse relatório de impacto deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a sua coleta e para a garantia da segurança das informações, bem como a análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Encarregado de Proteção de Dados (Data Protection Officer – DPO)

A LGPD determina que o operador deverá indicar um **encarregado pelo tratamento de dados pessoais**. O termo "**encarregado**" advém da versão portuguesa da GDPR, equivalente ao *Data Protection Officer* – DPO. Esse encarregado deverá ser a pessoa física responsável por garantir a conformidade da empresa com a LGPD. Pode ser um diretor, um gerente, um funcionário, ou até mesmo um escritório terceirizado, bastando que tenha autonomia para exercer suas funções.

Caberá ao Encarregado de Proteção de Dados: (i) **aceitar reclamações e comunicações dos titulares**, prestar esclarecimentos e adotar providências; (ii) **receber comunicações** da autoridade de proteção de dados e adotar providências; (iii) **orientar os funcionários e os contratados** da entidade a respeito das **práticas a serem tomadas em relação à proteção de dados**; e (iv) **executar as demais atribuições** determinadas pelo **controlador** ou estabelecidas em normas complementares.

De qualquer modo, entendemos que a autoridade de proteção de dados poderá dispensar a necessidade de sua indicação. Realmente, não faz sentido impor a obrigação de indicação de um Encarregado para todas as empresas e organizações. Nada impede que, a depender da organização interna da empresa ou entidade, esse cargo seja absorvido pela área responsável pelo *compliance*, pelo jurídico ou até mesmo pela área de recursos humanos.

Responsabilidade dos agentes de tratamento

O **controlador ou o operador** que, em razão do exercício de atividades de tratamento, **causar dano patrimonial, moral, individual ou coletivo**, em violação da LGPD, será obrigado a **repará-lo**. Salvo em casos excepcionais, **o operador responderá solidariamente** pelos dados quando **descumprir a LGPD** ou quando **não tiver seguido as instruções lícitas do controlador**, hipótese em que o operador será equiparado ao controlador. Já os **controladores** que estiverem **diretamente envolvidos em atividades de tratamento** que causarem danos ao titular dos dados, serão **solidariamente responsáveis**.

Assim, caso o operador atue em conformidade com a LGPD e atenda rigorosamente às instruções do controlador, não será solidariamente responsável por eventuais danos causados pelo controlador aos titulares de dados. Da mesma forma, o controlador que não participe do tratamento do qual decorram os danos aos titulares, não será solidariamente responsável por danos causados pelo operador. Desse modo, ao redigir contratos entre controlador e operador, é altamente recomendável que uma definição clara das atribuições de cada parte e das limitações de responsabilidade, de modo a mitigar riscos, evitar penalidades desnecessárias e garantir eventual direito de regresso.

Segurança da informação

A LGPD estabelece a obrigação para os agentes de tratamento de adoção de **medidas de segurança** 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 qualquer forma de tratamento inadequado ou ilícito.

Privacy by design

Inspirada na GDPR europeia, a LGPD incorporou o conceito de "***privacy by design***", ao estabelecer que as **medidas de segurança** visando à proteção de dados pessoais deverão ser observadas **desde a fase de concepção** do produto ou do serviço **até sua execução**.

Na prática, o conceito de ***privacy by design*** significa que o risco de privacidade deve ser levado em conta em todo o processo de concepção de uma nova tecnologia, produto, serviço ou modelo de negócio. Isso inclui projetos internos, desenvolvimento de produtos, desenvolvimento de software, sistemas de TI, dentre outros. Desse modo, será necessário garantir que privacidade e proteção de dados sejam incorporadas durante todo o ciclo de vida do sistema ou processo. Na prática, o conceito deverá afetar diretamente agentes que atuam em pesquisa, desenvolvimento e inovação, especialmente desenvolvedores de software e hardware.

Comunicação de incidentes

A LGPD obriga o controlador a **comunicar à autoridade de proteção de dados e aos titulares de dados a ocorrência de incidentes de segurança da informação** que possam acarretar **risco ou dano relevante** aos titulares de dados pessoais. Essa comunicação deverá

ocorrer em **prazo razoável**, a ser definido pela **autoridade de proteção de dados** , e deverá mencionar, no mínimo:

- **Descrição** e **natureza** dos dados pessoais afetados;
- Informações sobre os **titulares envolvidos**;
- Indicação das **medidas técnicas e de segurança utilizadas** para a proteção dos dados;
- Os **riscos** relacionados ao incidente;
- Os **motivos da demora**, no caso de a comunicação não ter sido imediata;
- As **medidas** que foram ou que serão **adotadas** para **reverter ou mitigar** os efeitos do prejuízo.

A depender da **gravidade do incidente**, a autoridade de proteção de dados poderá determinar ao controlador providências adicionais, tais como a **ampla divulgação** dos fatos em meios de comunicação e **medidas** para reverter ou mitigar os efeitos do incidente.

Sanções administrativas

As infrações às normas da LGPD poderão sujeitar os agentes de tratamento às seguintes sanções administrativas aplicáveis pela autoridade de proteção de dados, após procedimento administrativo que assegure a ampla defesa:

- **Advertência**, com indicação de prazo para a adoção de medidas corretivas;
- **Multa** de até **2% do faturamento** da empresa, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, **limitadas**, no total a **R$ 50.000.000,00** por infração;
- **Multa diária**, observado o limite total acima indicado;

- **Publicização da infração** após devidamente apurada e confirmada;
- **Bloqueio de dados pessoais** a que se refere a infração até sua regularização;
- **Eliminação dos dados pessoais** a que se refere a infração.

* * *

CONTATOS:

Para informações adicionais, entre em contato:

Zeca Berardo
zeca.berardo@lefosse.com
Tel.: (+55) 11 3024 6244

Paulo Lilla
paulo.lilla@lefosse.com
Tel.: (+55) 11 3024 6347

Elen Lizas
elen.lizas@lefosse.com
Tel.: (+55) 11 3024 6391

Lefosse Advogados
Rua Tabapuã, 1227 14º andar
04533-014 São Paulo SP Brasil

Avenida Presidente Wilson, 231 conj. 2703
20030-905 Rio de Janeiro RJ Brasil