LEI GERAL DE PROTEÇÃO DE DADOS

PARA O SEU ESCRITÓRIO

OAB MINAS GERAIS

13ª Subseção uberlândia

Comissão de Privacidade e Proteção de Dados

LGPD

PARA O SEU ESCRITÓRIO

Todos os direitos reservados. 2024

Sobre a Comissão de Privacidade e Proteção de Dados

A Comissão de Privacidade e Proteção de Dados da 13ª subseção da OAB/MG (Uberlândia), surgiu com o propósito de propagar conhecimento sobre a regulamentação, o controle e a fiscalização do tratamento de dados pessoais, garantindo a privacidade e proteção dos direitos dos titulares de informações. Também tem como objetivo contribuir com o debate e facilitar o dia a dia de quem pretende valer-se da LGPD a seu favor.

@comissaoppdudia

@comissaoppdudia

ÍNDICE

APRESENTAÇÃO

A Lei nº 13.709 (Lei Geral de Proteção de Dados ou LGPD) foi promulgada em agosto de 2018 para dispor, nos termos do artigo 1º, sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A legislação tem o seu âmbito de aplicação delimitado nos artigos 3º e 4º, sendo inequívoca a vinculação dos escritórios de advocacia e advogados autônomos que atuam em território nacional, haja vista que são prestadores de serviços para terceiros, mesmo quando se tratar de advocacia *pro bono*.

Com isso em mente, a Comissão de Privacidade e Proteção de Dados vinculada à 18ª Subseção de Minas Gerais da Ordem dos Advogados do Brasil promoveu o workshop intitulado "LGPD para seu escritório", nos dias 18 e 19 de maio de 2022, na própria sede da Subseção, no intuito de abordar aspectos teóricos introdutórios acerca da legislação, assim como questões práticas para orientar a implementação da Lei nos escritórios de advocacia pelos próprios advogados.

O workshop teve como palestrantes os próprios membros da Comissão (nomeadamente Aline Carneiro, Ana Cristina Stoco de Faria, Ana Paula Bougleux Andrade Resende, Ana Vitória D'Assumpção Guzman, Atila Pereira Lima, Débora de Oliveira Côco, João Victor Doreto e Pedro Augusto Abbot Soares), que compartilharam parte do seu conhecimento teórico e de sua experiência prática com toda a comunidade jurídica, sendo o público alvo do evento não apenas advogados, mas também assistentes jurídicos, estagiários, estudantes e demais interessados.

Diante dos elogios ao evento e subsistindo a relevância da temática, no ano em que a publicação da legislação completou cinco anos, tomou-se a iniciativa de elaborar um e-book capaz de consolidar tudo o que foi tratado no workshop.

Assim, a presente publicação contou com a colaboração de membros da Comissão de Privacidade e Proteção de Dados (quais sejam, Aline Lemes, Ana Cristina Stoco de Faria, Ana Paula Bougleux Andrade Resende, Ana Vitória D'Assumpção Guzman, Débora de Oliveira Côco, João Victor Doreto, Lorena Rochael Mello e Sarah Carolina de Sales Globo), que subscrevem os capítulos que compõem esta publicação, cabendo a ressalva de que cada capítulo reflete exclusivamente o ponto de vista de quem o elaborou, sendo certo que seu o conteúdo não necessariamente corresponde ao posicionamento de todos os membros da Comissão.

A seguir, serão abordados os seguintes assuntos: (1) Breve introdução da LGPD, (2) Direitos dos titulares e canal de atendimento, (3) Hipóteses de tratamento de dados pessoais, (4) Agentes de tratamento e outros atores, (5) Responsabilidades entre agentes de tratamento, (6) Boas práticas e governança de dados pessoais, (7) Aspectos básicos de segurança da informação, (8) Fluxo de implementação da Lei Geral de Proteção de Dados, (9) Documentos internos importantes em proteção de dados pessoais.

Como é de se imaginar, a ideia de mesclar aspectos teóricos e práticos permaneceu, sendo este um subsídio para a adequação à LGPD por parte de escritórios de advocacia, ou até mesmo para auxiliar nos processos de melhoria e aprimoramento.

Por último, mas não menos importante, cabe destacar a contribuição imprescindível da membra da Comissão, Sarah Carolina de Sales Globo, que se dispôs a editar este e-book, na intenção de tornar a sua leitura mais interessante.

Boa leitura a todos!

Ana Paula Bougleux Andrade Resende

Coordenadora da obra

BREVE INTRODUÇÃO

Por Sarah Carolina de Sales Globo*

É um fato que vivemos em uma era tecnológica. As mídias sociais, aplicativos e sites cresceram exponencialmente nas últimas décadas, e com eles o volume de dados pessoais produzidos e em trânsito. Desde número de telefone, nome, e-mail até quais pesquisas são realizadas em buscadores de internet, quais compras são feitas com frequências e em qual período do mês. Todos esses dados, facilmente localizáveis, representam valor nas mãos de quem sabe como utilizá-los.

Diante desse cenário, ao longo dos anos foram editadas legislações que visavam regular e proteger dados pessoais ao redor do mundo. O Brasil, nesse sentido, também conta com normas que visam proteger os direitos relacionados à privacidade e intimidade. Em ordem cronológica podemos facilmente verificar:

- Constituição Federal da República Federativa do Brasil de 1988.
- O Código de Defesa do Consumidor (Lein°.8.078/90).
- Lei n°.12.527/2011 (Lei do Acesso à informação).
- Lei n°.12.965/2014 (Marco Civil da Internet).
- Lei n°13.709/2018 (Lei Geral de Proteção de Dados).
- Lei n°13.853/2019 (Lei que cria a Autoridade Nacional de Proteção de Dados).

Desta forma, podemos dizer que a Lei Geral de Proteção de Dados (LGPD) representa a consolidação das legislações que antes protegiam a intimidade e os dados pessoais, complementando-as e estabelecendo diálogo, e não confrontando-as.

Dentre os objetivos da LGPD, é possível afirmar o intuito de preservar a privacidade e proteção dos dados dos titulares em face de atividades comerciais exploradoras dessas informações.
Isso não importa, contudo, em obstar a livre iniciativa e a livre concorrência, mas em traçar balizas para o tratamento adequado dessas informações.

Para que seja efetivamente entendida e aplicada, faz-se necessário que alguns novos conceitos cheguem ao conhecimento de todos. Ressalta-se que a Lei é de aplicação em todos os meios, tanto físicos quanto digitais.

*Advogada, pós-graduada em Advocacia Cível e Lei Geral de Proteção de Dados, DPO na Orion Soluções T.I; membro da Comissão de Privacidade e Proteção de Dados da OAB Uberlândia.

Cumpre, primeiramente, destacar que a Lei traz em seu artigo 2° os fundamentos basilares que a compõem. Dentre eles, destaca-se o princípio da autodeterminação informativa que corresponde ao direito do titular de dados pessoais decidir compartilhar ou não seus dados, bem como quais dados serão ou não compartilhados, visando transferir ao titular de dados pessoais o real controle sobre eles.

Já o artigo 5° da lei traz as definições dos principais conceitos. A seguir, destacamos alguns deles.

Dado Pessoal e Titular de dados

- Dado Pessoal é informação relacionada a pessoa natural identificada ou identificável. Poderá ser direto, como: nome, altura, RG, CPF, endereço e telefone. Ou indireto, como: foto, geolocalização e perfil comportamental. Em suma, toda informação que se permita relacionar a uma pessoa pode ser considerada dado pessoal.
- Dado pessoal sensível é o 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 à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Merece mais atenção, pois pode indicar convicções íntimas ou gerar situações de discriminação e vulnerabilidade, de modo a causar transtornos graves caso não sejam tratados da maneira correta. Sem dúvidas, os dados pessoais sensíveis ensejam maior cuidado e ponderação quanto a sua utilização.
- Titular de dados pessoais: é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. Note-se que aqui o texto da lei menciona expressamente "pessoa natural", assim, não se incluem as pessoas jurídicas.

Tratamento de dados pessoais

Tratamento de dados refere-se a toda operação realizada com dados pessoais, como 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.

O tratamento de dados pessoais representa a ação, o fazer. Toda operação em que constar o dado pessoal de uma pessoa natural identificada ou identificável, ressalvadas as hipóteses trazidas pelo seu artigo 4°, deverá cumprir a LGPD.

Quando se fala em tratamento de dados pessoais, deve-se ter em mente o seu ciclo de vida.
O ciclo de vida nada mais é do que o percurso que o dado percorre desde que surge até o momento em que é descartado. Em síntese temos:

Coleta: Obtenção, recepção ou produção independente do meio utilizado (documento em papel, meio eletrônico, sistema, aplicativos, etc.)

Armazenamento: Arquivamento ou armazenamento independente do meio utilizado.

Uso: Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação.

Transferência: Transmissão, distribuição, comunicação, transferência, difusão e compartilhamento.

Eliminação: Operação que visa deletar ou eliminar, contemplando ainda o descarte de ativos organizacionais.

Agentes de tratamento

Controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. É o controlador quem decidirá como os dados serão tratados e quais serão as formas de tratamento.

Operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O operador age em nome do controlador, ou seja, traduz os comandos do controlador.

Autoridade Nacional de Proteção de Dados

Importante, ainda, conhecer a Autoridade Nacional de Proteção de Dados (ANPD), pois ela é o órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

É função da ANPD, ainda, editar normativas que visam a plena execução e instrumentalização da LGPD. É ela, ainda, que recebe denúncias dos titulares de dados sobre quaisquer irregularidades quanto ao tratamento de dados pessoais.

Encarregado de Dados

Relevante, também, conhecer a figura do encarregado de dados, que é a pessoa indicada pelo agente de tratamento para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). É função dele ouvir as solicitações, requisições dos titulares, esclarecer dúvidas, levá-las até os agentes de tratamento, responder à ANPD. Ele é o elo entre titular, agentes de tratamento e ANPD.

As premissas e conceitos brevemente abordados acima não têm, nem ao longe, a pretensão de exaurir o rol de pressupostos básicos que envolvem a Lei Geral de Proteção de Dados. São capazes, contudo, de servir o mínimo conhecimento para a leitura e compreensão das considerações apresentadas a seguir.

Comissão de Privacidade
e Proteção de Dados

DIREITOS DOS TITULARES
E
CANAL DE ATENDIMENTO

Por Ana Cristina Stoco

Advogada com experiência em Privacidade e Proteção de Dados
e Governança Corporativa. Analista de Compliance.

Segundo a definição de Rodotà (2008, p. 15), o conceito de privacidade engloba um direito complexo, cujo elemento central é a autodeterminação informativa. Esse direito diz respeito à capacidade de uma pessoa manter controle sobre suas informações e determinar como sua esfera pessoal é construída. A esfera pessoal abrange um conjunto de ações, comportamentos, opiniões, preferências e informações pessoais que o indivíduo deseja manter sob seu controle exclusivo.

Conforme o conceito de privacidade exemplificado acima, a Lei Geral de Proteção de Dados (LGPD) prevê uma ampla gama de direitos dos titulares de dados, garantindo a proteção de sua privacidade e liberdade. Alguns dos principais direitos estabelecidos pela LGPD são:

1. Direito ao acesso facilitado às informações (Art. 9º): O titular tem o direito de ter acesso fácil e claro às informações sobre o tratamento de seus dados pessoais. Isso inclui a finalidade específica do tratamento, a forma e duração do tratamento, a identificação do controlador, informações de contato do controlador, uso compartilhado de dados, responsabilidades dos agentes envolvidos no tratamento e os direitos do titular, conforme descrito no Art. 18 da LGPD.

Exemplo: Uma empresa que coleta dados pessoais de clientes deve fornecer em seu site uma política de privacidade que explique detalhadamente como os dados serão tratados, a finalidade desse tratamento, bem como as informações de contato para que os titulares possam solicitar mais informações ou exercer seus direitos.

2. Titularidade e direitos fundamentais (Art. 17): A LGPD reconhece a titularidade dos dados pessoais e garante os direitos fundamentais de liberdade, intimidade e privacidade para todas as pessoas naturais.

Exemplo: Um indivíduo tem o direito de controlar suas informações pessoais e decidir como elas serão utilizadas. Ele pode decidir compartilhar seus dados com uma empresa, mas também tem o direito de revogar seu consentimento e solicitar a exclusão desses dados quando desejar.

3. Direito à obtenção de informações (Art. 18): O titular dos dados tem o direito de obter do controlador, mediante requisição, uma série de informações relacionadas ao tratamento de seus dados. Isso inclui a confirmação da existência de tratamento, acesso aos dados, correção de informações incompletas ou inexatas, anonimização, bloqueio ou eliminação de dados desnecessários ou tratados de forma inadequada, portabilidade dos dados, eliminação dos dados pessoais tratados com consentimento, informação sobre uso compartilhado de dados e a possibilidade de não fornecer consentimento e suas consequências, revogação do consentimento e revisão de decisões tomadas com base em tratamento automatizado.

Exemplo: Um titular de dados pode solicitar ao controlador que forneça todas as informações que possua sobre ele, corrija dados incorretos ou desatualizados, solicite a exclusão de dados desnecessários ou revogue seu consentimento para o tratamento de seus dados pessoais.

Esses direitos conferidos aos titulares de dados pela LGPD visam empoderar os indivíduos, permitindo-lhes maior controle sobre suas informações pessoais e promovendo uma cultura de proteção e privacidade no tratamento de dados.

Para elucidar os direitos dos titulares, o Serviço Federal de Processamento de Dados (SERPRO) desenvolveu um excelente quadro explicativo, colacionado a seguir:

Disponível em: https://www.serpro.gov.br/lgpd/cidadao/quais-sao-os-seus-direitos-lgpd; acesso em: 10 de maio de 2023.

Ao compreender seus direitos, os titulares de dados têm condições de tomar decisões informadas sobre o compartilhamento e o consentimento para o tratamento de seus dados pessoais.

Eles podem avaliar se as organizações estão seguindo os princípios da LGPD, como a finalidade específica do tratamento, e decidir se desejam ou não fornecer consentimento. Essa consciência permite que os titulares façam escolhas alinhadas com seus interesses e valores.

Além disso, auxilia com a compreensão das responsabilidades dos próprios titulares, como a necessidade de fornecer informações corretas e atualizadas para garantir a precisão dos dados tratados. O entendimento dos direitos conferidos pelo Artigo 18 da Lei promove o empoderamento dos titulares de dados, tornando-os participantes ativos no ecossistema de proteção de dados. Eles podem monitorar e fiscalizar as práticas das organizações em relação ao tratamento de seus dados, denunciar abusos e contribuir para a construção de um ambiente digital mais seguro e ético. Esse engajamento fortalece a cultura de proteção de dados e amplia a conscientização sobre a importância da privacidade.

Canal de Atendimento

O Canal de atendimento ao cliente desempenha um papel fundamental na comunicação e no relacionamento dos agentes de tratamento com seu público. No contexto da Lei Geral de Proteção de Dados (LGPD), esse canal se refere ao atendimento relacionado ao tratamento de dados pessoais.

O Encarregado será o responsável por acompanhar e zelar pelo tratamento de dados pessoais, atuando como um canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Sua função é fiscalizar a conformidade com a LGPD e facilitar a comunicação entre as partes envolvidas.

Existem várias formas de disponibilizar esse atendimento, como a utilização de tecnologias automatizadas de atendimento ao cliente, incluindo Unidade de Resposta Audível (URA) em telefones, Chatbots com Inteligência Artificial, e-mail, entre outros.

Essas ferramentas, por sua vez, permitem interações eficientes e contínuas com os titulares de dados, minimizando possíveis falhas no atendimento.

De acordo com a legislação, é obrigatório que a identidade e as informações de contato do encarregado sejam publicadas no site do controlador, de forma a ser facilmente encontradas tanto pela ANPD quanto pelos titulares dos dados e outros interessados.

Essa transparência é de suma importância, pois os direitos dos titulares (art. 18) são exercidos perante o controlador, que tem a responsabilidade de fornecer informações precisas sobre o tratamento, garantir a correção e eventual exclusão dos dados pessoais, além de receber solicitações de oposição ao tratamento.

É importante ressaltar que o controlador tem a obrigação de processar todas as solicitações recebidas, mesmo que pareçam ilegítimas ou inadequadas. Os prazos de resposta variam de acordo com a natureza da solicitação. Em casos de resposta imediata, pode ser fornecido em formato simplificado. Para respostas mais completas, indicando como os dados foram coletados, a finalidade e os critérios utilizados para o tratamento, o prazo é de até 15 dias.

Exemplos de práticas de atendimento ao cliente alinhadas com a LGPD incluem o fornecimento de respostas claras e detalhadas sobre o tratamento de dados pessoais, a adoção de medidas de segurança para proteger as informações dos titulares e a implementação de processos eficientes para lidar com solicitações de direitos dos titulares, como retificação, exclusão ou oposição ao tratamento.

No contexto do canal de atendimento ao cliente, é essencial que os agentes de tratamento de dados assegurem a conformidade com a LGPD e estabeleçam um ambiente propício para lidar com questionamentos e solicitações relacionadas aos dados pessoais dos indivíduos. Para tanto, é recomendável que as empresas busquem orientação especializada para obter uma compreensão abrangente das diretrizes da LGPD, realizem análises de risco específicas para sua operação e adotem políticas e procedimentos internos claros e consistentes.

A implementação de um canal de atendimento eficiente e seguro, dedicado a responder questionamentos e solicitações dos titulares de dados, é de extrema importância para garantir a transparência e a conformidade com a LGPD. Esse canal deve fornecer respostas esclarecedoras e detalhadas, abordando de forma adequada os direitos dos titulares, como retificação, exclusão e oposição ao tratamento de seus dados pessoais.

Além disso, é essencial que as empresas estejam preparadas para lidar com o fluxo de questionamentos e solicitações de forma eficiente e dentro dos prazos estabelecidos pela legislação. Isso envolve o estabelecimento de processos internos bem definidos para o tratamento e a resposta a essas demandas, além de contar com profissionais capacitados e devidamente informados sobre as obrigações e direitos previstos na LGPD.

Ao adotar essas medidas, os agentes de tratamento demonstram seu compromisso em assegurar a conformidade com a LGPD, fortalecendo a confiança dos titulares de dados e contribuindo para um relacionamento transparente e respeitoso no âmbito do tratamento de dados pessoais.

Comissão de Privacidade
e Proteção de Dados

HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

Por Ana Paula Bougleux Andrade Resende

Advogada, sócia do escritório Guzmán, Finoto e Bougleux Advogados. Especialista em Direito Digital, com certificado pela EXIN (Privacy and Data Protection Essentials - PDPE). Mestra em Direito pela UNESP/Franca. Integrante da Comissão de Privacidade e Proteção de Dados e da Comissão de Direito para Startup da OAB/Uberlândia. Autora de capítulos e artigos em direito digital e proteção de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) está amparada em duas questões fundamentais: (i) a proteção do titular de dados pessoais e (ii) o estabelecimento de condições para o tratamento lícito de dados pessoais. A partir dessa premissa, emergem observações cruciais. A primeira delas é que, por uma opção do Poder Legislativo, adotou-se uma concepção abrangente das operações às quais os dados pessoais são submetidos. Assim, conforme mencionado anteriormente, a referência a tratamento de dados abrange qualquer operação realizada com dados pessoais, de modo que todas as operações referidas estejam submetidas ao regramento estabelecido pela Lei.

Nesse sentido, todo tratamento de dados deve estar fundamentado em uma hipótese legal (também intitulada base legal). Ou seja, o cumprimento das obrigações impostas pela LGPD pressupõe que todo tratamento de dados pessoais esteja justificado por uma das hipóteses legais de tratamento, previstas nos artigos 7º e 11 da Lei. Portanto, o foco deste tópico é elucidar quais são essas hipóteses e destacar aquelas que têm maior pertinência com o desenvolvimento das atividades em um escritório de advocacia.

Antes de abordar as hipóteses propriamente ditas, a segunda observação importante refere-se ao fato de que, em qualquer situação, é indispensável a observância da boa-fé e dos princípios estabelecidos no artigo 6º da Lei, quais sejam, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. No contexto aqui analisado, destacam-se os dois primeiros, estabelecidos nos incisos I e II:

- Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades

- Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento

Assim, a escolha de uma hipótese legal encontra-se diretamente relacionada à finalidade do tratamento previamente estabelecida, bem como à compatibilidade entre o que fora informado ao titular de dados e o tratamento que efetivamente ocorre.

Em uma situação hipotética, em que um contrato de prestação de serviços advocatícios prevê que o cliente (contratante) será comunicado quinzenalmente pelo advogado (contratado) acerca da situação de sua demanda (objeto do contrato), poderia ser considerada irregular a utilização desse meio de contato para fins de divulgação de eventos ou envio de newsletter, por exemplo (a menos que essa finalidade também fosse informada e que, preferencialmente, o cliente tivesse a possibilidade de concordar ou discordar do envio).

A terceira e última observação é relativa à não exclusão de incidência de demais normas que disciplinam o tratamento de dados pessoais, conforme dispõe o artigo 64 da Lei. Assim, em uma relação de consumo, por exemplo, serão aplicadas tanto as normas dispostas no Código de Defesa do Consumidor, quanto na LGPD. De forma análoga, quando da prestação de serviços advocatícios à pessoa natural, será pertinente tanto o disposto na LGPD, quanto no Código de Ética da Ordem dos Advogados do Brasil e demais legislações específicas.

Deve-se destacar, nesse sentido, que o sigilo profissional ao qual o advogado está vinculado não resta prejudicado tampouco deve ser confundido com todo o regramento estabelecido na legislação dedicada à proteção de dados pessoais, que visa preservar o titular em uma dimensão mais abrangente. Assim, para além do termo de confidencialidade assinado entre advogado e cliente com o objetivo de assegurar o sigilo profissional, faz-se necessário informar o titular de dados, minimamente, sobre a finalidade, forma e duração do tratamento de dados, bem como sobre o exercício de seus direitos.

Feitas as observações preliminares, destaca-se que a eleição de uma hipótese de tratamento de dados pessoais é condição para sua licitude. Nesse sentido, o que deve ser feito é uma análise atenta ao contexto e à realidade concreta, levando-se em consideração as atividades e processos internos de determinada organização, bem como suas respectivas finalidades, com vistas a eleger a hipótese legal que melhor se encaixa em cada caso.

O artigo 7º da LGPD prevê dez hipóteses em que os dados pessoais podem ser tratados; de forma complementar, o artigo 11 prevê oito hipóteses, em se tratando especificamente de dados pessoais sensíveis. Ressalta-se, ainda, que é um equívoco afirmar qualquer hierarquia entre as hipóteses legais de tratamento, uma vez que cada uma delas possui especificidades e requisitos, aplicáveis a situações e contextos diversos.

Passemos, então, às hipóteses de tratamento de dados previstas no artigo 7°:

Art. 7° O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de **consentimento** pelo titular;

II - para o **cumprimento de obrigação legal ou regulatória** pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à **execução de políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a **realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a **execução de contrato ou de procedimentos preliminare**s relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o **exercício regular de direitos em processo judicial, administrativo ou arbitral**, esse último nos termos da Lei n° 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a **proteção da vida ou da incolumidade física do titular ou de terceiro;**

VIII - para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos **interesses legítimos do controlador ou de terceiro**, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente. (grifos nossos)

Já com relação ao artigo 11, em se tratando de dados pessoais sensíveis, tem-se a supressão de algumas hipóteses (referentes à execução de contrato ou de procedimentos preliminares relacionados a contrato, ao legítimo interesse do controlador ou de terceiro, e à proteção ao crédito) e acréscimo de outra (prevenção à fraude e à segurança do titular), conforme pode ser observado a seguir:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - **quando o titular ou seu responsável legal consentir**, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
a) **cumprimento de obrigação legal ou regulatória** pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de **políticas públicas** previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei n° 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
e) **proteção da vida ou da incolumidade física do titular ou de terceiro;**
f) **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
g) **garantia da prevenção à fraude e à segurança do titular,** nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9° desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (grifos nossos)

Levando-se em consideração que este material tem como público alvo os escritórios de advocacia e considerando que, a depender do teor da demanda apresentada pelo cliente, poderão ser tratados dados pessoais sensíveis variados, optou-se pela abordagem pormenorizada das hipóteses legais que apresentam maior pertinência temática, ou seja, que têm maior probabilidade de serem utilizadas no contexto estabelecido.

Deve-se ter em mente que o consentimento (art. 7°, I, e art. 11, I) e o legítimo interesse (art. 7°, IX) são hipóteses legais consideradas genéricas, ao passo que as demais hipóteses, por possuírem um âmbito de aplicação melhor delimitado, são consideradas específicas. Assim, é preciso estar atento aos requisitos inerentes às duas primeiras situações, as quais serão objeto de análise a seguir.

De início, ressalta-se que um dos grandes equívocos relacionados à LGPD é a afirmação de que o **consentimento** do titular é indispensável para qualquer tratamento de dados pessoais. Conforme mencionado, trata-se de um mito, uma vez que existem diversas hipóteses capazes de respaldar o tratamento de dados, sendo o consentimento apenas uma delas. Além disso, o artigo 7°, §6° deixa claro que a dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais imposições legais, com destaque à observância dos princípios e garantias dos direitos do titular.

Ademais, ao consentimento estão relacionados atributos específicos, ou seja, o consentimento deve ser manifestação livre, informada e inequívoca, além de ser dado por escrito e em cláusula destacada, ou em outro meio que demonstre a manifestação de vontade do titular. Justamente por constituir manifestação livre da vontade, é que o consentimento pode ser revogado a qualquer momento por mera liberalidade do titular, bastando sua manifestação para tanto, por meio de procedimento gratuito e facilitado. Vale destacar, ainda, que cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade ao que a Lei prevê.

Ressalta-se, por todo exposto, que o consentimento é uma hipótese legal utilizada de forma residual, especialmente pelo fato de poder ser revogado a qualquer momento. A título exemplificativo, imagine ser contratado para ajuizar um processo judicial e utilizar o consentimento como hipótese legal de tratamento de dados; uma vez ajuizado o processo, a revogação do consentimento torna-se impraticável, sendo, portanto, uma hipótese legal inadequada para a situação. Por outro lado, a hipótese em questão pode ser adequada para os casos em que se pretende o envio de newsletter aos clientes ou até mesmo de convites de eventos promovidos pelo escritório de advocacia.

A segunda hipótese genérica refere-se ao **legítimo interesse** do controlador ou de terceiro. Apesar de parecer uma hipótese de avaliação bastante subjetiva, é certo que a Lei oferece requisitos para avaliação de cada situação concreta, de modo que a hipótese não seja uma brecha para o tratamento de dados pessoais de forma arbitrária por parte do controlador. Além disso, conforme mencionado, não pode ser utilizada para fins de tratamento de dados pessoais sensíveis, uma vez que não se encontra no rol estabelecido pelo artigo 11.

Nas situações em que o tratamento for baseado no legítimo interesse, deve-se proceder ao que a doutrina nomeia de Teste de Legítimo Interesse, pelo qual é realizada (i) a avaliação da finalidade, que deve ser lícita, (ii) a avaliação da necessidade, segundo a qual somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, (iii) o balanceamento entre impactos sobre o titular de dados, especialmente sobre direitos e liberdades fundamentais, e suas legítimas expectativas, e (iv) a adoação de salvaguardas, as quais incluem, mas não se limitam, a garantia de transparência com relação ao tratamento, o direito de oposição exercido pelo titular (direito ao opt-out, por exemplo), bem como medidas técnicas de pseudonimização.

Adentrando às hipóteses de âmbito de aplicação específico, destaca-se o tratamento de dados pessoais para fins de **cumprimento de obrigação legal ou regulatória** pelo controlador. Como o próprio dispositivo revela, a presente hipótese deve ser utilizada sempre que o tratamento de dados ocorrer não por liberalidade do controlador, mas por uma imposição legal ou regulatória decorrente do exercício das atividades. Tem-se, portanto, que quando da contratação de um advogado ou assistente jurídico como empregado, a coleta de dados pessoais para fins de assinatura da Carteira de Trabalho e de recolhimento de verbas previdenciárias não é uma faculdade do empregador, mas uma obrigação legal.

Outra hipótese que merece destaque é referente à execução de contrato. O art. 7º, V, da LGPD, respalda o tratamento de dados necessários tanto para a execução de contrato, quanto de procedimentos preliminares relacionados a contrato, de modo que o segundo cenário seja capaz de contemplar as situações em que ocorre tratamento de dados para fins de elaboração de proposta de honorários ou de obtenção do endereço do titular onde determinada prestação será executada, previamente ao efetivo firmamento do contrato.

Muito provavelmente, esta será a base legal mais utilizada por escritórios de advocacia no exercício de suas atividades, uma vez que ampara o tratamento de dados para fins de execução de contratos de prestação de serviços advocatícios. Deve-se destacar que a disposição não foi replicada no artigo 11, apesar disso, a hipótese de tratamento de dados pessoais sensíveis para o exercício regular de direitos em contrato é indicada no art. 11, II, "d".

A última hipótese que será comentada refere-se ao **exercício regular de direitos em processo judicial, administrativo ou arbitral** (este último nos termos da Lei nº 9.307/1996, Lei de Arbitragem). Nesse sentido, na defesa de seus interesses, podem os litigantes tratar dados pessoais, em consonância ao que dispõe a Constituição Federal em seu art. 5º, LV: "aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes". Essa hipótese legal será utilizada para o exercício de direitos do próprio escritório de advocacia ou do advogado, a exemplo de uma ação de regresso em face de um parceiro, ação de cobrança ou execução de um cliente, bem como exercício de direitos em face de órgãos fiscalizadores, como o Procon ou a própria Autoridade Nacional de Proteção de Dados (ANPD).

A Lei dispõe, ainda, sobre dados pessoais cujo acesso é público ou dados tornados manifestamente públicos pelo titular, para asseverar que poderão ser tratados para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento, bem como preservados os direitos do titular, fundamentos e princípios estabelecidos pela LGPD (nos termos do art. 7º, §7º, da Lei). Assim, é certo que esses dados poderão eventualmente ser utilizados como meio de prova em um processo judicial, entretanto, deve-se observar as condições para tratamento lícito estabelecidas.

Por fim, destaca-se que em caso de alteração da finalidade, forma e duração do tratamento de dados, bem como da identificação do controlador e/ou uso compartilhado de dados, há necessidade de que o controlador informe o titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração, em conformidade com o art. 8º, §6º, da LGPD. Portanto, eventual alteração da hipótese legal que embasa o tratamento de dados pessoais deve ser informada de forma clara e precisa ao titular, enquanto condição para a licitude do tratamento.

Comissão de Privacidade
e Proteção de Dados

AGENTES DE TRATAMENTO E OUTROS ATORES

Por Ana Vitória D'Assumpção Guzmán

Advogada, Sócia do Guzmán Finoto e Bougleux Advogados, Especialista em Direito Digital e Compliance e Pós-graduanda em Governança da Tecnologia da Informação. Integrante da Comunidade Internacional de Estudos em Direito Digital (CIED) e Presidente Interina da Comissão de Privacidade e Proteção de Dados da OAB/Uberlândia. Autora de capítulos e artigos em direito digital e proteção de dados pessoais.

A Lei Geral de Proteção de Dados (LGPD), assim como as demais leis que compõem o ordenamento jurídico brasileiro, tem como finalidade, dentre outras, trazer segurança para as partes que mantêm relações jurídicas cujo cerne é o tratamento de dados pessoais. Mas, quem são essas partes?

Também como ocorre em outras legislações, a exemplo do Código de Defesa do Consumidor ou do Marco Civil da Internet, que, não por acaso, interagem com a LGPD a ponto de compor um microssistema, o legislador se preocupou em identificar, nomear e conceituar essas partes. E, dentre estas, temos os agentes de tratamento de dados pessoais.

De acordo com a LGPD, os agentes de tratamento de dados são o controlador e o operador, os quais podem ser pessoas naturais ou jurídicas, de direito público ou privado. De acordo com a Autoridade Nacional de Proteção de Dados (ANPD), o controlador é o agente responsável por tomar as decisões essenciais ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais.

O núcleo definidor desta figura, portanto, é o poder de decisão atrelado à definição da finalidade. E, nesse ínterim, é relevante relembrar que a finalidade é um princípio norteador do tratamento de dados, sendo certo que o seu atendimento compete primordialmente ao controlador. É ele quem dirá para quê e porquê aquele dado será tratado. A finalidade é, assim, a palavra chave para compreensão dessa figura.

O operador, por outro lado, é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada. É importante destacar que a terceirização de eventuais e pontuais decisões acerca do modo em que o tratamento se dará não descaracteriza as figuras em comento, admitindo-se que o controlador forneça instruções para que o operador realize o tratamento em seu nome, sendo usual e legítimo que parte das decisões a respeito do tratamento, limitadas aos seus elementos não essenciais, fique sob a alçada do operador.

Sobre este ponto, a ANPD afirma que:

> O segundo ponto relevante é a desnecessidade de que todas as decisões sejam tomadas pelo controlador, bastando apenas que este mantenha sob sua influência e controle as principais decisões, isto é, aquelas relativas aos elementos essenciais para o cumprimento da finalidade do tratamento. De fato, especialmente quando há a contratação de um operador, é usual e legítimo que parte das decisões a respeito do tratamento, limitadas aos seus elementos não essenciais, fique sob a alçada do operador. A título de exemplo, podem ser mencionados a escolha dos *softwares* e equipamentos que serão utilizados e o detalhamento de medidas de prevenção e segurança. (2022, *online*)

Ademais, é preciso compreender que, numa relação jurídica firmada, a atribuição dessas figuras a uma das partes não é estática. Ou seja, em dada relação negocial, composta por duas partes, por exemplo, o controlador não será necessariamente sempre uma delas, assim como o operador será necessariamente a outra. Isso porque a análise sobre quem é o controlador ou operador deve ser feita e enquadrada de acordo com cada processo de tratamento de dados identificado.

Num escritório de advocacia, por exemplo, diversas relações são entabuladas com variáveis finalidades. A depender da essência de cada uma delas, a sociedade advocatícia poderá ser controladora ou operadora e, mais do que isso, numa mesma relação, o escritório poderá ser controlador de um processo, operador de outro.

Outra anotação importante sobre essas figuras é que devem ser sempre analisadas a nível institucional. Assim, o diretor de uma empresa não é o controlador, enquanto o seu funcionário é o operador, assim como num escritório de advocacia o advogado não é o controlador e o estagiário, por exemplo, o operador. O enquadramento destas figuras deverá ser feito a nível institucional, assim, o escritório, enquanto sociedade, por exemplo, será o controlador ou operador, a variar conforme o tratamento realizado.

Mencione-se, ainda, que apesar de não estar expressamente previsto na lei, a doutrina e a própria ANPD já admitem a existência de co-controladores, isto é, ocasiões em que ambos os agentes identificados naquele tratamento são controladores de dados, situação que pode ser entendida como "a determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD" (ANPD, 2022, online).

Admite-se também que existem sub operadores, ou seja, aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador.

A simples leitura dos conceitos legais ou análise teórica que paira sobre eles pode não ser tão didática, motivo pelo qual a utilização de exemplos cotidianos para escritórios de advocacia pode ser bastante útil nesse momento. Assim, imagine-se as seguintes hipóteses: (a) a contratação de diligentes para protocolo, minutas de petições ou despachos; e a (b) atuação em parceria.

No primeiro caso, é possível afirmar que o advogado contratante será, em regra, o controlador, e o contratado, o operador. Isso porque os dados cedidos tem a finalidade específica de execução do serviço contratado pelo titular diretamente ao advogado contratante, que cede esses dados ao contratado na intenção de que este o auxilie com o escopo pretendido. O contratado não deverá utilizar os dados cedidos com outro fim que não aquele especificado na diligência.

Já no segundo caso, os parceiros podem ser co-controladores e, a depender da situação concreta, o advogado que a princípio detinha o cliente, isto é, que foi diretamente contratado pelo cliente, pode ser até mesmo o operador. Não é incomum transferir parte importante da estratégia advocatícia ao parceiro, situação que pode implicar na delegação de decisão absolutamente relevante para o tratamento de dados do cliente.

Veja, portanto, que as figuras dos agentes de tratamento de dados são relativamente complexas e bastante relevantes, especialmente porque estão intrinsecamente atreladas às responsabilidades legal e contratualmente previstas, questão abordada em capítulo subsequente.

Por fim, é importante esclarecer que os agentes de tratamento são alguns dos atores previstos pela LGPD, mas há outros. O titular de dados, definido por lei como a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento", a Autoridade Nacional de Dados, "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional", e o Encarregado de Dados, enquanto "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", também são partes de possíveis relações firmadas sob o manto e geridas pela LGPD.

Há, ainda, a possibilidade de que outras partes interessadas, não expressamente previstas em lei, componham e interfiram nessas relações, a exemplo do Ministério Público, da Defensoria Pública, do PROCON, dentre outros, que, não raro, atuam respaldados pela LGPD ou, mais do que isso, buscando o seu efetivo cumprimento pela sociedade.

Comissão de Privacidade
e Proteção de Dados

RESPONSABILIDADES ENTRE AGENTES DE TRATAMENTO

Por Lorena Rochael Mello

Advogada do escritório Lee, Brock e Camargo Advogados, pós-graduada em Direito Constitucional e Digital pela ITS-Rio/UERJ. Integrante da Comissão de Privacidade e Proteção de Dados da OAB/Uberlândia.

Em relação direta com a proteção dos dados pessoais propriamente dita, está a responsabilidade atribuída a cada agente no tratamento dos dados, uma vez que se individualizam as obrigações de cada parte envolvida no processo de tratamento dos dados.

Conforme mencionado, a ANPD emitiu um guia orientativo para a definição dos agentes de tratamento de dados pessoais e estabeleceu que "agentes de tratamento devem ser definidos a partir de seu caráter institucional"; desse modo, "uma organização pode ser controladora e operadora, de acordo com sua atuação em diferentes operações de tratamento" (2022, online).

A LGPD estabelece que os agentes de tratamento - controlador e operador - têm responsabilidades claras em relação ao tratamento de dados pessoais e ambos têm a obrigação de garantir a proteção dos dados pessoais, cumprindo com as disposições legais.

Nesse sentido, o controlador deve seguir as obrigações específicas impostas a ele pela LGPD, tais como: (i) elaborar o relatório de impacto à proteção de dados pessoais (art. 38); (ii) comprovar que o consentimento obtido do titular atende às exigências legais (art. 8°, §2°); (iii) comunicar à ANPD a ocorrência de incidentes de segurança (art. 48); e (iv) atender às solicitações dos titulares de dados (art. 18), mas aos exemplos não se limitando.

O operador, por sua vez, como responsável por realizar o tratamento dos dados em nome do controlador, segue as instruções definidas e fornecidas por ele. Tendo como obrigação (i) seguir as instruções do controlador; (ii) firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador; (iii) dar ciência ao controlador em caso de contrato com eventual suboperador.

Então, como identificar a função do agente de tratamento?
A própria ANPD explica que a identificação deve partir do conceito legal, e deve considerar também o contexto fático e as circunstâncias relevantes do caso, tais como as obrigações estipuladas em instrumentos legais e regulamentares ou contratos firmados entre as partes. Além de se analisar a efetiva atividade desempenhada pela organização.

A pessoa natural que atua como profissional subordinado a uma pessoa jurídica não será controladora, tampouco operador, aqui incluem-se os empregados, administradores, sócios, servidores ou outra pessoa natural que integra a pessoa jurídica. Nesse caso, a organização será a considerada o agente de tratamento e assumirá a responsabilidade pelos atos praticados por seus agentes e prepostos em face dos titulares, demais agentes de tratamento e da própria ANPD.

Por outro lado, os profissionais liberais, tais como os advogados, que atuam como responsáveis pelas principais decisões referentes ao tratamento de dados pessoais, agindo de forma independente e em nome próprio, não estando subordinados a uma pessoa jurídica, serão considerados controladores de dados.

Portanto, para analisarmos a responsabilidades de um escritório de advocacia, é importante identificar a função institucional do escritório: se o advogado, enquanto profissional liberal, armazena os dados pessoais de seus clientes em pastas ou computador do escritório, ele será o controlador dos dados pessoais, tendo uma "responsabilidade mais abrangente, pois caberá a ele definir todos os aspectos relacionados aos dados recebidos para tratamento" (GUARIENTO, 2020,online).

Caso o escritório de advocacia seja contratado para trabalhos mais específicos, como correspondente ou funções terceirizadas, a sua função pode ser considerada como operador dos dados, pois atua em nome da empresa ou escritório contratante, que são os controladores, e para realizar o tratamento conforme as instruções e finalidades da controladora.

Via de regra, a responsabilidade por eventuais prejuízos a terceiros será do controlador dos dados. Ademais, caso o operador descumpra as obrigações impostas pela legislação de proteção de dados ou quando não seguir as instruções lícitas do controlador, responderá solidariamente.

Assim, controlador e operador possuem a obrigação de reparação se causarem dano patrimonial, moral, individual ou coletivo a outrem, no âmbito de suas respectivas esferas de atuação, nos termos do artigo 42 da LGPD:

Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:
I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

Em caso de descumprimento da legislação, poderão ser impostas sanções administrativas, aplicadas pela própria ANPD. Relembre-se que, com a aprovação da Lei 14.010/2020, as sanções administrativas previstas na LGPD (que antes estavam suspensas) entraram em vigor em agosto de 2021, tendo a ANPD competência para fiscalizar e aplicar sanções em casos de violação da segurança dos dados e descumprimento das normas da LGPD.

As sanções previstas para as situações de descumprimento da legislação estão previstas no artigo 52 e permitem a aplicação de advertência, eliminação dos dados pessoais, suspensão, multa no valor de até 2% do faturamento da empresa e até proibição do exercício de atividades relacionadas ao tratamento de dados pessoais, dentre outras.

Além das sanções administrativas, ao tratamento irregular de dados pessoais também se aplica a responsabilização civil para a reparação dos danos causados e que deve ser analisada a partir da função do agente de tratamento, conforme abordado.

Vale mencionar que, em se tratamento de responsabilização nos casos de vazamento de dados pessoais, o Superior Tribunal de Justiça, em decisão recente, reconheceu no Agravo em Recurso Especial nº 2130619 – SP (2022152262-2) que o vazamento de dados pessoais não gera dano moral presumido, e por isso o titular de dados deve comprovar o dano, ou seja:

O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.

Por fim, um ponto comum a todos os agentes de tratamento é a necessária conformidade com os princípios da LGPD, principalmente com o princípio da transparência, uma vez que por meio dele, se garante aos titulares que as informações sejam claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

Além disso, a LGPD prevê que é responsabilidade dos agentes de tratamento a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais contra incidentes, imputando a eles a responsabilidade pelo dano decorrente da violação de segurança dos dados, quando comprovado.

Nesse sentido, vale destacar os seguintes dispositivos:

> Art. 44. 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.
>
> Art. 46. Os agentes de tratamento devem adotar 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.
>
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

Por fim, cabe ressaltar a importância de delimitar contratualmente as funções e as responsabilidades de cada agente de tratamento, de modo a facilitar a atribuição de responsabilidades em caso de prejuízo a terceiros. Além disso, exploraremos adiante boas práticas e medidas em matéria de segurança da informação que podem ser adotadas pelos agentes de tratamento no sentido de se resguardar e prevenir riscos.

Comissão de Privacidade
e Proteção de Dados

BOAS PRÁTICAS E GOVERNANÇA DE DADOS PESSOAIS

Por João Victor Vieira Doreto

Advogado, especialista em Direito Civil pela FDRP/USP. Pós-graduando em Direito Contratual pela EBRADI. Especializado em proteção de dados pela Data Privacy Brasil e IDP. Membro da International Association of Privacy Professional (IAPP). Membro de Comissões da OAB/MG e OAB/SP. Head Member do Uberhub Legaltech. Sócio na banca Cerizze Soluções Jurídicas.

Boas práticas de governança de dados pessoais têm se tornado cada vez mais importantes no mundo atual, em que a coleta e o uso de informações pessoais se tornaram práticas comuns e até obrigatórias em diversos setores da sociedade.

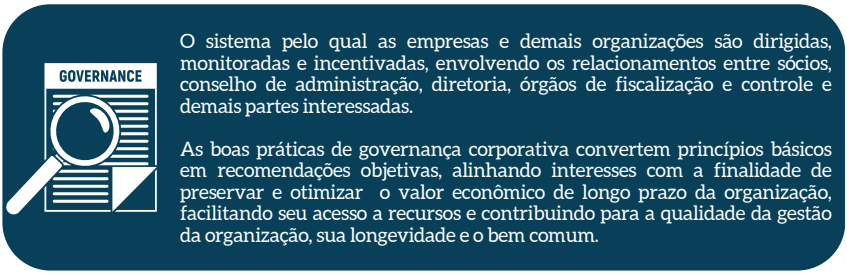
O tema é de tamanha importância que a Lei Geral de Proteção de Dados tem uma seção exclusiva para o tema: "Capítulo VII - Seção II: Das boas práticas e da Governança". Este define que controladores e operadores de dados pessoais poderão formular regras de boas práticas e de governança, seja por meio de associações ou de forma individual pelo controlador ou operador de dados pessoais.

Apesar de não ser de caráter obrigatório, a LGPD prevê incentivos para aqueles que contribuem para garantir ao titular maior proteção em relação aos seus dados pessoais. Os artigos 50 e 51, ao trazerem a possibilidade de os agentes de tratamento, por si ou através de método colaborativo, estabelecerem tais regras, contribui e estimula o diálogo entre os principais atores, que colaboraram para a formação da lei e contribuem para a construção de regulamentações complementares através, principalmente, da participação em consultas públicas.

Os constantes avanços tecnológicos, de forma acelerada, colocam a proteção de dados como passo fundamental para garantir a privacidade e o direito à autodeterminação. Isso, contudo, não pode ser atingido exclusivamente a partir de regulamentações, é preciso estimular o desenvolvimento de uma cultura de privacidade, devendo os agentes de tratamento assumir o papel de educador.

A governança de dados pessoais tem como objetivo garantir a segurança, a privacidade e o correto uso das informações fornecidas pelos usuários. Isso significa que os agentes de tratamento precisarão reconstruir seus processos internos, principalmente aqueles nos quais é necessário tratamento de dados pessoais para atingimento da finalidade estabelecida, bem como a responsabilização e transparência no gerenciamento dessas informações. Em outras palavras, a aplicação de princípios de governança dos dados pessoais busca garantir que estes sejam usados de forma segura, transparente e adequada.

O Instituto Brasileiro de Governança Corporativo (2015) define Governança Corporativa como:



A partir das diretrizes para o uso e a proteção dos dados pessoais disponíveis na LGPD, os agentes de tratamento devem estabelecer seus objetivos de proteção de dados de acordo com o modelo de negócio, definir os meios para atingir os objetivos e acompanhar a performance da organização.

Existem quatro fatores fundamentais para a estruturação, organização e uso de forma inteligente de dados pessoais. Inicialmente é necessário estabelecer os objetivos de proteção de dados através de políticas internas, na sequência é necessário revisar e reconstruir processos internos da organização para adequá-los às novas políticas. Para tanto, é necessário trabalhar intensamente a construção da cultura interna de proteção de dados utilizando de forma eficaz os recursos humanos, definindo seus papéis e responsabilidades, e tecnológicos, com o objetivo de auxiliar e trazer eficácia às tarefas repetitivas

De forma prática, a Governança de Dados pode ser exemplificada pelo fluxograma abaixo desenvolvido pela Serasa Experian:

Adotar boas práticas de governança de dados pessoais não apenas garantirá a conformidade com as leis de proteção de dados, mas também proporcionará maior confiança dos usuários em relação às empresas.

O fluxograma anteriormente indicado está em total consonância com a LGPD, que estabelece em seu art. 50, parágrafo 2°, os requisitos mínimos de um Programa de Governança em Privacidade:

- Contar com a adoção de processos internos que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais;
- Ser aplicável a todo o conjunto de dados pessoais tratados, independente de como tenha sido realizada a coleta;
- Ser adaptado à estrutura, à escala e ao volume do escritório;
- Estabelecer políticas e salvaguardas adequadas à realidade do escritório;
- Estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- Estabelecer e aplicar mecanismos de supervisão internos e externos;
- Contar com planos de resposta a incidentes e remediação; e
- Ser atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Como já bem ressaltado, o legislador, ao prever a possibilidade de organizações criarem as próprias regras de tratamento de dados pessoais, além de estimular meios que facilitam o exercício da autodeterminação informativa do titular, traz a previsão de que a Autoridade Nacional de Proteção de Dados estimulará tal prática.

Uma faceta deste estímulo está consolidado no art. 7º Resolução CD/ANPD nº 4/2023, que aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas, estando previsto que na definição da sanção, será levado em consideração pela ANPD a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com a LGPD e a adoção de política de boas práticas e governança.

A autoridade estabeleceu ainda, através do artigo 13 da Resolução CD/ANPD nº 4/2023, descontos na aplicação de multas em caso de implementação de boas práticas de governança, nos seguintes critérios:

I. 20%(vinte por cento), nos casos de implementação de política de boas práticas e de governança ou de adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar os danos aos titulares, voltados ao tratamento seguro e adequado de dados, até a prolação da decisão de primeira instância no âmbito do processo administrativo sancionador;

II. nos casos em que o infrator tenha comprovado a implementação de medidas capazes de reverter ou mitigar os efeitos da infração sobre os titulares de dados pessoais afetados:
A. 20%, previamente à instauração de procedimento preparatório ou processo administrativo sancionador pela ANPD; ou
B. 10% se após a instauração de procedimento preparatório e até a instauração de processo administrativo sancionador; e
C. 5% nos casos em que se verifique a cooperação ou boa-fé por parte do infrator.

Como demonstrado, há grande interesse de uma participação ativa dos agentes de tratamento no processo de adequação da cultura brasileira em prol de possibilitar aos cidadãos maior segurança no tratamento de seus dados pessoais e, assim, garantir o direito à privacidade.

A implementação de um Programa de Governança, para além de um requisito legal, melhora a imagem da empresa, aumenta a confiança dos clientes e ajuda a evitar violações previstas na LGPD, que podem resultar em multas significativas e danos reputacionais, que também poderão ser reduzidas em caso de demonstração de um robusto programa de governança.

Um programa de governança de dados pessoais também pode melhorar a eficiência operacional, reduzindo riscos de erros e retrabalho, e pode ser um diferencial competitivo, atraindo clientes que valorizam a privacidade dos seus dados.

Comissão de Privacidade
e Proteção de Dados

ASPECTOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

Por Débora de Oliveira Côco

Advogada, implementadora de projetos de adequação à LGPD e projetos de DPO na GEP Soluções em Compliance, integrante da Comissão de Privacidade e Proteção de Dados da OAB Uberlândia.

Ao iniciar um processo de adequação à Lei Geral de Proteção de Dados (LGPD) é importante que, além da elaboração dos documentos relacionados à privacidade, os escritórios de advocacia adotem medidas técnicas e administrativas de segurança da informação, que possam garantir a proteção dos dados pessoais, conforme estabelece o princípio da segurança, disposto no art. 6°, inciso VII, da LGPD. Ainda nesse sentido, o art. 46 estabelece especificamente que:

> Os agentes de tratamento devem adotar 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.

Portanto, o processo de adequação à LGPD também envolve a adoção de medidas técnicas e administrativas que garantam o cumprimento dos pilares da segurança da informação. Sendo assim, o presente texto tem como objetivo orientar os escritórios de advocacia sobre os aspectos básicos de segurança da informação necessários para a conformidade com a legislação.

Para que se possa entender o que é segurança da informação, explicamos a seguir os conceitos dos seus pilares que orientará a implementação prática de algumas ações.

Em linhas gerais os pilares da segurança da informação são:
i) confidencialidade: visa garantir que a informação não estará disponível ou será divulgada a pessoas não autorizadas sem prévia autorização dos responsáveis pela informação;
ii) integridade: tem como objetivo garantir que as informações são autênticas e não foram adulteradas indevidamente;
iii) disponibilidade: garante que os dados pessoais e as informações estarão disponíveis apenas para as pessoas autorizadas.

O estabelecimento de diretrizes que garantam o cumprimento dos pilares de segurança da informação é fundamental para evitar os incidentes de segurança, que são eventos adversos confirmados ou não relacionados à violação na segurança de dados pessoais. São exemplos de incidentes de segurança: acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais, conforme definiu a ANPD (2022, online).

A prevenção aos incidentes de segurança é essencial para garantir um bom cumprimento da LGPD, haja vista que eles estão acontecendo com maior frequência nas organizações. Na maioria dos casos, a técnica utilizada pelos criminosos é a engenharia social, na qual o golpista consegue fazer com que pessoas façam o download de arquivos contendo vírus ou malwares, principalmente através de e-mails falsos que simulam e-mails de bancos, operadoras de telefonia e colegas de trabalho.

A prática de golpes digitais vem assolando o Brasil, que já se tornou o 5º país mais afetado do mundo por ataques hackers, de acordo com relatório da Security Report. Além disso, conforme relatório da IBM 2021 os ataques de ransomware custam mais caros do que a média de violação de dados e as credenciais comprometidas foram o vetor de ataque inicial mais comum, responsável por 20% das violações.

Para que os incidentes de segurança sejam evitados, é fundamental que os escritórios adotem medidas de segurança para a proteção dos dados pessoais. Esses procedimentos podem ser encontrados nas normativas ISO, que são referência internacional em segurança da informação e no Brasil são disponibilizadas pela ABNT. Assim, as normas ABNT NBR ISO nº 27001, ABNT NBR ISO nº 27002 e ABNT NBR ISO nº 27701 proporcionam excelentes parâmetros de controle para a implementação das medidas de segurança.

Neste sentido, com o intuito de auxiliar os escritórios de advocacia na implementação de algumas boas práticas de segurança da informação, seguem alguns exemplos que podem ser adotados para que os dados pessoais estejam protegidos:

a) **Controles de Acesso**: Os escritórios devem definir controles de acessos sobre os sistemas e pastas que contém dados pessoais e informações, classificando o tipo de confidencialidade da informação e quem poderá ter acesso a ela. Uma forma prática de realizar esse controle é criar credenciais (login + senha) para cada usuário com gerenciamento de privilégios e acessos. Além disso, o escritório poderá elaborar uma política de controle de acesso determinando quais serão as regras de autorização, compartilhamento e disponibilização dos
dados pessoais, inclusive dos dados que estão armazenados de maneira física.

b) **Gestão de senhas**: As senhas dos usuários devem ser individuais e intransferíveis, inclusive aquelas utilizadas nos tokens de acesso aos tribunais e de assinaturas eletrônicas. É importante também que as senhas tenham no mínimo 08 caracteres com inclusão de letras maiúsculas e minúsculas, números e caracteres especiais, assim como que sejam trocadas periodicamente e que não sejam anotadas em papéis, agendas e post-its.

c) **Eliminação de documentos**: A LGPD estabelece que os dados pessoais devem ser eliminados após cumprida sua finalidade e ao término do seu tratamento, portanto, os escritórios devem eliminar dados pessoais desnecessários, conforme determina o art. 15 da LGPD. A eliminação de dados deve ser realizada conforme as melhores práticas para garantir a segurança dos dados pessoais:

i) Documentos físicos: devem ser triturados ou incinerados;

ii) Documentos digitais: devem ser eliminados permanentemente dos computadores, sistemas e dispositivos móveis, inclusive da lixeira.

d) **Armazenamento de documentos**: Os documentos que contém dados pessoais devem ser armazenados em local seguro com restrição de acesso. Os arquivos digitais preferencialmente, devem ser armazenados na nuvem.

e) **Antivírus**: As medidas de segurança também envolvem a instalação de softwares que ajudam a proteger o os dispositivos contra a maior parte dos vírus que podem danificar os documentos. É importante também que o escritório possua uma infraestrutura em segurança da informação com rede interna e monitoramento constante dos sistemas e aplicativos.

Além das medidas elencadas acima, é imprescindível que o escritório possua uma Política de Segurança da Informação, documento que serve de parâmetro para as diretrizes de segurança e descreve os princípios, valores, compromissos, orientações e responsabilidades de todos os colaboradores, sócios e contratados a respeito do tema. E ainda, os escritórios deverão implementar medidas de conscientização e treinamento com todos os envolvidos para que as boas práticas de segurança da informação sejam disponibilizadas para todos. Este ponto é fundamental para que os incidentes de segurança ocasionados por erros humanos sejam evitados e para que os escritórios evidenciem o cumprimento das boas práticas de privacidade e segurança da informação.

Para que as medidas sejam implementadas é orientado que exista um profissional interdisciplinar que tenha domínio dos conceitos e diretrizes de segurança da informação e saiba estabelecer indicadores de desempenho e propostas de melhoria neste segmento, conforme as normativas internacionais.

As medidas elencadas acima não buscam exaurir o tema, pelo contrário, são exemplos práticos de como os escritórios podem iniciar a implementação dos aspectos básicos de segurança da informação. Ressaltamos que para uma completa adequação à LGPD é necessário a elaboração de diagnósticos específicos voltados aos controles de segurança da informação com a indicação de planos de ação e acompanhamento permanente de profissional capacitado nesta seara.

Comissão de Privacidade
e Proteção de Dados

FLUXO DE IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

por Ana Paula Bougleux Andrade Resende

Advogada, sócia do escritório Guzmán, Finoto e Bougleux Advogados. Especialista em Direito Digital, com certificado pela EXIN (Privacy and Data Protection Essentials - PDPE). Mestranda em Direito pela UNESP/Franca. Integrante da Comissão de Privacidade e Proteção de Dados e da Comissão de Direito para Startup da OAB/Uberlândia. Autora de capítulos e artigos em direito digital e proteção de dados pessoais.

*Esta sessão contou com contribuição da apresentação de slides elaborada pela advogada Aline Carneiro para o evento “Workshop- LGPD para seu escritório”.

Diante do que foi exposto até o momento, ficou claro que um programa de adequação à LGPD não se trata de uma tarefa restrita às atividades e conhecimentos do âmbito jurídico.

Estar em compliance à Lei Geral de Proteção de Dados requer a tomada de medidas técnicas e administrativas que estão muito além da letra da lei. Envolve o engajamento das pessoas que compõem a organização, a revisão de processos internos e tecnologias capazes de assegurar a segurança da informação. Por esse motivo é muito comum dizer que o Programa de Adequação requer o empenho de pessoas, processos e tecnologia, necessariamente nessa ordem.

Ademais, as medidas necessárias dependerão, em muito, do porte da organização, da quantidade de dados pessoais, dos recursos disponíveis, da forma de tratamento dos dados, dentre outras questões, o que faz cada Programa de Adequação ser tão particular e variável conforme a instituição em questão.

Apesar das particularidades de cada projeto, é preciso compreender o que buscamos ao longo de um trabalho de Proteção de Dados:

- Identificar obrigações relacionadas à Privacidade e Proteção de Dados.
- Identificar riscos de Privacidade e Proteção de Dados relacionados ao negócio, colaboradores e clientes.
- Identificar documentação, práticas, políticas e procedimentos já existentes.
- Criar, revisar e implementar políticas e procedimentos que afetem positivamente a Privacidade e a Proteção de Dados e que, juntos, formarão um Programa de Privacidade e Proteção de Dados.

Via de regra, são fases de um Programa de Adequação à LGPD:

1) Identificação do Contexto;
2) Mapeamento de Dados;
3) Análise de riscos e Planejamento;
4) Implementação;
5) Monitoramento.

Passemos, então, a cada uma dessas etapas.

1) Identificação do contexto

É comum que o Programa de Adequação à LGPD se inicie com um levantamento de informações gerais acerca da organização e uma conscientização dos colaboradores.

Assim, tratando de um escritório de advocacia, deve-se buscar compreender quais são as prioridades com relação à Proteção de Dados Pessoais (por exemplo: um arquivo físico de documentos de clientes que não possui qualquer controle ou uma base de gerenciamento de processos sem backup).

Também é importante fazer um levantamento dos requisitos legais (reconhecimento da legislação aplicável ao negócio), identificar as partes interessadas (como fornecedores, parceiros e clientes) e eleger um Comitê Interno de Proteção de Dados Pessoais ou um Encarregado de Dados.

Caso o escritório entenda como relevante, é válido comunicar às partes interessadas (no todo ou em parte) que a instituição está passando por um Programa de Adequação à LGPD e que, eventualmente, isso influenciará a relação estabelecida entre as partes em questão.

Por fim, mas não menos importante, deve-se realizar treinamento e conscientização dos colaboradores do escritório, pois isso difunde a importância da temática por toda a instituição e estimula a colaboração no decorrer do Programa.

A partir disso, teremos uma noção inicial de quais são as principais lacunas (gaps) da instituição com relação à Proteção de Dados.

2) Mapeamento

A segunda etapa é o mapeamento de dados, que tem como finalidade registrar o tratamento (a LGPD determina que os agentes de tratamento deverão manter registro das atividades de tratamento de dados pessoais), identificar riscos (do mapeamento derivam informações para o plano de ação de mitigação de riscos), prestar contas (facilita o entendimento da categoria, tipos e fluxos dos dados na empresa), e monitorar processos (auxilia as atividades de inventariar, monitorar e determinar impactos que os processos e sistemas organizacionais terão sobre a privacidade e proteção de dados).

Assim, ao observar a rotina de trabalho da instituição, buscaremos as seguintes informações (mas a elas não se limitando):

- Que tipo de dado é coletado?
- Por que é coletado?
- Como o dado é armazenado?
- Por quanto tempo o dado é mantido?
- Há compartilhamento com quais instituições?
- Os dados são regularmente revisados?
- São assegurados os direitos do titular?

Neste momento é feita uma análise sobre o ciclo de vida dos dados e da função que cada agente de tratamento desempenha, sendo relevante atribuir adequadamente as figuras de controlador, operador, controladores conjuntos e suboperador, uma vez que isso reflete as responsabilidades e poder decisório em cada caso.

A ideia é que, a partir de entrevistas diretas com os colaboradores e da análise de outras fontes, como documentos internos, telas de sistemas, relatórios e formulários, seja possível desenhar fluxogramas que reflitam as atividades de tratamento de dados pessoais.

Com base nisso, será possível preencher um inventário de dados constando os processos de tratamento de dados pessoais com os respectivos agentes de tratamento, normas legais aplicáveis, bases legais que amparam o tratamento de dados, controles de Segurança da Informação adotados, dentre outras informações, e, por último, analisar os riscos inerentes a cada processo identificado.

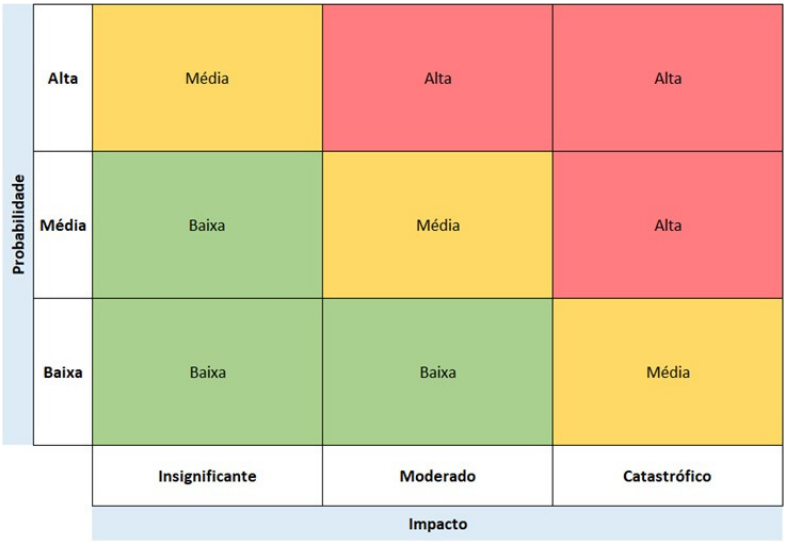
Para tanto, é possível utilizar ferramentas como planilhas, aplicativos e sistemas (a exemplo do Miro, LucidChart, Bizagi, Diagrams.net), bem como plataformas automatizadas do mercado (como OneTrust e Privacy Tools).

3) Análise de riscos e Planejamento

A partir da análise do mapeamento de dados e de todo subsídio tomado, passamos a relacionar as situações que podem revelar desconformidade com a Lei e que representam riscos prejudiciais ao bom funcionamento do escritório, com o objetivo de elaborar um relatório que indique a provável consequência e a respectiva probabilidade de cada evento (intitulado Análise de Riscos), para posteriormente estabelecer medidas capazes de solucionar as problemáticas identificadas (Plano de Ação).

Nesse sentido, esta etapa busca (I) identificar, analisar e avaliar riscos, e (II) traçar estratégias para tratar os riscos identificados e aumentar o nível de conformidade da empresa com a Lei Geral de Proteção de Dados.

Portanto, devem ser considerados os contextos interno e externo do escritório, bem como sua tolerância ao risco (que reflete os valores, objetivos e recursos da organização, sem deixar de considerar os requisitos legais e regulatórios impostos), em uma análise que confronta probabilidade e impacto, conforme ilustrado na seguinte matriz de riscos:



Deve-se ressaltar, ainda, que os riscos podem ser variáveis conforme o decurso do tempo e a modificação dos contextos. Desse ponto decorre a importância de manter monitoramento e análise crítica dos riscos.

4) Implementação

Uma vez identificadas as situação de maior criticidade, serão traçadas estratégias para remediar cada uma delas, de modo a estabelecer um plano para tratamento de riscos que tenha como base medidas em níveis técnico (adoção de ferramentas e controles adequados), documental (atualização de normas, políticas e contratos), procedimental (adequação da governança e da gestão dos dados pessoais) e cultural (realização de treinamentos e campanhas de conscientização das equipes, dos parceiros, fornecedores e, quando for o caso, clientes).

Após a identificação de um risco, define-se a sua tratativa, o que inclui a adoção de medidas preventivas e de mitigação. Para tanto, é preciso que a instituição defina o seu apetite de risco, que, em síntese, reflete o nível de risco que uma organização está disposta a aceitar enquanto persegue seus objetivos.

5) Monitoramento e melhoria contínua

É natural que os processos de determinada organização se modifiquem com o passar do tempo. Também é completamente esperado que o estado da técnica avance com o decorrer dos anos, de modo que novas vulnerabilidades e ameaças sejam identificadas e, por consequência, novas medidas devam ser tomadas em matéria de segurança da informação.

Assim, faz-se necessário que haja frequente análise dos ambientes interno e externo em vista da "quantidade e tipo de risco que uma organização está disposta a buscar, manter ou assumir", ou seja, do apetite de risco da organização, para fins de conformação entre riscos admitidos e medidas tomadas. A prática mencionada consiste na gestão de riscos e é fundamental para a manutenção do Programa de Governança em Proteção de Dados.

Outro ponto relevante, e complementar ao que foi mencionado, é a necessária revisão da documentação, para que esteja sempre atualizada conforme as práticas da organização e, por consequência, sejam sempre pertinentes.

Nesse sentido, ao final, são resultados esperados:

- Alcançar confiança e segurança dos clientes.
- Melhorar a reputação da organização.
- Facilitar a conscientização junto às partes interessadas.
- Garantir aderência à legislação.
- Monitorar continuamente para manter e melhorar o programa de Privacidade e Proteção de Dados.

Comissão de Privacidade
e Proteção de Dados

DOCUMENTOS INTERNOS IMPORTANTES EM PROTEÇÃO DE DADOS PESSOAIS

Por Aline Lemes

Advogada, Consultora jurídica em Proteção de Dados. Graduada em Direito pela Universidade Federal de Uberlândia. Pós-Graduada em Direito Processual pela PUC Minas. Pós-Graduada em Direito Digital pela EBRADI. Extensão em propriedade intelectual pela World Intelectual Property Organization. Certificada em Compliance na Proteção de Dados (CPC-PD) pela LEC em parceria com a FGV. Certificada em Lead Implementer ABNT ISO 27701. Membro da Comissão de Privacidade e Proteção de Dados e Direito para Startup da OAB-MG, Subseção de Uberlândia.

Independentemente se o seu escritório for de grande ou pequeno porte, ou se você for advogado autônomo, estar em conformidade com a LGPD é obrigação de todos os profissionais e as organizações, e o programa de adequação deve ser elaborado respeitando as singularidades de cada negócio, pensando na sua realidade, propósito e desafios.

Isso pode significar desde a atualização de sistemas e software - os quais podem apresentar brechas que podem ser exploradas por criminosos, abrindo caminho para vazamentos e acessos indevidos aos dados pessoais -, necessidade de instalação de câmeras de segurança, limitação de acessos e controle de uso de equipamentos, até um complexo plano de segurança, estabelecido por uma equipe de Tecnologia da Informação.

Ademais, colocar uma organização em conformidade com a LGPD envolve a criação de uma cultura de proteção de dados através de um programa efetivo de Governança em Proteção de Dados. E, para ocorrer essa mudança cultural é indispensável o treinamento contínuo dos seus colaboradores.

A conscientização para os colaboradores, por serem o elo mais fraco da segurança da informação, ajuda incorporar a cultura de proteção de dados no dia a dia do escritório. Por isso, devemos conscientizar os colaboradores a respeito de medidas básicas de segurança, principalmente no que diz respeito aos riscos e as consequências em razão do acesso e compartilhamento indevido de dados pessoais, conforme brevemente exposto anteriormente.

Destaca-se que o programa de governança em proteção de dados tem como objetivo estabelecer a confiança entre organização e titular de dados, demonstrar comprometimento e transparência, assim como elevar o nível de satisfação do cliente ao proporcionar uma melhor experiência.

Entretanto, a adequação de uma organização às regras da LGPD não se resume em treinamento de pessoal e no emprego de medidas de segurança, especialmente pela adoção de tecnologias, mas inclui também a obrigatoriedade de elaboração, manutenção e revisão de documentos capazes de formalizar as medidas e instruções adotadas.

Isso porque os documentos e registros elaborados em um processo de adequação à LGPD são muito mais que evidências fundamentais (as quais eventualmente serão utilizadas em demandas administrativas, processos judiciais e/ou due diligence), são ferramentas importantes para a manutenção, avaliação, mitigação e gestão dos riscos relacionados à privacidade e proteção de dados. E, claro, servem também à melhoria contínua e ao atendimento constante da Lei Geral de Proteção de Dados.

Diante disso, antes de adentrar na descrição dos principais documentos que ajudam a comprovar a conformidade com a LGPD, é importante esclarecer algumas questões. A LGPD exige registros e documentos? Onde exatamente está especificado quais são os documentos necessários?

Pois bem, o artigo 37 da LGPD traz expressamente que é dever do controlador e do operador manter registros das suas atividades de tratamento de dados pessoais. Porém, não descreve quais registros ou conteúdos devem ser elaborados. Confira:

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Não bastasse isso, o art. 50 da LGPD traz a necessidade de adotar boas práticas e governança para o tratamento de dados pessoais, assim como a mitigação dos riscos associados. Vejamos:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Assim, como a lei não é taxativa quanto a documentação, reiteramos que é possível que os documentos necessários para adequação à LGPD variem, a depender do modelo de negócio e dos propósitos e riscos. Contudo, existem alguns documentos que são comuns às mais variadas formas. Desse modo, a seguir estão dispostos alguns documentos capazes de demonstrar boas práticas e ajudar a comprovar a conformidade com a LGPD.

Frise-se, entretanto, que a mera existência desses documentos no âmbito de uma organização não é capaz de suprir qualquer demanda relacionada à LGPD: é preciso que eles reflitam a realidade prática!

Ademais, caso seja um grande escritório, é importante que seja designada uma equipe que cuidará da implementação e da manutenção do programa de adequação, orientando e fiscalizando os demais quanto às novas regras e corrigindo eventuais falhas na execução do projeto. Já nos casos de pequenos escritórios ou advocacia autônoma, o ideal é que uma pessoa seja designada para desempenhar tal função, conforme a possibilidade.

Cronograma de gestão

O cronograma de gestão tem como objetivo alicerçar e consolidar o planejamento das ações e atividades a serem desenvolvidas. Este documento é fundamental para o acompanhamento das ações de adequação, execução e implementação, pois servirá como um norteador das diretrizes para uma governança e alinhamento às boas práticas. Trata-se, ainda, de uma forma de evidenciar as medidas adotadas pela organização ou em vias de serem adotadas.

Mapeamento de Dados

O mapeamento de dados, ou ainda, data mapping ou data flow, refere-se a um documento essencial no processo de adequação à LGPD. O principal objetivo desse documento é demonstrar o caminho percorrido pelos dados pessoais dentro da instituição, que vai desde a coleta, armazenamento, compartilhamento até o efetivo descarte.

Em razão da quantidade de informações que esse documento deve conter, e até mesmo para melhor compreensão, ele tem sido apresentado em forma de planilha. A sua elaboração constitui um trabalho minucioso, pois é no mapeamento de dados que o escritório irá levantar todos os dados coletados, estabelecer finalidades, bases legais, formas de acesso e armazenamento, fluxo dos dados e métodos de eliminação e descarte.

Registro de Operações de Tratamento de Dados

O Registro de Operações de Tratamento de Dados Pessoais visa descrever os processos e atividades de tratamento de dados pessoais realizados pela empresa, na qualidade de operadora e/ou controladora, refletindo o que foi constatado no mapeamento de dados. Trata-se de documento obrigatório a todos aqueles que se qualificam como agentes de tratamento de dados e que atende o disposto no artigo 37 da LGPD, mencionado anteriormente.

Política de privacidade

A política de privacidade normalmente está disponível em sites, blogs, aplicativos e redes sociais, de forma a alcançar o titular e indicar a atualização das questões da organização relacionadas à Privacidade e Proteção de Dados

. É na política de privacidade que o controlador ou o operador deve informar para o titular o que será feito com seus dados pessoais, motivo pelo qual é recomendável utilizar uma linguagem clara e objetiva, de forma que o homem médio compreenda o que está sendo dito.

O art. 9º da LGPD traz algumas informações que esta política deve contemplar, tais como: finalidade específica do tratamento; forma e duração do tratamento de dados; identificação do controlador dos dados; informações sobre o compartilhamento dos dados pelo controlador e a sua finalidade; responsabilidades dos agentes que realizam o tratamento de dados; informações sobre os direitos do titular e como são atendidos esses direitos. Por fim, é importante que esse documento seja público, isto é, disponibilizado em lugar de fácil acesso, como no website da empresa.

Política de retenção e exclusão de dados

A política de retenção e exclusão de dados determinará como será a retenção (durante o tratamento) e a exclusão (quando não mais houver utilidade) dos dados. A LGPD determina que os dados recolhidos devem ser armazenados pelo tempo que se fizer necessário para cumprir a finalidade desejada pela entidade, sendo que tais finalidades devem ser amparadas pelas bases legais dispostas nos artigos 7º e 11.

Código de conduta

O Código de Conduta é o documento que define padrões de comportamento e forma de atuação do escritório com o seu público externo, assim como internamente na rotina de trabalho. Nesse documento constarão publicamente todas as práticas relacionadas à proteção de dados pessoais, com o intuito de consolidar um padrão de funcionamento relacionado às informações relevantes e sensíveis para o escritório. A ideia é conseguir trazer, a partir de uma linguagem simples e objetiva, qual é a postura do escritório frente à Proteção dos Dados do titular e frente à própria LGPD.

Plano para atendimento dos direitos dos titulares

Basicamente, este plano deverá ser um guia orientativo para atender às solicitações do titular (previstas no art. 18 da LGPD, mas a ele não se restringindo) e para isso é importante: entender o papel do escritório dentro de determinada atividade de tratamento de dados (isto é, se é controlador ou se é operador de dados), assim como

um processo interno para verificar a identidade do solicitante, sendo certo que o procedimento de solicitação pelo titular deve ser gratuito e facilitado.

Além disso, deve ser observado o tempo de resposta. Embora a LGPD não estabeleça o tempo determinado de resposta para todas as solicitações (mas somente para as de confirmação de existência e de acesso), recomenda-se que a resposta seja imediata, se em formato simplificado, ou em 15 (quinze) dias, quando por meio de declaração completa. Assim, o escritório deve estar preparado para atender o titular no menor tempo possível, de modo a mitigar riscos relacionados ao bom atendimento.

Política de segurança da informação e plano para gestão de incidentes

A Política de Segurança da Informação é o documento responsável por sintetizar as medidas e controles adotados em matéria de segurança da informação, cujos aspectos básicos foram mencionados anteriormente. Já o Plano para gestão de incidentes é o documento que concentra as estratégias que serão adotadas para lidar em situações de conversão das ameaças e vulnerabilidades em prejuízo material. Mais precisamente, ele deve descrever o processo adotado para gerenciar os incidentes, como também a maneira em que será realizada a comunicação interna, assim como para as Autoridades e para os titulares envolvidos.

Por fim, para além dos documentos brevemente expostos, sugere-se que os contratos contenham cláusulas específicas sobre a proteção de dados, sendo necessária uma análise das atividades que requerem a coleta de dados pessoais, a fim de estabelecer as cláusulas que serão inseridas. Essa orientação serve tanto para contratos com clientes, quanto com parceiros,
colaboradores e prestadores de serviços.

Todo o exposto revela a necessidade de documentar questões específicas relativas à atuação de um escritório de advocacia. Entretanto, a depender de cada caso específico, muitas outras medidas serão necessárias e recomendadas para garantir o cumprimento da Lei. Repisa-se que a manutenção da conformidade e a efetividade de todas as políticas e documentos dependerá da constante realização de capacitação dos colaboradores, que é medida indispensável ao fortalecimento da cultura de proteção de dados e da valorização dos controles internos da gestão.

REFERÊNCIAS

ANPD. Autoridade Nacional de Proteção de Dados. Comunicação de Incidente de Segurança. Publicado em 23 de dezembro de 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em 05 de junho de 2023.

ANPD. Autoridade Nacional de Proteção de Dados. Guia Orientativo Para Definições Dos Agentes De Tratamento De Dados Pessoais E Do Encarregado. Abril de 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em 20 de março de 2023.

ANPD. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-regulamento-de-dosimetria/Resoluca on4CDANPD24.02.2023.pdf/view. Acesso em 05 de junho de 2023.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2ª ed Rio de Janeiro: Forense, 2020. BRASIL. Superior Tribunal de Justiça. Agravo em Recurso Especial nº 2130619 – SP (2022152262-2). Relator: Ministro Francisco Falcão. Brasília, 7 de março de 2023. Disponível em:https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp? livre=%27202201522622%27.REG. Acesso em 15 mar. 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15/06/2022.

GUARIENTO, Daniel Bittencourt; MARTINS, Ricardo Maffeis. Qual o papel dos advogados enquanto agentes de tratamento de dados: controladores ou operadores? Publicado em: 6 de novembro de 2020. Disponível em: https://www.migalhas.com.br/coluna/impressoes-digitais/336001/qual-o-papel-dos-advogados-enquanto-agentes-de-tratamento-de-dados--controladores-ou-operadores. Acesso em 16 de abril de 2023.

IBGC. Instituto Brasileiro de Governança Corporativa. Código das Melhores Práticas de Governança Corporativa. 5ª Edição. São Paulo: IBGC, 2015.

IBMSECURITY.Relatóriodocustodeumaviolaçãodedados2021.Disponívelem:
https://www.ibm.com/downloads/cas/RBJ6BJVN. Acesso em: 25/06/2022.

MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura [coord.]. Comentários à Lei Geral de Proteção de Dados. Indaiatuba, SP: Editora Foco, 2022.

RODOTÁ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SECURITY REPORT. Brasil foi o 5° país com mais ataques cibernéticos em 2021. Grandes empresas fazem parte de um total de 9,1 milhões de ocorrências, apenas no primeiro trimestre. Publicado em 11 de abril de 2022. Disponível em:
https://www.securityreport.com.br/overview/brasil-foi-o-5o-pais-com-mais-ataques-ciberneticos-em -2021/#.YrElV3bMLrc. Acesso em: 05 de junho de 2023.

SERASA EXPERIAN. Boas Práticas em Governança de Dados. Disponível em https://www.serasaexperian.com.br/images-cms/wp-ontent/uploads/2021/05/whitepaper-lgpd-v2.p df. Acesso em 20 de março de 2023.

SERPRO. Quais são os seus direitos. Acessar, corrigir, eliminar dados, e outros. Conhecer seus direitos, garantidos pela LGPD, é o primeiro passo para poder exercê-los. Disponível em: https://www.serpro.gov.br/lgpd/cidadao/quais-sao-os-seus-direitos-lgpd. Acesso em: 10 de maio de 2023.

Comissão de Privacidade
e Proteção de Dados

13ª SUBSEÇÃO
UBERLÂNDIA