OAB RIO GRANDE DO SUL

ESA 35 anos

Comissão Especial de
Proteção de Dados e Privacidade

CARTILHA DE PROTEÇÃO DE DADOS PARA A ADVOCACIA

PORTO ALEGRE
2020

CARTILHADE PROTEÇÃO DE DADOS E PRIVACIDADE PARA A ADVOCACIA - OAB/RS

CEPDP

Comissão Especial de Proteção de Dados e Privacidade da OAB/RS

RIO GRANDE DO SUL ESA 35 anos | Comissão Especial de Proteção de Dados e Privacidade

Porto Alegre, 2020

CEPDP – Comissão Especial de Proteção de Dados e Privacidade da OAB/RS

Presidente
André Luiz Pontin
1º Vice-Presidente
Ana Paula Oliveira Ávila
2º Vice-Presidente
Shamir Haim
Secretária-Geral
Ana Paula França Cavalari
Secretária Redes Sociais e Comunicação
Maria Alice dos Santos Severo
Também colaboraram com esta cartilha
Giovani A. Saavedra e Caroline Stürmer Corrêa

C727

Comissão Especial de Proteção de Dados e Privacidade da OAB/RS.

Cartilha LGPD para a Advocacia. – Porto Alegre: OABRS, 2020. 20p.

1. LGPD – Proteção de Dados e Privacidade. Cartilha. 2. Advocacia. I. Título.

347.721

O conteúdo é de exclusiva responsabilidade dos seus autores.

Ordem dos Advogados do Brasil
Rua Washington Luiz, 1110 – Centro – CEP 90010-460 – Porto Alegre -RS

ORDEM DOS ADVOGADOS DO BRASIL - SECCIONAL DO RIO GRANDE DO SUL

Presidente: Ricardo Breier

Vice-Presidente: Jorge Luiz Dias Fara

Secretária-Geral: Regina Adylles Endler Guimarães

Secretária-Geral Adjunta: Fabiana Azevedo da Cunha Barth

Tesoureiro: André Luis Sonntag

SUMÁRIO

PALAVRA DO PRESIDENTE

A temática do compliance é uma realidade na sociedade brasileira. A advocacia gaúcha precisa estar alinhada com estes conceitos e estas práticas que passam a fazer parte do universo de muitas empresas.

Observando que as boas práticas de governança corporativa e compliance constituem um pilar de sustentação para todas as organizações, orientando a atuação destas pela ética, integridade e transparência, a diretoria da OAB/RS criou o Comitê de Governança e Proteção de Dados no Sistema OAB/RS, que será responsável pela observância das melhores práticas de Governança, Compliance e Proteção de Dados e difusão de uma cultura de ética e de integridade no âmbito da Seccional.

É importante reforçar que a Lei Geral de Proteção de Dados Pessoais (LGPD) foi aprovada em agosto de 2018 e ainda tem uma data incerta para entrar em vigor – a previsão inicial era agosto de 2020, mas ainda não há uma confirmação. A nova lei busca criar um cenário de segurança jurídica, com a padronização de normas e práticas, para promover a proteção de dados pessoais de todo cidadão que esteja no Brasil.

O objetivo é o de proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Ciente da relevância do tema e da importância dessas medidas, a OAB/RS também se movimenta para que essa proteção de dados ocorra dentro da entidade. Medidas serão implantadas na Ordem, mesmo antes da vigência da lei.

É mais do que necessário nos aprofundarmos em novos desafios que a sociedade traz. A OAB/RS, que incorpora nas suas práticas o compliance, cumpre o seu papel de ser protagonista dos debates e da difusão do conhecimento, aproximando advogados e advogadas das melhores práticas e diretrizes de compliance e proteção de dados e de privacidade.

Ricardo Breier

Presidente da Ordem dos Advogados do Brasil/RS

APRESENTAÇÃO

Esta obra pretende ser um guia aos profissionais da advocacia, vislumbrando os novos riscos e responsabilidades advindos da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) em suas atividades profissionais. Também tem como meta auxiliar o profissional no exercício de suas atividades como consultor nos programas de adequação em proteção de dados e privacidade para organizações públicas e privadas, assim como na defesa dos interesses do cidadão titular de dados.

A construção desta cartilha foi coletiva, com contribuições oriundas dos membros da Comissão Especial de Proteção de Dados e Privacidade da OAB/RS e supervisão, coordenação e redação final realizada por sua Diretoria. As diferentes experiências e competências da equipe foram fundamentais para o resultado obtido.

Durante a realização desta obra, a Comissão Especial de Compliance da OAB/RS elaborou a Cartilha de Compliance para a Advocacia, com um capítulo especial sobre *compliance de dados*. Considerando a qualidade do texto, as zonas de intersecção dos temas e a participação comum de membros desta comissão na elaboração daquele material, optamos por reproduzir o referido capítulo, e desde já agradeço a cedência, parabenizando seus autores.

Esta Cartilha foi concluída e está sendo lançada durante o prazo de vigência da MP 959, que prorroga (dependendo de sua conversão em Lei) a maior parte da LGPD para maio de 2021, sendo que as sanções administrativas já foram prorrogadas para agosto de 2021. A Autoridade Nacional de Proteção de Dados - ANPD também não foi formalmente criada, tampouco ocorreu a indicação dos nomes técnicos para a composição de seu Conselho Diretor.

Dessa maneira, a leitura desta Cartilha deve ser realizada no contexto de uma relativa insegurança jurídica. Em que pese a norma e seus princípios não sofrerem alterações, é provável que a atuação judicial e a construção dessa importante disciplina pela ANPD representem fatores de mudança, para os quais devemos estar permanentemente atentos.

Esperamos com essa cartilha colaborar para o aprofundamento da cultura de proteção de dados e privacidade nas organizações e na vida quotidiana, além de motivar os advogados para o exercício de uma de suas missões mais relevantes, a defesa dos direitos e liberdades.

André Luiz Pontin
Presidente CEPDP OAB/RS

1. HISTÓRICO – CONTEXTUALIZAÇÃO – LEGISLAÇÃO

A preocupação pela preservação da privacidade, intimidade e sigilo não é nova. Nasceu, praticamente, com a própria sociedade e, com as nuances características de cada época histórica, sempre foi importante para a harmonia social e para o bom desenvolvimento das relações humanas. Mesmo não sendo uma noção recente, somente no final do séc. XIX o direito à privacidade começou a ser objeto de normatização.

Geralmente se reconhece como marco inicial o trabalho realizado por Warren e Brandeis, com seu artigo *The right to privacy* (1890). Outras obras e um detalhamento sobre a evolução histórica do conceito, passando pelo "direito de estar só" (the right to be let alone) e alcançando, modernamente, uma complexidade que indica até mesmo a interconexão dos conceitos de privacidade e proteção de dados, podem ser encontradas na bibliografia citada ao final desta cartilha.

Parece essencial referir a importância que o tema atingiu, por um lado, após diversas experiências autoritárias no cenário global, as quais promoveram perseguição ativa de opositores a partir da utilização dos dados pessoais revelados; por outro lado, as exigências de proteção da privacidade se elevam com o surgimento de novas tecnologias e a disseminação do uso de computadores em rede, proporcionando as condições para um incremento inédito na forma de coleta, armazenamento e processamento de dados.

Quanto à evolução legislativa, esta somente tornou-se sistêmica, estruturada e de aplicabilidade geral quando as relações de comércio internacional e comunitárias, fomentadas pelas novas facilidades tecnológicas, necessitaram garantir a livre circulação dos dados pessoais, com alguma garantia de privacidade e segurança.

A conjunção desses fatores (aprimoramento das redes de telecomunicação, quebra de barreiras comerciais e acordos de cooperação técnica) potencializou a necessidade da criação de leis de proteção de dados pessoais, de maneira a garantir a continuidade das transações de compartilhamento e transferência internacional de dados, mantendo um nível compatível de segurança e proteção.

Na evolução legislativa, os europeus sempre estiveram na vanguarda. É importante referir que a primeira lei específica sobre proteção de dados pessoais foi publicada no Estado alemão de Hesse, em 1970, sendo seguida por legislações nacionais em vários países europeus. Em 1995 foi criada a Diretiva 95/46/CE, tratando especificamente da proteção de dados pessoais para todos os países membros da União Europeia, diretiva essa que evoluiu até a publicação, em 2016, da GDPR (General Data Protection Regulation), que entrou em vigor em 2018.

A partir deste marco legal, a inserção real e prática do tema proteção de dados pessoais para a garantia das liberdades políticas, somada a escândalos de manipulação eleitoral em países centrais, gerou uma demanda no mundo inteiro para criação de legislações próprias e autoridades nacionais.

No Brasil, a privacidade é protegida por diversas fontes, dentre as quais destacamos a Constituição Federal (CF/88), o Código de Defesa do Consumidor, o Marco Civil da Internet (Lei 12.965, de 2014) e sua regulamentação (Decreto 8.771, de 2016), a Lei do Cadastro Positivo (Lei Complementar 166, de 2019) e a Lei de Acesso à Informação (Lei 12.527, de 2011).

A par da proteção constitucional e dos microssistemas regulatórios, a evolução para uma Lei Geral iniciou em 2010 com a primeira consulta pública de um Anteprojeto de Lei, mas só ocorreu de fato a partir da pressão internacional para que o Brasil adotas se mecanismos de proteção de dados pessoais equivalentes aos dos países do bloco europeu. Com a sanção da Lei nº 13.709, em 14 de agosto de 2018, instituiu-se no país um regime geral de proteção de dados, consolidando e complementando o marco normativo da sociedade da informação então vigente no Brasil.

Há muito se discute se também existe no ordenamento brasileiro um direito fundamental à proteção de dados. Uma leitura atenta do texto constitucional permite notar que a Constituição Federal traz normas e princípios que podem tutelar os dados pessoais, notadamente a partir da interpretação conjunta da garantia da inviolabilidade da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art.1º, III, CF/88,) e da garantia processual do habeas data (art. 5º, LXXII).

O Supremo Tribunal Federal, em recente decisão monocrática da ministra Rosa Weber, suspendeu a eficácia da MP 954/2020 e reconheceu a existência no ordenamento brasileiro do direito à autodeterminação informativa.

Até o momento de fechamento deste material, está em apreciação uma Proposta de Emenda à Constituição (PEC 17/2019) que inclui a proteção de dados pessoais disponíveis em meios digitais na lista das garantias individuais da Constituição Federal.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) foi promulgada em 14 de agosto de 2018, estando vigente desde sua promulgação a criação da Autoridade Nacional de Proteção de Dados - ANPD. No momento do fechamento deste guia, as sanções da LGPD foram postergadas para agosto de 2021 e o texto efetivo da Lei aguardando a extinção ou conversão em Lei da MP 959, que prevê sua vigência em maio de 2021.

2. PRINCÍPIOS DA LGPD

A Lei Geral de Proteção de Dados Pessoais – LGPD tem como fundamento norteador a proteção dos direitos e garantias fundamentais do indivíduo, como o respeito à privacidade, inviolabilidade da intimidade, da honra e da imagem, livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania.

No entanto, a proteção de tais direitos deve ser assegurada mantendo o equilíbrio com outras garantias, tais como a liberdade de expressão, de informação, de comunicação e de opinião, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor.

A LGPD objetiva a efetividade desses direitos fundamentais, arrolando princípios que permeiam todos os dispositivos da lei e orientam a compreensão, interpretação e aplicação das regras por ela estabelecidas.

BOA-FÉ

A boa-fé é princípio que norteia amplamente nosso ordenamento jurídico e, na LGPD, serve de orientação às condutas relacionadas ao tratamento de dados pessoais,

criando deveres anexos aos decorrentes da lei, tais como de lealdade, transparência e lisura aos agentes de tratamento.

Ao realizar o tratamento dos dados, devem ser observados os direitos e liberdades fundamentais e a relação de confiança estabelecida diante das legítimas expectativas do titular, originadas a partir das informações previamente fornecidas pelos agentes.

FINALIDADE

O legislador vincula o princípio da finalidade ao tratamento dos dados de acordo com os propósitos legítimos específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com estas finalidades.

A finalidade é elemento central, pois é a partir dela que serão definidos os limites no tratamento dos dados. Neste sentido, o tratamento em desacordo com a finalidade prevista no consentimento dado ou em lei torna o consentimento ineficaz e configura conduta ilícita, gerando a pretensão à reparação aos danos materiais e morais, de acordo com o caso concreto e sem prejuízo das demais sanções cabíveis.

ADEQUAÇÃO

Previsto no art. 6º, II, o princípio da adequação estabelece que o tratamento de dados deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

Por esta razão, o agente deverá verificar se, no caso concreto, o tratamento dos dados está realmente vinculado, adequado e compatível com as finalidades legais admitidas e com aquelas informadas no termo de consentimento apresentado ao titular.

Igualmente, no eventual tratamento posterior ou uso secundário dos dados, deve ser analisado o contexto do tratamento, de forma a respeitar os limites estabelecidos na sua finalidade.

NECESSIDADE

Segundo o princípio da necessidade, o tratamento dos dados (coleta, recepção, classificação, transmissão, armazenamento, etc.) deve se limitar ao mínimo necessário para a consecução das suas finalidades.

O agente deve avaliar se os dados são realmente pertinentes, essenciais e não excessivos para atingir os resultados pretendidos. A análise inicial e sistemática desses dados permite aferir sua real necessidade e mitigar potenciais riscos aos titulares, preservando seus direitos à privacidade, à inviolabilidade da intimidade, da honra e da imagem.

LIVRE ACESSO

Considerando que o tratamento dos dados deve estar de acordo com as finalidades legais admitidas e com aquelas previstas no consentimento dado, o titular

deve ter livre acesso à integralidade de seus dados, bem como à forma e duração do tratamento mediante consulta facilitada e gratuita.

Mediante o livre acesso aos seus dados, o titular poderá acompanhar sua utilização e, quando for o caso, exigir a retificação dos registros incorretos ou imprecisos, bem como anonimização, bloqueio ou eliminação daqueles que forem excessivos.

QUALIDADE DOS DADOS

O princípio da qualidade dos dados, conforme expresso no artigo 6º, V, da LGPD, visa a *"garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. "*

O controlador deve manter os dados de forma exata, clara e atualizados, impedindo que informações incorretas, incompletas, imprecisas, excessivas e em desacordo com a lei sejam associadas ao titular, visando preservar seus legítimos interesses.

A ausência de qualidade dos dados resultará em cruzamentos, transmissão e outras operações de forma viciada, gerando riscos potenciais ao titular, cujos direitos devem ser preservados.

TRANSPARÊNCIA

Este princípio tem como enfoque principal a possibilidade de o titular ter acesso às informações sobre a realização do tratamento dos dados e seus agentes. Tais informações devem ser prestadas ao titular, ressalvados os segredos comerciais e industriais, de forma clara, precisa e facilmente acessível, inclusive com relação às consequências deste tratamento. A partir destes elementos, o titular poderá identificar se estão sendo observados os dispositivos da lei no tratamento de seus dados e tomar decisões para garantir a efetividade de seus direitos.

SEGURANÇA

O tratamento de dados pessoais, sensíveis ou não, envolve riscos que são inerentes à atividade desenvolvida pelo controlador, que deverá adotar as medidas "*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 difusão*", conforme expresso no artigo 6º, VII, da LGPD.

Além do controlador, o operador ou qualquer outra pessoa que intervenha em uma das fases do tratamento deverá garantir a segurança da informação, mesmo após o seu término, podendo responder por eventuais danos causados pela violação caso não tenha adotado as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. A autoridade nacional poderá dispor sobre os padrões mínimos destas medidas.

PREVENÇÃO

Em complemento à segurança das informações, o princípio da prevenção requer, em uma etapa anterior, que sejam adotadas medidas capazes de prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, em todas as etapas de desenvolvimento de produtos e serviços.

Além das medidas de prevenção no desenvolvimento de produtos e serviços, o legislador destaca a importância da elaboração de regras de boas práticas e de governança em privacidade que considerem a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

NÃO-DISCRIMINAÇÃO

Os dados sensíveis trazem informações como a origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual etc., que podem gerar vulnerabilidade aos direitos fundamentais do indivíduo, considerando a possibilidade de serem utilizados para fins discriminatórios ilícitos ou abusivos.

A LGPD, em convergência com a Constituição Federal, a qual proíbe preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação, veda expressamente que o tratamento desses dados seja realizado com aqueles fins.

PRESTAÇÃO DE CONTAS E RESPONSABILIZAÇÃO

O agente, além de observar e cumprir as normas de proteção de dados pessoais deve ser capaz de demonstrá-lo, inclusive no que se refere à eficácia das medidas adotadas.

O artigo 50 da LGPD prevê o dever do controlador de demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável.

3. DIREITOS E DEVERES DECORRENTES DA PROTEÇÃO DOS DADOS PESSOAIS:

Os advogados, para além de cidadãos no gozo do direito à privacidade e à proteção de seus dados pessoais, são também depositários de dados pessoais dos clientes. A seu turno, as sociedades de advocacia são depositárias de dados pessoais dos clientes e também dos seus colaboradores. O Código de Ética da OAB sempre consagrou como dever o sigilo profissional e a confidencialidade de todas as informações obtidas junto aos clientes por força da contratação de serviços advocatícios. Agora, além disso, advogados e escritórios serão considerados agentes de tratamento para todos os efeitos da Lei Geral de Proteção de Dados. Diante disso, devem estar cientes tanto dos direitos previstos na Lei, quanto dos deveres que deles decorrem, por isso foram selecionados os aspectos legais que mais atenção exigirão da advocacia:

TITULARIDADE DOS DADOS PESSOAIS:

O titular, em geral não é obrigado a fornecer dados pessoais; no entanto, em alguns casos, a lei exige que sejam fornecidos como condição à prática de certos atos, como é o caso de operações em casas de câmbio e da aquisição de bens imóveis, em que a identificação do comprador é uma exigência regulamentada no âmbito do COAF. Noutras situações, como na celebração de contratos, haverá interesse na identificação das partes contratantes e, portanto, os dados deverão ser coletados. Em todos os casos, o titular deverá ser informado da finalidade para a qual seus dados estão sendo exigidos.

O CONSENTIMENTO PARA A COLETA DE DADOS PESSOAIS:

Fora das situações legais, os dados pessoais somente serão coletados se houver o consentimento do titular, manifestado de forma expressa. Nessa oportunidade, o titular deve ser informado da finalidade da coleta dos dados, decidindo se os fornece ou não. As consequências do não fornecimento dos dados também deverão ser informadas ao titular.

O consentimento para tratamento dos dados pode ser revogado a qualquer momento e os dados poderão ser eliminados mediante requerimento expresso do titular. Essa solicitação deverá ser atendida imediatamente, salvo quando o requerido não seja o agente de tratamento (caso em que deverá indicar, sempre que possível, quem é o agente) ou apresente justificativa que impeça a eliminação imediata dos dados (art. 18, §§3º e 4º). Os dados não poderão ser eliminados nos casos em que a lei determine sua conservação, para cumprimento de obrigação legal ou regulatória pelo controlador, entre outros casos (art. 18, VI, c/c 16).

Ainda que a exigência do consentimento seja uma das questões centrais da LGPD, a celebração de contrato para a prestação de serviços advocatícios pode ser reconhecida entre as hipóteses em que o tratamento dos dados é permitido pela lei independentemente da manifestação do consentimento, ou seja: (a) quando necessário para a execução de contrato ou procedimentos preliminares de contrato em que seja parte o titular, a pedido seu (art. 7º, inc. V); (b) para o exercício de direitos em processo judicial, administrativo ou arbitral (art. 7º, inc. VI); (c) quando necessário para atender aos legítimos interesses de controlador ou de terceiro (art. 7º, inc. IX). Mesmo assim, como a informação quanto à finalidade do tratamento dos dados do cliente é indispensável, recomenda-se que o contrato especifique a necessidade e a finalidade da coleta, já que necessária à defesa dos seus interesses.

Atente-se que a coleta de dados para formação de cadastro em sítios de internet (web sites), assim como o envio de “new letters” e informativos por parte do escritório não se inserem naquelas categorias e, por isso, somente podem realizados mediante o consentimento dos destinatários.

DIREITO DE INFORMAÇÃO:

O titular deve ser informado sobre a finalidade do tratamento dos seus dados, e a operação dos dados deve estar estritamente vinculada à finalidade informada; se mudar a finalidade, novo consentimento deve ser manifestado. Deve haver o cuidado de que somente os dados estritamente pertinentes e necessários para a finalidade sejam

coletados. O titular também tem o direito de saber sempre que houver compartilhamento dos seus dados com outras entidades, sejam públicas ou privadas. Recomenda-se que todas essas informações sejam disponibilizadas ao cliente no ato de contratação dos serviços advocatícios, preferencialmente no próprio instrumento contratual, pois a documentação comprobatória quanto à comunicação ao cliente poderá ser necessária perante a ANPD.

DIREITO AO LIVRE ACESSO:

O titular tem livre acesso às informações sobre o tratamento dos seus dados, que deverão ser claras e precisas. A consulta quanto à forma e duração do tratamento, assim como a exatidão dos seus dados pessoais é gratuita. Os dados deverão ser armazenados em formato que favoreça o acesso, e poderão ser solicitados aos agentes de tratamento por via eletrônica ou impressa. O titular tem o direito de obter, a qualquer tempo e mediante requisição, a confirmação da existência de tratamento quanto aos seus dados, sendo atendido imediatamente e em formato simplificado, ou no prazo de 15 dias no caso de informações mais complexas.

Esse direito, contemplado no art. 18, inc. II e no art. 19 da LGPD, exigirá uma organização bem estruturada das informações pessoais dos clientes que são mantidas nos escritórios de advocacia, tanto em arquivos físicos como digitais, além da garantia de que estejam protegidos contra o acesso indevido, por conta do direito à segurança dos dados. Recomenda-se que os escritórios organizem procedimentos-padrão de pronta resposta às solicitações de clientes quanto aos dados pessoais armazenados e também quanto ao tratamento a eles dispensado.

DIREITO À SEGURANÇA DOS DADOS:

O titular tem direito à segurança dos dados pessoais fornecidos, com o correspondente dever dos agentes de tratamento de adotar medidas técnicas para garantir a proteção dos dados contra o acesso indevido, destruição, perda, alteração, comunicação ou difusão. As medidas de segurança adotadas devem ser comunicadas ao cliente e devem ser passíveis de comprovação perante a autoridade nacional; os cuidados devem ser redobrados em relação às demandas judiciais que requeiram dados sensíveis, ou de menores, concernentes a clientes, contrapartes e também testemunhas que participem nos processos.

RESPONSABILIDADE DOS AGENTES DE TRATAMENTO:

No caso de danos decorrentes do tratamento dos dados pessoais (dano efetivo ou risco relevante), o titular terá direito à responsabilização dos agentes de tratamento e à correspondente indenização. Conforme a especificidade do dano, os escritórios e seus profissionais poderão responder a processo disciplinar perante o Tribunal de Ética e Disciplina da OAB e/ou a processo administrativo perante a Autoridade Nacional de Proteção de Dados, além de eventual demanda individual do titular lesado para ressarcimento do dano causado. Por tal razão, recomenda-se o treinamento específico e contínuo de todos os advogados e demais colaboradores quanto às políticas de proteção dos dados vigentes no escritório.

DIREITO À NÃO-DISCRIMINAÇÃO:

O titular tem direito a não ser discriminado de forma ilícita ou abusiva com base nos dados pessoais informados.

DIREITO À RETIFICAÇÃO, ANONIMIZAÇÃO, ELIMINAÇÃO OU BLOQUEIO DOS DADOS:

O titular tem direito à retificação de dados incorretos ou incompletos e, se os dados não forem de manutenção obrigatória por exigência legal ou contratual, tem direito a solicitar sua eliminação. Segundo a LGPD, sempre que possível, os dados serão anonimizados, ou seja, tratados de forma a não permitir a identificação do titular; dados desnecessários ou excessivos são aqueles que não atendem às finalidades informadas para o tratamento e, por isso, devem ser eliminados.

Sempre que requerida a correção, anonimização, bloqueio ou eliminação dos dados pessoais do titular, o agente de tratamento deverá providenciar para que a mesma medida seja adotada por todos os demais agentes com quem tenha havido compartilhamento das informações.

DIREITO À REVISÃO DE DECISÕES AUTOMATIZADAS:

Sempre que sujeito a decisões automatizadas por sistema de algoritmo, o titular tem direito a obter informações sobre os critérios e procedimentos empregados no processo de decisão, além do direito a solicitar a revisão dessas decisões (LGPD, art. 20).

DIREITO À PORTABILIDADE DOS DADOS:

A lei assegura que o titular possa portar seus dados para outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional (desde que isso não importe em violação de segredos comercial e industrial); assim, por exemplo, se o cliente deseja substituir seu procurador, o anterior mandatário deverá providenciar para que o novo receba todos os dados concernentes ao titular, quando assim requerido.

4. COMPLIANCE DE DADOS: ELEMENTOS PARA ADEQUAÇÃO À LGPD

De modo sintético, a implementação de um programa de conformidade à LGPD deverá considerar as seguintes etapas:

a. Planejamento: *A devida compreensão da lei e como ela irá afetar as atividades da empresa;*

b. Comprometimento da Alta Direção: *O comprometimento da estrutura de gestão da empresa em destinar recursos necessários para as adaptações à LGPD;*

c. Auditoria de Lacunas (*gap assessment*),

d. Definição do *Data Protection Officer* (DPO) ou Encarregado de Proteção de Dados: *A nomeação de um encarregado (pessoa física ou jurídica) que será*

responsável pela estruturação, monitoramento e aprimoramento das boas práticas;

e. Treinamentos iniciais: *Realização de treinamentos/capacitações acerca da necessidade de atender aos requisitos da LGPD (permanente durante o processo);*

f. Mapeamento de Dados (*data mapping*) e Fluxo de Dados (*data flow*),

g. Gerenciamento de Riscos: *Realizar análise de riscos, apontando eventuais inconformidades que possam ocasionar prejuízos às empresas durante o tratamento de dados, com o devido mapeamento das informações em cada uma das etapas – coleta, tratamento, compartilhamento e até mesmo o descarte;*

h. Políticas: *Criar Políticas de Privacidade para os serviços que realizem tratamento de dados pessoais onde fiquem claros os motivos, com finalidade legítima, pelos quais os dados estão sendo coletados e por quanto tempo permanecerão armazenados;*

i. Processos (requerimentos, procedimentos, registros);

j. Revisão de Contratos;

k. Relatório de Impacto a Proteção de Dados (DPIA);

l. Vazamento de Dados (*Data Breaches*);

m. Transferência Internacional de Dados.

Durante o processo de adequação, algumas observações são essenciais:

- ✓ A integração das áreas da empresa, para garantir uma visão global das necessidades de se apoiarem e aprimorarem os projetos de proteção de dados.
- ✓ Fazer ajustes por meio da estruturação de regras que garantam uma política de governança, com normas internas voltadas para a proteção dos dados pessoais, por meio de adequação dos contratos firmados, dos sistemas utilizados, dos processos e procedimentos internos e externos, da limitação dos acessos aos dados protegidos.
- ✓ Criação de um plano de gestão de crise no caso de incidente acarretado pelo descumprimento da lei ou até mesmo vazamento de dados, oportunizando com isso uma capacidade de gerenciamento constante e de resposta imediata, incluindo notificações à ANPD, nos termos exigidos pela Lei.
- ✓ Obtenção de consentimento do titular para tratamento dos dados pessoais existentes na empresa, bem como os que serão coletados.
- ✓ Reavaliação dos dados já coletados, de forma a definir a necessidade de sua manutenção e a eventualidade de seu descarte, primando, desde logo, pela transparência nesses procedimentos.
- ✓ Trabalhar com fornecedores que estejam adequados à LGPD, de forma a evitar riscos indiretos com relação à utilização indevida de dados.
- ✓ Implementar medidas técnicas e administrativas para garantir, por meio de evidências, a segurança de dados pessoais, com a utilização de normas e procedimentos de Gestão de Segurança da Informação e Processos.

5. ANPD: O QUE PODE MUDAR COM O INÍCIO DAS ATIVIDADES DA AUTORIDADE

A Lei Geral de Proteção de Dados (Lei 13.709/2018) se preocupa com o tratamento dos dados pessoais do cidadão. No entanto, diferente do GDPR - Regulamento Geral de Proteção de Dados da União Europeia, em que 173 parágrafos introdutórios explicam os artigos da legislação, a LGPD não traz em seu texto um detalhamento operacional da sua aplicação legal. Nesse viés, a criação da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) é necessária não somente pelo aspecto social e pedagógico de que a lei seja cumprida, como também em razão da regulamentação e do detalhamento dos pontos obscuros dos artigos, os quais serão esclarecidos mediante a normatização e a publicação de orientações técnicas para assegurar a conformidade da implementação.

A Lei 13.853/2019, por sua vez, foi sancionada com o principal objetivo de criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão com vinculação transitória ao Chefe do Executivo pelo prazo máximo de 2 (dois) anos da data de entrada em vigor de sua estrutura regimental. A eficácia e a estabilidade da Autoridade Nacional dependerão da concretização da autonomia e da independência previstas no artigo 55-B, bem como das nomeações dotadas de respaldo técnico, como prevê a legislação.

Entre outras atribuições, a ANPD será responsável por regulamentar as matrizes principiológicas previstas na LGPD, originando conceitos que, todavia, somente estarão disponíveis a partir do início das atividades da Autoridade.

O artigo 48, §1º, da Lei 13.709/2018, por exemplo, impõe ao controlador o dever de comunicar à Autoridade Nacional e ao titular a ocorrência de vazamento de dados que possa acarretar risco ou dano relevante em um prazo razoável. Ainda que o caput do artigo não tenha fixado prazo para comunicação, o inciso V impõe a necessidade de justificar eventual demora, caso não tenha sido “imediata”. Assim, até o momento a Legislação dispõe de conceitos amplos, abertos e até mesmo contraditórios, caso do prazo e da forma de notificação ainda passíveis de definição pela ANPD.

Os acordos contratuais para transferência internacional de dados pessoais por meio das cláusulas-padrão contratuais e as cláusulas específicas para tal finalidade também pendem de regulamentação pela ANPD. Da mesma forma, as empresas que transferem dados para suas subsidiárias fora do país esperam pela definição do mecanismo de aprovação de regras corporativas vinculantes.

O conteúdo e a obrigatoriedade dos relatórios de impacto à proteção de dados pessoais (art.38), assim definida a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, são também objeto da preocupação da Autoridade Nacional.

Além da fiscalização e da garantia da aplicação da Lei, o aspecto mais importante da aguardada regulamentação da lei pela ANPD está na elaboração de pareceres e orientações sobre os temas que auxiliarão nas atividades de conformidade com segurança jurídica. Por esse motivo, é indispensável que os membros da Autoridade tenham conhecimentos técnicos multidisciplinares, além da participação de diversos segmentos sociais afetados.

Presentes na lei diversos artigos que prevê em atribuições à Autoridade Nacional de Proteção de Dados, a ANPD deve ser considerada a referência ativa de uma cultura da privacidade no país, mediante a adoção de condutas que fomentem o comportamento preventivo dos agentes de tratamento e dos próprios cidadãos. A busca é pela conscientização e pela adequação às exigências da LGPD, mediante a elaboração de diretrizes para a própria atuação da Autoridade e da regulamentação da aplicação da Lei.

6. RISCOS E POLÍTICA DE PROTEÇÃO DE DADOS ESPECÍFICOS PARA ADVOCACIA[1]

O Código de Ética e Disciplina da OAB possui um capítulo específico acerca do sigilo profissional, que se impõe aos advogados quanto a todos os fatos a respeito dos clientes de que tome conhecimento no exercício da profissão. A quebra de sigilo pode gerar processo disciplinar junto à Comissão de Ética da OAB, podendo também ter consequências criminais, uma vez que o Código Penal tipifica a quebra de sigilo profissional sem justa causa. Em acréscimo, a recente Lei Geral de Proteção de Dados – LGPD – trouxe novas obrigações a todos os sujeitos que operam com dados pessoais e criou a Autoridade Nacional de Proteção de Dados – ANPD –, órgão responsável por fiscalizar e aplicar as sanções administrativas previstas na lei.

Os escritórios de advocacia também estarão sujeitos à regulamentação da LGPD, uma vez que realizam operação de tratamento de dados quanto aos clientes e colaboradores. Portanto, deverão implementar medidas de segurança quanto às informações mantidas pelo escritório, tanto em meio digital quanto físico. As políticas de proteção de dados adotadas pelo escritório deverão ser executadas e documentadas, pois estarão sujeitas a comprovação em caso de fiscalização pela ANPD. Para estar em plena conformidade com a lei, também é recomendável o treinamento de um encarregado da segurança das informações – o DPO, ou "*data protection officer*" – que ficará responsável pela interface com a Autoridade Nacional e com a comunidade.

Em que pese a dispensa do consentimento expresso, o contrato de prestação de serviços firmado com o escritório deverá informar a finalidade do tratamento dos dados pessoais dos clientes, garantindo o sigilo quanto aos mesmos. As políticas de proteção de dados devem assegurar que todos os envolvidos no negócio (alta direção, advogados, estagiários, correspondentes, mensageiros ou afins, demais colaboradores, parceiros de negócios, terceiros contratados e clientes contratantes) estejam comprometidos com a proteção dos dados, documentos e informações compartilhadas na atividade advocatícia e, particularmente com as seguintes práticas:

- Guardar sigilo dos fatos que tome conhecimento no exercício da profissão.
- O dever de confidencialidade, independentemente de solicitação do cliente, quanto aos seus dados, informações e comunicações.

[1] Capítulo foi extraído integralmente da Cartilha de Compliance para Advocacia, elaborado pela CECOM Comissão Especial de Compliance da OAB/RS.

- O dever de confidencialidade quanto aos dados e informações compartilhadas por cliente potencial deve ser preservado, e se mantém mesmo que a contratação não ocorra.
- O dever de confidencialidade quanto aos documentos que sejam reservados do escritório e não disponíveis ao público, referentes aos negócios do escritório, de seus clientes, de parceiros, de terceiros fornecedores ou contratados.
- A adesão à política de confidencialidade deve ser exigida já na contratação de profissionais e colaboradores pelo escritório; as regras de boas práticas e governança dos sistemas de proteção de dados e informações devem objeto de constante treinamento desde o on-boarding.
- Deve-se exigir o respeito pelos direitos autorais nos termos da lei 9.610/98, quanto aos materiais produzidos pelo escritório.
- Todas as pessoas vinculadas ao escritório devem evitar comentários a respeito dos casos por ele patrocinados fora do ambiente profissional.
- Deve-se respeitar o sigilo profissional nas comunicações com a imprensa e materiais destinados à publicidade.
- Deve-se abster da coleta de informações que envolvam dados sensíveis (exemplificativamente: preferência ideológica, política, religião, raça, saúde, orientação sexual) que possam ser utilizados como fator de discriminação, restringido a coleta desses dados tão somente às hipóteses legais (art. 11 da Lei 13.709/2018).
- Ao contratar serviços de empresas de Tecnologia da Informação (servidores, provedores de internet, hosts de sites etc.), deve-se realizar a due diligence quanto às empresas prestadoras e certificar-se sobre a segurança das informações que serão por elas armazenadas e compartilhadas, tomando o compromisso formal dessas empresas com o devido sigilo e com as normas da Lei Geral de Proteção de Dados.
- Deve-se garantir a segurança da informação, realizando o controle de acesso às informações mantidas no sistema de informática do escritório (política de acesso restrito, com revisão periódica de senha), entre outras medidas assecuratórias.
- Deve-se implementar a proteção e controle do acesso a computadores e aparelhos eletrônicos pessoais (tablets, smartphones etc), por meio de senha pessoal e intransferível (política de treinamentos em segurança da informação).
- Estabelecer prazos para a eliminação dos dados que não se façam mais necessários para o exercício das atividades advocatícias.
- Deve-se instituir formas de acesso e controle a toda comunicação interna e externa estabelecida entre membros do escritório, com meios de acesso ao conteúdo de mensagens e e-mails recebidos; diante da possibilidade de celebração de acordos de leniência ou delação premiada, a impossibilidade de acesso aos documentos e demais materiais probatórios poderá inviabilizar a celebração de tais acordos.

BIBLIOGRAFIA RECOMENDADA

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Gen-Forense: Rio de Janeiro, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei geral de proteção de dados. 2ª Ed. – São Paulo: Thomson Reuters Brasil, 2019.

NÓBREGA, Viviane *et al. Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2019.

SCHERTEL MENDES, Laura. *Privacidade, Proteção de Dados e Defesa do Consumidor: Linhas Gerais de um Novo Direito Fundamenta.*

SHOSHANA, Zuboff: *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Powe.*

MIRAGEM, Bruno. *A Lei Geral de Proteção de Dados (Lei 13.709/2018 e o Direito do Consumidor*. Revista dos Tribunais. vol. 1009/2019. p. 173 – 222. Nov / 2019. DTR\2019\40668

Cartilha de Compliance para a Advocacia. – Porto Alegre: OABRS, 2020.