OAB/DF apresenta

Guia para LGPD na Advocacia

Brasília/DF, 1º de outubro de 2020.

CAA DF
CAIXA DE ASSISTÊNCIA DOS ADVOGADOS DO DF

60 ANOS

OAB
DISTRITO FEDERAL

CAIXA DE ASSISTÊNCIA DOS ADVOGADOS DO DF

60 ANOS

OAB DISTRITO FEDERAL

Expediente

ORDEM DOS ADVOGADOS DO BRASIL
GESTÃO 2019-2021 SECCIONAL DO DISTRITO FEDERAL

Délio Lins e Silva Júnior – Presidente
Cristiane Damasceno – Vice-Presidente
Márcio de Souza Oliveira – Secretário-Geral
Andréa Sabóia de Arruda – Secretária-Geral Adjunta
Paulo Maurício Braz Siqueira - Diretor-Tesoureiro

Escola Superior de Advocacia
Fabiano Jantalia – Diretor-Geral
Dulce Furquim - Diretora Adjunta

Caixa de Assistência dos Advogados
Eduardo Uchoa Athayde – Presidente
Mauro Jr. Pires do Nascimento - Vice-Presidente
Karlos Eduardo de Souza Mares - Secretário-Geral
Aline Cristina de Melo Franco e Oliveira - Secretária-Geral Adjunta
Ana Carolina Franco Costa de Carvalho Rodrigues - Diretora Tesoureira

Comissão de Privacidade e Proteção de Dados Pessoais

Adriana Antunes Winkler – Presidente

Ilderlândio Teixeira – Vice-Presidente

Renata Garcia – Secretária-Geral

Aylon Estrela Neto – Secretário-Geral Adjunto

Comissão de Compliance

Inácio Bento de Loyola Alencastro – Presidente

Flávia Nogueira de Siqueira Campos – Vice-Presidente

Patrícia Andrade de Sá – Secretária-Geral

Antônio Alfredo Ventura de Loiola – Secretário-Geral Adjunto

Encarregado de Dados

Karina Costa - Conselheira Seccional

Organização e Coordenação:

Adriana Antunes Winkler

Revisão:
Adriana Antunes Winkler
Wanderson Melo

Arte:
Isabella Correia

Ordem dos Advogados do Brasil
Seção do Distrito Federal
SEPN 516 Bloco B Lote 7 | Asa Norte | Brasília-DF | 70770-522
Telefone: (61) 3036 9700

Website:
www.oabdf.org.br

Distribuição:
Gratuita - Versão eletrônica disponível para download

Índice

f. Operador

g. Encarregado

h. Autoridade Nacional de Proteção de Dados

i. Tratamento de Dados

j. Mapeamento de Dados

k. Relatório de Impacto a Proteção de Dados

l. Transferência Internacional de Dados

Página 23

4. Princípios

a. Boa-fé

b. Finalidade

c. Adequação

d. Necessidade

e. Livre Acesso

f. Qualidade dos dados

g. Transparência

h. Segurança

i. Prevenção

j. Não Discriminação

k. Responsabilidade e Prestação de Contas

Página 28

5. Direitos do Titular

a. Confirmação da existência do tratamento

b. Acesso aos dados pessoais

c. Correção de seus dados pessoais

d. Eliminação de dados desnecessários, excessivos ou tratamento ilícito

e. Portabilidade dos dados

f. Eliminação dos dados pessoais tratados com o consentimento

g. Informação de compartilhamentos dos dados

h. Informação sobre a possibilidade de não fornecer consentimento

i. Revogação do consentimento

j. Reclamação perante a Autoridade Nacional de Proteção de Dados

k. Oposição ao tratamento nos casos em que discordar do tratamento feito sem seu consentimento e entender que seja irregular

Página 34

6. Bases Legais de Tratamento de Dados
    a. Consentimento
    b. Cumprimento de obrigação legal ou regulatória
    c. Execução de políticas públicas
    d. Estudos em órgãos de pesquisa
    e. Execução de contrato
    f. Exercício regular de direito
    g. Proteção à vida
    h. Tutela da saúde
    i. Interesse legítimo
    j. Proteção do crédito

Página 40

7. Compliance e Proteção de Dados

1.Introdução

a. Palavra do Presidente

É com enorme satisfação que a OAB/DF disponibiliza à advocacia um Guia sobre a LGPD, com o intuito de trazer subsídios necessários ao enfrentamento dos novos desafios advindos da entrada em vigor, no dia 18 de setembro de 2020, da Lei nº 13.709/2018.

O objetivo precípuo do Guia é servir de instrumento básico de consulta aos advogados sobre os diversos temas da LGPD, cujos desafios ainda estão se iniciando.

O Guia aborda conceitos básicos da Lei, princípios que a regem, direitos do titular, bases legais para o tratamento de dados, compliance e proteção de dados e, ainda, as sanções trazidas.

Essa é mais uma iniciativa da OAB/DF para facilitar o exercício profissional da advocacia, notadamente do Distrito Federal, nessa nova área que se abre ao Direito brasileiro; um novo mercado, extremamente promissor e lucrativo para o profissional da advocacia.

Aproveitem o material, que foi feito com muita dedicação e afinco, com a finalidade de aprimorar conhecimentos e trazer luzes ao tema.

Bons estudos e ótimos honorários!

Délio Lins e Silva Junior

b. Sobre a Comissão de Privacidade e Proteção de Dados Pessoais

É a "caçula" das Comissões da OAB/DF, tendo sido oficialmente instituída pela Portaria nº 55, de 20 de agosto de 2020, poucos dias antes da votação da MP 959, que, dentre diversos assuntos em seu texto trazia também a data de entrada em vigor da Lei Geral de Proteção de Dados, ponto extremamente controverso até então.

Ter uma Comissão com a especificidade em Privacidade e Proteção de Dados como outras Seccionais – Rio de Janeiro, Rio Grande do Sul, Minas Gerais e Acre – é falar à sociedade e às organizações brasileiras quanto a OAB/DF está inserida e disposta a contribuir nesta importante temática.

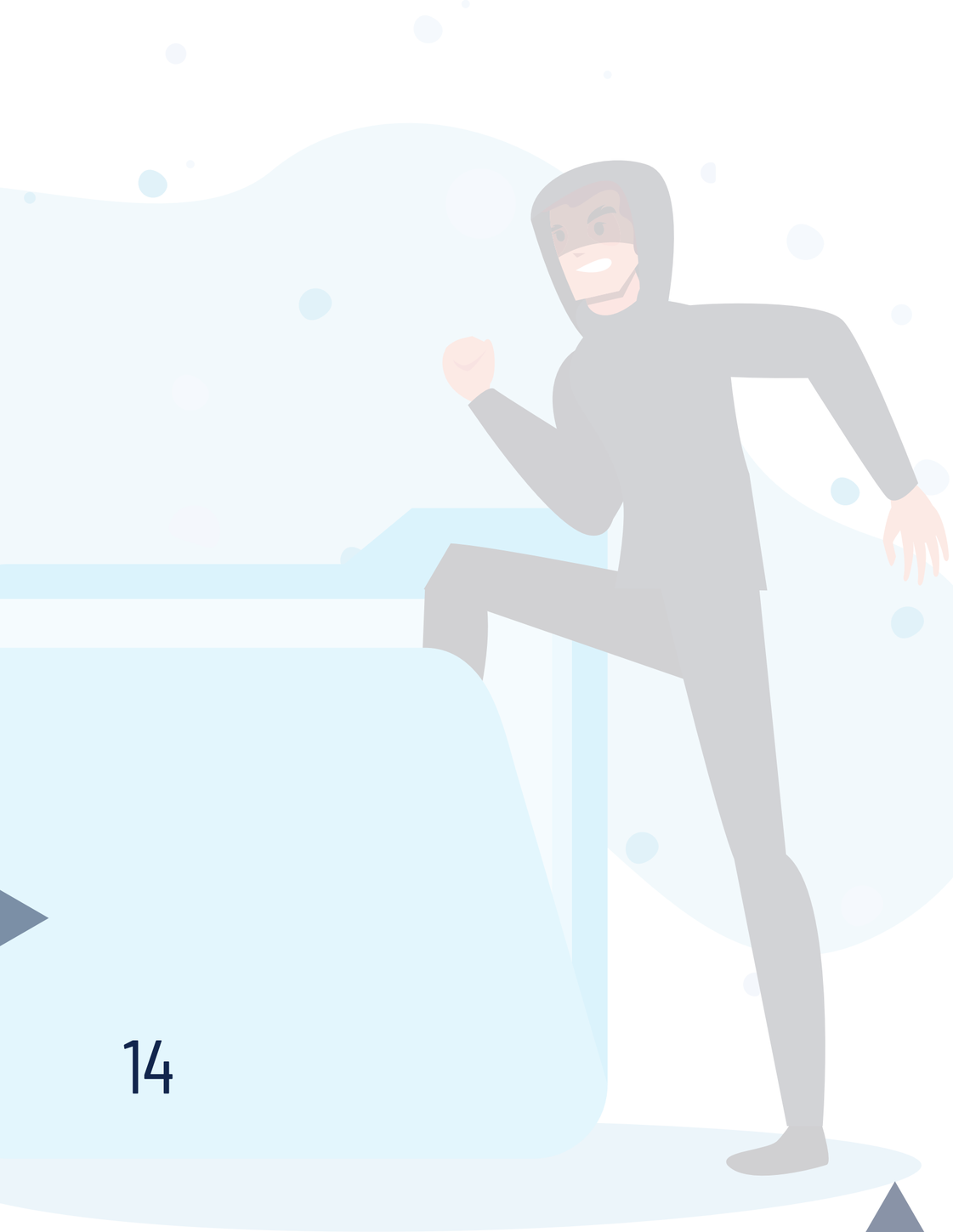
Sabe-se que o Distrito Federal larga na frente perante os demais entes Federativos quando propõe o projeto de lei nº 1.133/2020, que "dispõe sobre garantias de liberdade individual e proteção de dados pessoais no monitoramento inteligente para combate a pandemias, e dá outras providências", tendo como base a própria Lei Geral de Proteção de Dados.

E também, o Supremo Tribunal Federal (STF) posicionou-se pela inconstitucionalidade da MP 954/2020, que trata do compartilhamento de dados de usuários dos serviços de telecomunicação em face de a OAB e partidos políticos terem apontado sua inconstitucionalidade – pela OAB (ADI 6387), pelo PSDB (ADI 6388), pelo PSB (ADI 6389), pelo PSOL (ADI 6390) e pelo PCB (ADI 6393). Mais uma razão que motiva a criação da Comissão.

Ainda, a PEC 17/2019 , texto que "acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria" é outro fator primordial para que as advogadas e os advogados tenham uma especificidade para atuação profissional na temática.

Há muitos pontos a serem tratados no Direito Comparado via GDPR, CCPA, HIPPA, PIPEDA e várias outras legislações que ratificam a necessidade de um aprofundamento na privacidade e na proteção de dados pessoais.

Assim, temos o orgulho de ser uma das poucas Seccionais, em todo o país, que possui uma Comissão com a temática sobre privacidade e proteção de dados, que já conta com quase cinquenta membros dispostos a trabalhar com assunto que nos parece ser muito novo, mas que é muito mais antigo do que se pensa: data de 1980!

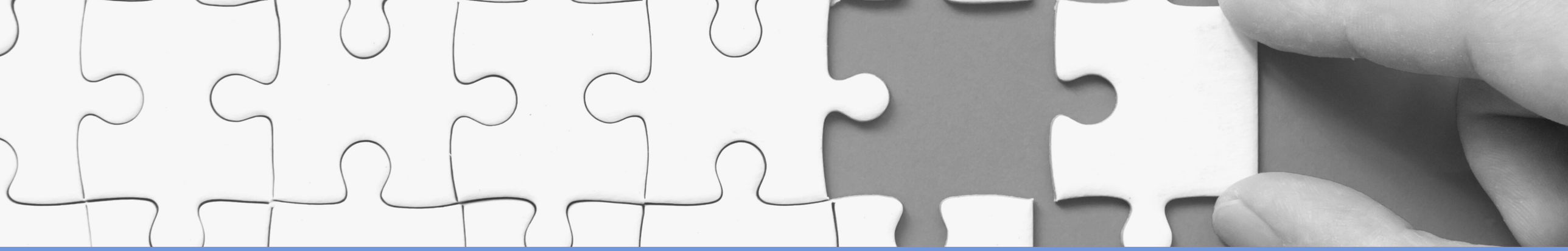


Destacamos trecho, do original em inglês, desse fascinante artigo intitulado “The Right to Privacy” publicado pela Harvard Review Magazine:

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right “to be let alone” Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the house-tops.” For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer. The alleged facts of a somewhat notorious case brought before an inferior tribunal in New York a few months ago, directly involved the consideration of the right of circulating portraits ; and the question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration."

A LGPD veio para mudar a forma como lidamos com os nossos dados, e nós, da Comissão de Privacidade e Proteção de Dados Pessoais, temos a importante missão de auxiliar a todos os profissionais advogados nas suas principais demandas do dia a dia que dizem respeito ao assunto.

Adriana Antunes Winkler
Presidente da Comissão de Privacidade e Proteção de Dados Pessoais da OAB/DF

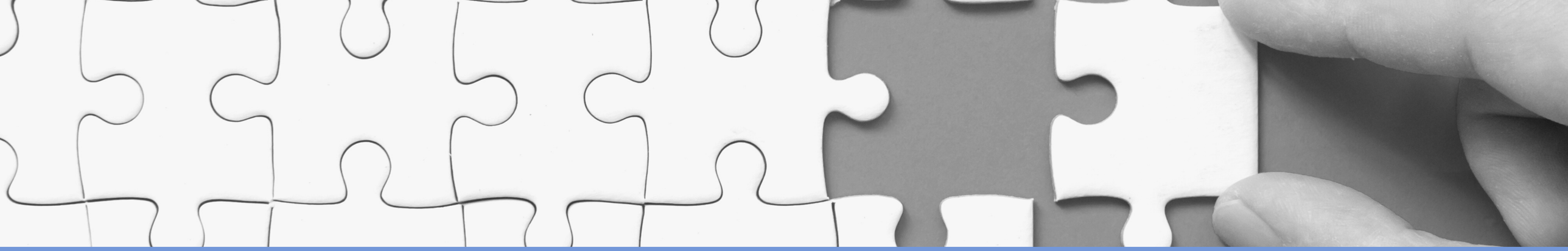


c. Sobre a Comissão de *Compliance*

A Comissão de *Compliance* da OAB/DF, na gestão 2019 a 2021, tem a missão, enquanto parte de uma instituição respeitada e séria, referência em boas práticas e que cobra atitudes éticas e probas de nossos governantes, de difundir a cultura da integridade no âmbito da sociedade organizada por meio da ampliação dos debates sobre a legislação aplicada.

Entendemos que a busca por um país mais justo, transparente e íntegro é dever de todos e, como peça essencial à administração da justiça, a advocacia não pode se eximir do debate. Para tanto, temos, dentro de nossa comissão, subcomissões temáticas compostas por especialistas que se aprofundam nos assuntos relevantes para toda a sociedade como Compliance Ambiental, Trabalhista e Digital (Lei Geral de Proteção de Dados).

O escopo de nosso trabalho percorre objetivos pioneiros nesta Seccional, como a implementação do nosso próprio Programa de *Compliance*. É um projeto ambicioso, em andamento, para dar o exemplo e incentivar a cultura da integridade em nossa sociedade. É preciso sair do âmbito teórico e partir para a prática. Nesse sentido, alçamos caminhar cada vez mais em busca das boas atitudes de governança e de eficiência.



Ademais, lançamos, no ano passado, o Portal da Transparência da OAB/DF. Mais uma realização da Comissão de *Compliance* com a Diretoria desta Seccional, que reafirma o comprometimento desta gestão com a integridade, *accountability*, probidade, ética e legalidade. Por meio do portal, a advocacia e a sociedade civil podem acessar informações contábeis e financeiras desta instituição. Isso porque, apesar de não receber recursos do governo, a OAB/DF entende que não é possível cobrar lisura no uso do dinheiro público sem dar, dentro de sua própria casa, bom exemplo de governança.

Além dos projetos citados, temos como objetivo contribuir com discussões relevantes como a ampliação para o âmbito civil e administrativo das Investigações Defensivas, amparadas pelo Provimento nº 188/2018 do Conselho Federal da OAB, por entender que é prerrogativa da advogada ou do advogado trabalhar em busca do contraditório e da ampla defesa em sentido lato sensu e em igualdade de condições com outras instituições democráticas.

Aproveitamos a publicação deste Guia para confirmar nosso compromisso com os anseios da advocacia e da própria sociedade em busca do verdadeiro Estado Democrático de Direito.

Inácio Bento de Loyola Alencastro
Presidente da Comissão de Compliance da OAB/DF

2. Como surgiu a LGPD?

Breve contexto histórico sobre a Lei 13.709/2018

Embora pareça um tema novo, a proteção de dados e da privacidade de usuários é debatido há décadas. Ganhou notabilidade nos últimos anos devido ao aumento exponencial da utilização da internet.

No período pós-Segunda Guerra Mundial, as melhores definições do conceito vêm com a Declaração Universal dos Direitos Humanos e com o Pacto da Nações Unidas sobre Direitos Civis e, posteriormente, com a Convenção Europeia dos Direitos do Homem, que estabelece que "qualquer pessoa tem direito ao respeito à sua vida privada e familiar, ao seu domicílio e à sua correspondência". Este mesmo objetivo é disposto em cartas constitucionais de vários países.

Nesse tema, a Europa tem protagonismo porque, historicamente, governos autoritários já faziam coleta e processamento de dados da população. As novas tecnologias da informação e de comunicação aceleraram essa ação.

A Alemanha criou a primeira lei que oficialmente tratou sobre proteção de dados pessoais, em 1970, e foi acompanhada por diversos países como França, Noruega, Suécia e Áustria que, seguindo a tendência, produziram legislações sobre o tema.

Depois, o Parlamento Europeu criou a Diretiva 95/46/CE, relativa à proteção das pessoas no que diz respeito ao tratamento dos dados pessoais e à circulação de dados. Em 2016, foi publicado o Regulamento Geral de Proteção de Dados da União Europeia – RGPD (ou, do inglês GDPR, como é mais conhecido), que serviu como base para a legislação brasileira.

A entrada em vigor do GDPR, em 2018, com o objetivo de garantir a sua eficácia devido ao ambiente globalizado das instituições, ampliou a sua extensão da territorialidade, para alcançar agentes de tratamento estrangeiros que ofereçam bens ou serviços e/ou realizem o monitoramento do comportamento de pessoas que estejam na União Europeia. Além disso, proíbe a transferência internacional de dados pessoais para países que não possuem a adequação e segurança necessárias. Esses dois aspectos contribuíram, significativamente, para a nossa Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018). É uma legislação de proteção de dados pessoais, com forte influência da Constituição Federal de 1988 e das legislações infraconstitucionais que, de alguma forma, tratam sobre a temática.

A norma brasileira regulamenta as atividades de tratamento de dados pessoais, estabelece direitos e boas práticas para a garantia de privacidade dos titulares, cria a Autoridade Nacional de Proteção de Dados. Também, prevê as penalidades que serão aplicadas, caso ocorram violações e descumprimento da legislação.

3. Conceitos Básicos

DADO PESSOAL

Compreende-se por
toda informação relacionada à pessoa natural, que possa identificá-la ou torná-la passível de identificação, tal como nome, CPF, data de nascimento, filiação, naturalização, endereço, profissão, estado civil etc.

DADO PESSOAL SENSÍVEL

Trata-se de um dado capaz de ensejar discriminações e preconceitos. Recebe maior proteção legal. Citamos como exemplo: origem racial ou étnica, convicções religiosas, políticas, sexuais ou filosóficas da pessoa natural, suas características genéticas etc.

DADO ANONIMIZADO

É aquele que, mediante a utilização de meios técnicos razoáveis e disponíveis, não é considerado um "Dado Pessoal" pela LGPD por não possuir mais a característica da "possibilidade de identificação".
São anonimizados, via de regra, os dados utilizados em pesquisas acadêmicas, por exemplo, onde indica-se apenas uma categoria de pessoas: "70% de homens da região sudeste".

TITULAR DE DADOS

É a pessoa física
(ou natural) a quem os dados pessoais, tratados, referem-se.

CONTROLADOR

É um agente de tratamento e, portanto, o responsável pelas determinações referentes ao tratamento dos dados. É a pessoa física ou jurídica, de direito público ou privado, que determina e, dessa forma, exerce o controle do tratamento dos dados pessoais. É uma espécie de "Agente de Tratamento Indireto".

OPERADOR

É, também um agente de tratamento, mas, ao contrário do controlador, é um "Agente de Tratamento Direto", pois é ele quem realiza, **de fato**, todo o tratamento dos dados pessoais, em nome do controlador.

ENCARREGADO

O encarregado não é um agente de tratamento, mas uma figura imprescindível ao lidar com os dados pessoais. A LGPD exige a divulgação e publicação dos contatos do encarregado por tratar-se de pessoa física ou jurídica, indicada pelo controlador e pelo operador, com a finalidade de fazer a interligação entre o controlador e o titular dos dados, bem como entre estes e a Autoridade Nacional de Dados (ANPD). Ele funciona, de acordo com o texto legal, como um canal de comunicação.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

É um órgão da Administração Pública Direta. Tem como atribuições a realização da fiscalização do cumprimento da Lei nº 13.709/18 e um papel educador em relação à proteção de dados pessoais e à privacidade. Suas atribuições e composição estão elencados no Capítulo IX, seção I da referida Lei, onde se destacam no seu art.55-J, entre outras atividades, zelar pela proteção dos dados pessoais, nos termos da legislação (inciso I); elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (inciso III) e fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso (inciso IV).

A ANPD é responsável por deliberar, na esfera administrativa e em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos. Desta forma é imprescindível que sua composição e seus membros possuam conhecimentos técnicos que permitam que os operadores da Lei ou afetados por ela se sintam seguros quanto ao respaldo técnico de sua aplicação.

TRATAMENTO DE DADOS

É qualquer operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

MAPEAMENTO DE DADOS

É o documento que indica quais os caminhos percorridos pelo dado pessoal dentro da empresa, incluindo os processos e os procedimentos pelos quais esse dado foi submetido

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS

Instrumento de responsabilidade do controlador, por meio do qual, em qualquer operação que envolva o tratamento de dados pessoais que possa gerar riscos às liberdades civis e aos direitos fundamentais, realizará a descrição dos processos para mitigação de riscos e de responsabilidades.

TRANSFERÊNCIA INTERNACIONAL DE DADOS

Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro. O conceito básico de transferência é o ato ou efeito de transferir ou de ser transferido e, nesse caso, amplia-se quando a transferência está relacionada a uma informação (dado). Transferir dados
em sua essência significa transferir informações. Os limites desta transferência passam a extrapolar o território nacional, pois são destinados a países ou organismos internacionais. A transferência internacional de dados está descrita no Capítulo V, em seus artigos 33 a 36 da LGPD e não limitam o meio escolhido para esta transmissão.

4. Princípios da Proteção de Dados Pessoais

O art. 1º da Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece a proteção dos direitos fundamentais de liberdade, da privacidade e do livre desenvolvimento da personalidade da pessoa natural.

A fim de cumprir os objetivos acima dispostos, o art. 6º da referida Lei elencou princípios que deverão guiar a atividade de tratamento de dados pessoais, de modo a impor limitações ao seu exercício, bem como assegurar ao titular desses dados uma série de direitos, dentre os quais destacam-se: i) a confirmação da existência de tratamento; ii) acesso aos dados; iii) correção de dados incompletos, inexatos ou desatualizados, iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei; v) portabilidade dos dados a outro fornecedor de serviço ou produto; e vi) eliminação dos dados pessoais.

A convergência estabelecida em âmbito internacional acerca dos princípios que devem nortear a atividade de tratamento de dados sugere a relevância dessas normas para a efetivação dos direitos de seus titulares.

BOA-FÉ

O primeiro princípio mencionado no art. 6º da LGPD e que serve como norte para toda e qualquer atividade de tratamento de dados pessoais é o princípio da boa-fé. Portanto, ao realizar o tratamento de dados, devem o controlador e o operador (agentes de tratamento) observar a relação de confiança estabelecida com os titulares de dados pessoais, no intuito de atender à legítima expectativa neles criada a partir das informações que lhes foram fornecidas.

FINALIDADE

As operações de tratamento de dados pessoais devem ser realizadas em consonância com a finalidade informada ao titular dos dados no momento de sua coleta. Por meio do princípio da finalidade, definem-se, pois, quais são os limites impostos às operações de tratamento.

Assim, segundo o legislador ordinário, a realização do tratamento de dados deve ser guiada por propósitos legítimos, específicos, explícitos e informados ao titular, não sendo possível a realização de tratamento de dados posterior que se revele incompatível com essa finalidade.

ADEQUAÇÃO

O terceiro princípio ao qual a Lei faz referência tem relação direta com o princípio anteriormente citado e diz respeito à compatibilidade que deve existir entre o tratamento dos dados pessoais e as finalidades informadas ao titular em momento anterior à sua execução.

Analisando-se a finalidade informada ao titular quando da coleta de seus dados pessoais, será possível verificar se o uso daqueles dados afigura se adequado ao contexto do tratamento.

NECESSIDADE

Dispõe o art. 6º, inc. III, da LGPD, que o tratamento de dados pessoais deve se limitar ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação a tais finalidades.

Pretende o legislador, por meio do referido dispositivo, estabelecer severa limitação à coleta de dados pessoais que não sejam estritamente necessários às finalidades informadas ao titular para justificar as operações de tratamento e, em última análise, resguardar sua privacidade, intimidade, honra e imagem.

O princípio da necessidade foi contemplado, ainda, nos arts. 10, §1º, 16 e 18, inc. VI, que estabelecem hipóteses de eliminação de dados pessoais quando a sua manutenção não mais se justifique.

LIVRE ACESSO

Conforme mencionado anteriormente, a LGPD (art.18) confere aos titulares de dados pessoais uma série de direitos sobre os dados submetidos a operações de tratamento. A relevância do princípio do livre acesso é evidenciada por sua imprescindibilidade à efetiva garantia desses direitos.

O princípio do livre acesso assegura aos titulares de dados pessoais, por exemplo, o direito de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais, o que lhes permitirá confirmar a existência de tratamento, acessar os dados tratados e requerer a sua correção, atualização, anonimização, eliminação, portabilidade.

QUALIDADE DOS DADOS

O princípio em análise pretende assegurar clareza, ao titular dos dados pessoais, acerca da necessidade das operações de tratamento, bem como garantir que os dados tratados sejam exatos, atualizados e relevantes para o cumprimento da finalidade de seu tratamento.
Correlaciona-se, portanto, ao princípio do livre acesso, o qual constitui condição para que o titular possa assegurar a qualidade de seus dados.

TRANSPARÊNCIA

Um dos princípios mais importantes da LGPD é o princípio da transparência, também denominado de princípio da publicidade, o qual é responsável por garantir o livre exercício dos direitos fundamentais contemplados em seu texto.
Impõe o princípio em comento que a existência de bancos de dados seja de conhecimento público, bem como que as informações atinentes às operações de tratamento de dados sejam fornecidas de forma clara e precisa ao titular, com o intuito de que ele possa fiscalizar o cumprimento da legislação e tomar decisões que lhe assegurem a efetividade de seus direitos

SEGURANÇA

O princípio da segurança exige que as operações de tratamento, bem como os bancos de dados pessoais sejam seguros e possuam proteção contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Portanto, estabelece o legislador que, no decorrer das operações de tratamento, sejam utilizadas medidas técnicas e administrativas aptas a proteger
os dados pessoais, medidas essas que envolvem o uso da tecnologia e treinamento humano.

PREVENÇÃO

Enquanto o princípio da segurança objetiva a adoção de medidas técnicas e administrativas para a proteção de dados pessoais contra situações ilícitas, o princípio da prevenção visa à adoção de medidas para prevenir a ocorrência de danos ao titular em virtude do referido tratamento.

A fim de evitar a prática de situações ilícitas ou a ocorrência de danos aos titulares de dados, o legislador ordinário destacou a necessidade de que os agentes de tratamento (ou de qualquer outra pessoa que intervenha na relação) observem regras de boas práticas e de governança em privacidade.

5. Direitos do Titular

A Lei Geral de Proteção de Dados (LGPD) tutela a autodeterminação informativa, conferindo, ao titular dos dados um protagonismo nas questões relacionadas ao tratamento de suas informações pessoais.

Ou seja, deve-se permitir, ao titular dos dados, um real poder de controle sobre a destinação das informações colhidas.

Neste contexto, advogados autônomos e sociedades de advocacia, na condição de agentes de tratamento de dados pessoais, precisam estar atentos aos ditames da nova legislação de proteção de dados, para assegurar os direitos fundamentais de liberdade, de intimidade e de privacidade de seus clientes e, no caso das sociedades de advocacia, também, de seus colaboradores.

A LGPD traz um capítulo inteiro dedicado aos direitos dos titulares dos dados, restando expresso que poderão ser exercidos mediante requerimento expresso, do titular ou de representante legalmente constituído, a agente de tratamento.

É recomendável o estabelecimento, por advogados autônomos e por sociedades de advocacia, de canal de atendimento às solicitações dos titulares dos dados, podendo ser por e-mail, telefone, chat e outras vias. A partir da vigência da Lei, a indicação deste canal deverá constar nos Contratos e nas Políticas de Proteção de Dados.

De igual forma, advogados autônomos e sociedades de advocacia ainda deverão estabelecer mecanismos prévios de conferência da identidade do titular para evitar acessos indevidos aos dados pessoais e procedimentos de atendimento aos direitos dos titulares.

Nos termos do art. 18, o titular poderá exigir, dentre outros direitos, a confirmação, o acesso, a correção, a anonimização, o bloqueio e a portabilidade dos seus dados pessoais, conforme a seguir:

CONFIRMAÇÃO DA EXISTÊNCIA DE TRATAMENTO E ACESSO AOS DADOS PESSOAIS

Os direitos de confirmação da existência de tratamento e de livre acesso às informações pessoais deverão ser garantidos ao titular dos dados. A confirmação de existência ou o acesso aos dados pessoais serão providenciados pelo controlador: Os dados pessoais deverão ser armazenados em formato que favoreça o exercício do direito de acesso e poderão ser fornecidos, a critério do titular, por meio eletrônico ou sob forma impressa.

CORREÇÃO DE DADOS PESSOAIS

Os titulares dos dados poderão exigir a correção de dados incompletos, inexatos ou desatualizados.

INFORMAÇÃO DE COMPARTILHAMENTO DOS DADOS

Os titulares poderão exigir informações das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados pessoais.

ELIMINAÇÃO OU BLOQUEIO E ANONIMIZAÇÃO DE DADOS PESSOAIS

Os dados pessoais deverão ser eliminados após o término do tratamento, sendo autorizada a conservação para o cumprimento de obrigação legal ou regulatória.

Assim, os titulares poderão exigir a eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD.

Nos termos desta Lei, os dados pessoais serão, sempre que possível, anonimizados, de forma a não permitir a identificação do titular.

Ainda, o responsável pela eliminação ou bloqueio e pela anonimização deverá informar, de forma imediata, os demais agentes com os quais tenha realizado uso compartilhado de dados pessoais, para que repitam idêntico procedimento, exceto nos casos em que a comunicação seja comprovadamente impossível ou implique esforço desproporcional.

PORTABILIDADE DOS DADOS

Os titulares poderão receber os seus dados pessoais fornecidos a um controlador, inclusive em formato eletrônico e interoperável, a fim de que sejam transmitidos a outro fornecedor de serviço ou produto.

Registre-se que o direito de portabilidade dos dados pessoais dependerá de regulamentação por parte da Autoridade Nacional de Proteção de Dados (ANPD).

REVOGAÇÃO DO CONSENTIMENTO

Os titulares poderão revogar o consentimento para o tratamento de seus dados pessoais, a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado.

Importante ressaltar que o controlador poderá continuar o tratamento dos dados pessoais obtidos mediante consentimento, anteriormente ao pedido de revogação, até que a finalidade do tratamento seja alcançada ou nas demais hipóteses previstas em Lei.

INFORMAÇÃO SOBRE A POSSIBILIDADE DE NÃO FORNECER CONSENTIMENTO

Os titulares também poderão exigir informações sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

RECLAMAÇÃO PERANTE A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Os titulares poderão peticionar, em relação aos seus dados pessoais, contra o controlador, perante a Autoridade Nacional de Proteção de Dados (ANPD) e, também, junto aos organismos de defesa do consumidor.

OPOSIÇÃO AO TRATAMENTO DE DADOS

Os titulares dos dados poderão se opor a quaisquer tratamentos e informações que não estejam em conformidade com a Lei, bem como a decisões automatizadas que afetem seus interesses, como aquelas destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (*profiling*).

É de responsabilidade do controlador fornecer informações claras e objetivas sobre os critérios e os procedimentos adotados para a decisão automatizada, observados os segredos comercial e industrial. Em caso de não oferecimento das informações, sob a alegação de segredos comercial e industrial, a Autoridade Nacional de Proteção de Dados (ANPD) poderá realizar uma auditoria, para verificar eventuais aspectos discriminatórios do tratamento automatizado.

6. Bases Legais de Tratamento de Dados

O art. 7º da Lei Geral de Proteção de Dados (LGPD) especifica as dez bases legais que legitimam o tratamento dos dados pessoais. Cabe ressaltar que as bases legais são taxativas, ou seja, nenhuma outra hipótese poderá ser utilizada senão as dispostas no referido artigo.

Deve haver ao menos UM enquadramento em uma base legal para que o tratamento seja considerado legitimo, sendo, assim, possível a existência de duas ou mais bases legais para o mesmo tratamento.

CONSENTIMENTO

Apesar de o consentimento ser divulgado como a principal base legal é, na verdade, apenas uma das dez bases legais existentes. As outras nove bases independem do consentimento do titular para que sejam consideradas válidas.

O consentimento trata da vontade do titular, que para ser considerada válida precisa ter sua manifestação **livre, informada e inequívoca**, para uma finalidade.

A LGPD exige que o consentimento seja fornecido por escrito ou por outro meio que demonstre a manifestação inequívoca de vontade do titular.

Quando o consentimento se der por escrito, ele deverá constar em uma cláusula destacada das demais cláusulas contratuais, que não pode ser genérica, justamente para que seja comprovado que aquele consentimento foi dado para uma finalidade específica de tratamento.

O ônus da prova do consentimento caberá ao controlador, sendo vedado o vício de consentimento.

O consentimento pode ser revogado a qualquer tempo, mediante a manifestação expressa do titular. Por esse motivo, recomenda-se que a coleta de dados se dê com base no consentimento somente de forma residual, caso não seja possível o tratamento de dados através de outra das bases legais.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA

O controlador poderá realizar o tratamento dos dados pessoais dos titulares sempre que existir uma determinação legal ou regulatória que justifique ou determine o seu tratamento, dispensando assim o seu consentimento. Neste caso, o tratamento é justificado pela exigência de outras leis ou decretos, evitando que a LGPD entre em conflito com outras normas vigentes.

EXECUÇÃO DE POLÍTICAS PÚBLICAS

Quando o tratamento dos dados pessoais é resguardado pelo interesse público ou por necessidade de uma autoridade oficial, que passa a ser o controlador do dado pessoal.

Essa hipótese também dispensa o consentimento prévio do titular. Entretanto, sempre que a administração pública efetuar o tratamento dos dados pessoais do titular no exercício de suas competências legais, deverá informá-lo sobre a finalidade do tratamento e como os dados serão tratados.

ESTUDOS EM ÓRGÃOS DE PESQUISA

Dados pessoais poderão ser tratados com finalidade de pesquisa, por órgãos oficialmente credenciados. Sempre que possível os dados deverão ser anonimizados, para garantir a privacidade dos titulares ao máximo.

EXECUÇÃO DE CONTRATO

Aqui, os dados dos titulares podem ser tratados em duas situações: a) para que sejam cumpridas obrigações contratuais em que o titular figura como parte; b) quando se refere a atos preliminares do contrato, fase pré-contratual.
Neste caso, o tratamento de dados dar-se-á a pedido do próprio titular dos dados. Embora assemelhe-se ao consentimento, não poderá ser revogado a qualquer momento, estando o controlador resguardado para que possa manter os dados durante a vigência do contrato.

EXERCÍCIO REGULAR DE DIREITOS

O exercício regular de direitos é uma base legal que pode ser utilizada pelo controlador para o exercício regular de direitos em processo judicial, administrativo ou arbitral.
Essa hipótese visa resguardar os preceitos constitucionais de ampla defesa e do contraditório, uma vez que opor-se a este tipo de tratamento de dados seria cercear o direito de defesa da outra parte, impossibilitando a produção de provas.

PROTEÇÃO À VIDA

Justifica-se o tratamento para preservação da vida ou da incolumidade física do titular dos dados ou de terceiros.
O objetivo é garantir a proteção do bem maior da pessoa natural, desde que devidamente comprovada essa necessidade e demonstrada a finalidade do tratamento dos dados nesta situação.
Esta base legal autorizadora para o tratamento dos dados é tão específica que dispensa o consentimento do titular, inclusive em casos de dados pessoais sensíveis conforme o art. 11, II, e da LGPD.

TUTELA DA SAÚDE

Seguindo o mesmo entendimento da base legal de proteção à vida, a LGPD também autoriza o tratamento de dados para a tutela da saúde, desde que seja realizado por profissionais de saúde, serviços de saúde ou autoridades sanitárias.

Da mesma forma que a proteção à vida, esta também é uma base legal que dispensa o consentimento do titular, inclusive para dados sensíveis, caso sejam indispensáveis para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

PROTEÇÃO DO CRÉDITO

Esta base legal de proteção ao crédito tem como objetivo evitar que os titulares possam utilizar-se da legislação para ocultar-se de dívidas contraídas.

Sendo assim, para facilitar a aprovação de crédito, reduzir os riscos da transação, é possível que dados pessoais sejam consultados avaliando o perfil de crédito do titular com a devida observância da legislação pertinente.

LEGÍTIMO INTERESSE

O legítimo interesse é a base legal mais flexível e, também, com maior grau de subjetividade, pois não há uma definição clara sobre o que seria o "legitimo interesse". Acredita-se que esta deverá ser a base legal que gerará maior discussão no futuro, dado o vasto campo interpretativo do termo "legítimo interesse".

Assim, com o objetivo de tentar prestar os esclarecimentos iniciais, o legislador, ao redigir o artigo 10º, optou por incluir os principais requisitos para o exercício do legítimo interesse.

O controlador somente poderá utilizar-se desta base legal para finalidades legítimas, com situações concretas para apoio e promoção de suas atividades e proteção do exercício regular de direitos do titular ou serviços que o beneficiem, respeitadas as legítimas expectativas e os direitos e liberdades fundamentais e observados os princípios da necessidade e da transparência. Dessa forma, o controlador, ao optar por essa base legal, assumirá o risco pelo tratamento dos dados dos titulares. Por este motivo, deverá realizar um teste de ponderação para fundamentar sua decisão, além de implementar as medidas necessárias para garantir o seu uso adequado e mitigar os possíveis riscos aos direitos dos titulares.

7. *Compliance* e Proteção de Dados

A entrada em vigor da Lei Geral de Proteção de Dados Pessoa(Lei nº 13.709/2018), no Brasil, afetará em cheio o Departamento de *Compliance* das empresas. Estar em Compliance é atuar em conformidade com as leis e normas a que a organização está exposta, sejam elas de alcance geral ou específico de um determinado setor. Ao contrário do que se acredita, um bom Programa de *Compliance* vai além do combate à fraude e à corrupção e leva em consideração diversos aspectos legais: tributário, trabalhista, ambiental, criminal e até mesmo digital.

É sabido que nem todas as organizações possuem as mesmas preocupações e estão expostas aos mesmos riscos e, por essa razão, um Programa de *Compliance* efetivo deve ser customizado às necessidades de cada empresa. O escopo do trabalho de Departamento de *Compliance* será definido durante o mapeamento e análise de risco, quando as vulnerabilidades da empresa são trazidas à tona e as soluções para mitigar tais fraquezas começam a ser pensadas e apresentadas. Nesse momento, deverá surgir a preocupação em atender às determinações da LGPD que, apesar de parecer algo distante e que atingirá apenas grandes corporações, tem uma abrangência espantosa, incluindo pessoas físicas, bancos de dados públicos e privados, além de pequenas, médias e grandes empresas de todos os ramos de atuação.

Para se ter uma ideia do quão amplo é o alcance da LGPD, vamos pensar um pouco. Em qual ato da vida civil, desde o mais simples, não é preciso coletar dados? Onde esses dados ficam guardados? Quem tem acesso a eles? No dia a dia, deixamos nosso "rastro" o tempo todo em reservas de passagens aéreas, notas fiscais de restaurantes ou de supermercados, consultas e exames médicos, extratos bancários e muito mais. Toda essa rede de empresas e organizações terá que, em maior ou menor grau, adequar-se à LGPD, respeitando a privacidade dos dados e solicitando apenas os fundamentais, armazenando de forma adequada a evitar vazamentos e agindo proativamente em caso de desvios de conduta ou falhas.

Para essa adequação, será preciso ter nos quadros da empresa ou contratar um prestador de serviço terceirizado que entenda a Lei e conduza todo o processo: ele será chamado de *Data Protection Officer* (DPO/Encarregado de Dados). Esse profissional deve conhecer *Compliance*, risco, governança e proteção de dados e, não raro, em empresas de menor porte, a mesma pessoa acumulará as duas funções: encarregar-se pelo *Compliance* e pela proteção de dados na organização. Nesse sentido, é preciso pensar em dados da forma mais ampla possível, englobando informações sobre clientes, fornecedores e até mesmo dos colaboradores da empresa; ou seja, públicos externo e interno. Dados sensíveis como opção religiosa, preferência sexual e doenças graves e infecciosas requerem maior cuidado. Vale lembrar que a adequação à LGPD deve ser feita não só para a segurança de dados coletados a partir da entrada em vigor da Lei, mas também para os que já se encontram armazenados.

E onde o *Compliance* entra nisso tudo? Como guardião das boas práticas, cabe ao *Compliance* garantir o atendimento efetivo às exigências legais, incluindo as políticas de proteção de dados não somente no papel, como no dia a dia dos colaboradores. Será preciso rever procedimentos, mudar hábitos e treinar a equipe, explicando a Lei, suas implicações e impactos. Garantir a cultura da integridade e a internalização das normas está no DNA do Departamento de *Compliance* e deve estender-se a toda a organização, cuidando de prevenir descumprimentos e de mitigá-los quando porventura venham a ocorrer. Isso porque, além das punições pecuniárias severas impostas pela LGPD, deve haver constante preocupação com a reputação da companhia, considerada hoje o maior ativo de todos e a responsável pela longevidade ou não de uma corporação.

Nitidamente a atuação do *Compliance* estará ligada à do DPO (seja ele ou não a mesma pessoa). Isso porque, desde o primeiro momento, as áreas terão que atuar de forma integrada, e com apoio da tecnologia, na análise de quantos e quais dados a empresa detêm; quem acessa; quem armazena esses dados e na definição de como melhor proteger tais informações. Seguem abaixo detalhados alguns passos fundamentais:

PASSOS FUNDAMENTAIS

1

DEFINIR UM AGENTE DE PROTEÇÃO DE DADOS

Seja ele um colaborador interno ou consultor externo, é preciso designar alguém para o cargo, com o objetivo de adotar medidas de segurança, capazes de proteger os dados pessoais de acessos não autorizados, vazamentos e de situações acidentais ou ilícitas de destruição, perda alteração, comunicação ou qualquer forma de tratamento inadequado.

2

CONHECER E MAPEAR OS DADOS

Muitas vezes a empresa pode achar que não coleta dados relevantes, mas, em uma análise mais profunda, acaba por perceber que até mesmo nome e CPF em mãos erradas podem gerar dor de cabeça e prejuízo. Com um mapa dos dados coletados e armazenados, chegou a hora de avaliar quem visualiza tais informações e como são usadas. Muitas vezes, o fluxo de acesso aos dados é extenso e perpassa quase todos os departamentos com propósitos distintos, como o marketing analisando potenciais clientes e o recursos humanos gerindo colaboradores, por exemplo. De posse dessas informações será possível criar uma matriz de risco.

3

GERENCIAR OS DADOS

Gerenciar os dados é dar acesso apenas a quem realmente precise e na medida exata da necessidade. Vale lembrar que a conformidade com a LGPD depende ainda de como terceiros cumprem a lei, ou seja, mesmo que os dados não fiquem fisicamente na empresa ela pode ser responsabilizada em caso de descumprimento. Fica estabelecido o caminho que os dados percorrem dentro da empresa, inclusive com a coleta do consentimento do dono das informações.

4

PROTEGER OS DADOS

Momento em que a tecnologia entra em cena, não apenas com uso da criptografia, mas no monitoramento e diligência constantes e numa reação rápida no caso de violação ou vazamento dos dados. É preciso combinar técnicas de segurança, soluções de *backup*, fluxo de trabalho padronizado e treinamento interno.

5

DOCUMENTAR

Diante da importância dada pela lei aos direitos do titular dos dados, podendo corrigir, apagar informações desnecessárias e revogar o consentimento à guarda a qualquer instante, as empresas precisam comprovar o atendimento às exigências, inclusive comunicando rapidamente ao cliente os eventuais casos de vazamento de informações.

6

CRIAR POLÍTICAS E CÓDIGOS

Momento de atualizar ou mesmo criar o Código de Conduta da empresa com vistas a proteger os dados pessoais. Posteriormente, é preciso criar ou atualizar a Política de Privacidade e de Gestão de Dados Pessoais da empresa, dando conhecimento a colaboradores, fornecedores e terceiros, inclusive com assinatura de ciência. Caso necessário, realizar aditivos nos contratos existentes com as novas cláusulas de segurança de dados. O mesmo vale para contratos com consumidores finais, que devem dar o aceite nos Termos de Uso e Política de Privacidade da empresa. Este deve trazer de forma clara a justificativa para a coleta de informações pessoais.

7

REAVALIAR E MELHORAR SEMPRE

Traço marcante do Compliance que deve ser levado à proteção de dados é o **monitoramento contínuo**, com vistas a melhorar processos e corrigir falhas.

Em função da importância da proteção dos dados pessoais, tendo em vista salvaguardar direitos fundamentais como a liberdade de expressão, de informação, de opinião e de comunicação e a inviolabilidade da intimidade, da honra e da imagem, fica claro o tamanho do desafio a ser vencido.

Levando-se em conta a adequação inicial e todos os ajustes necessários ao longo do tempo, é possível notar que a LGPD exigirá das empresas o dever de segurança, ética e responsabilidade com os dados pessoais para que se torne parte da missão e valores das organizações, gerando um aumento no nível de maturidade dos Programas de Compliance.

A soma de toda essa mudança só pode trazer para as organizações, parceiros, colaboradores e consumidores a segurança jurídica de um ambiente ético, transparente e de governança necessário para a realização de negócios.

8. Penalidades e Sanções

Todos os advogados autônomos e os escritórios de advocacia deverão observar a regularidade do tratamento dos dados pessoais, a concretização dos direitos dos titulares, a questão da segurança das informações, além de outras exigências da LGPD, sob pena de incidência de penalidades administrativas, que poderão ser aplicadas, a partir de agosto de 2021, pela Autoridade Nacional de Proteção de Dados (ANPD).

A LGPD, em seu art. 52, estabelece penalidades que podem ser, em última instância, bastante rigorosas:

Para a aplicação das sanções descritas serão considerados os parâmetros e os critérios estabelecidos na Lei, como, por exemplo, a gravidade e a natureza das infrações, os direitos pessoais afetados, a boa-fé do infrator, a vantagem econômica auferida pelo infrator e sua condição econômica, a reincidência, a cooperação do infrator, a adoção de mecanismos e procedimentos para minimizar os danos e a adoção de políticas de boas práticas e governança.

Ademais, as penalidades descritas não substituem a aplicação de sanções administrativas, civis ou penais previstas em legislação específica, conforme §2º do art. 52. A situação de não conformidade à Lei também poderá afetar a imagem e a reputação do profissional e/ou do escritório de advocacia.

9. Advocacia e LGPD: o que esperar

O objetivo primordial da LGPD é criar um cenário de segurança jurídica, mediante a padronização de normas e de práticas, no território brasileiro, para garantir a privacidade e a proteção dos dados pessoais do titular.

Esse importante marco legal chegou em um período de pandemia do coronavírus, marcado por inúmeros vazamentos de dados pessoais e por discussões sobre a vigência da Lei Geral de Proteção de Dados e a criação efetiva da Autoridade Nacional de Proteção de Dados (ANPD).

Diante do profundo impacto da legislação na sociedade e da transformação dos negócios, os advogados e os escritórios de advocacia terão que adotar diversas providências voltadas à adequação, para garantir a proteção dos dados de seus clientes, funcionários e fornecedores.

Por outro lado, também surgem novas oportunidade de trabalho e de parceria, visto a necessidade do mercado de contratar consultorias especializadas no assunto, buscar serviços de DPO/encarregado de dados, atuar no contencioso, entre outros.

Oportunidades

CONSULTORIA PARA EMPRESAS

De acordo com pesquisa realizada em 2019, pela Serasa Experian, 85% das empresas consultadas declararam que não estavam prontas para atender às exigências da LGPD.

A atual crise econômica, derivada do coronavírus, atrasou ou mesmo paralisou a implementação de muitos programas de LGPD nas empresas. Não obstante, definida a questão da vigência da lei, ainda em 2020, revelam-se urgentes e necessárias as medidas de Compliance.

Um programa de adequação à LGPD requer profunda análise jurídica, na revisão de contratos, na elaboração de políticas internas de privacidade e proteção de dados, na definição da base legal de tratamento de dados pessoais, entre outros. E mesmo nas etapas de inventário de dados e eventuais auditorias, o jurídico terá demandas estratégicas, conceituais e táticas, contínuas e robustas.

DEMANDAS JUDICIAIS

As penalidades administrativas, descritas na Lei, só poderão ser aplicadas a partir de 1º de agosto de 2021. Todavia, com a entrada imediata da LGPD, os titulares dos dados pessoais já poderão exercer seus direitos, sendo esperado um **aumento de demandas judiciais** correlatas, especialmente no que tange à responsabilização civil pelo tratamento irregular dos dados pessoais.

Na Europa, restou evidente o aumento das reclamações dos titulares às autoridades de proteção de dados, desde a vigência do GDPR em 2018.

MEIOS EXTRAJUDICIAS DE RESOLUÇÃO DE CONFLITOS

As condenações decorrentes de alguma irregularidade no tratamento de dados pessoais permitem o ressarcimento de eventuais danos patrimoniais e morais. Para dirimir esses conflitos, os meios não judiciais de resolução de controvérsias, como a negociação, a conciliação e a mediação, tornam-se uma medida adequada, por conferir celeridade ao caso.

De acordo com o Relatório Justiça em Números 2019, do Conselho Nacional de Justiça, havia, no final do ano de 2018, 78,7 milhões de ações judiciais em tramitação no Brasil. Tal cenário deixa claro que o Poder Judiciário não pode ser encarado como o único meio para solucionar os conflitos que surgirão com a entrada em vigor da LGPD.

Ademais, a própria legislação, em seu art. 52, §7º, preconiza que os vazamentos individuais ou os acessos não autorizados poderão ser objeto de conciliação direta entre controlador e titular, e, não sendo possível um acordo, o controlador estará sujeito à aplicação das penalidades administrativas.

10. Recomendações gerais para a Advocacia

Além do trabalho que será realizado pelos profissionais da área jurídica junto aos seus clientes, que envolverá longo processo de adequação à Lei por qualquer pessoa natural ou jurídica que realize operação de tratamento de dados (incluem-se, aqui, empresas, associações, sindicatos, profissionais autônomos, ONGs, Igrejas, dentre outros), os próprios escritórios de advocacia deverão estar em conformidade com a legislação para oferecer segurança e soluções adequadas.

Isso porque, consoante exposto nesta cartilha, os escritórios de advocacia se enquadram na categoria de agentes de tratamento (seja em relação aos dados de seus clientes, seja em relação aos dados de seus colaboradores), sujeitando-se, portanto, à LGPD e às suas penalidades. Essa é, inclusive, a ideia de *Compliance*, que significa "agir em conformidade" e pressupõe a coerência entre o que dizem os profissionais que atuam na área e as condutas por eles adotadas em seu cotidiano.

Em outras palavras, é imprescindível que o profissional com atuação na área "dê o exemplo" e assegure ao tratamento de dados de seu cliente a mesma segurança e sigilo que ele julgar ser imprescindível de ser adotada no âmbito desse último.

Quanto ao ponto, destaca-se que, apesar da nova roupagem dada pela LGPD à disciplina de tratamento de dados pessoais entre cliente e advogado, o Código de Ética e Disciplina da OAB já conta, há anos, com um capítulo específico (Capítulo III) que impõe aos advogados o **dever de sigilo profissional sobre informações** que venha a ter conhecimento em razão do exercício da profissão. Acrescenta-se, aos deveres já existentes, a obrigação que nos será imposta de prestar informações à Autoridade Nacional de Proteção de Dados (ANPD), a qual possui, inclusive, competência para fiscalizar e punir as hipóteses de descumprimento legal.

Ademais, deve-se salientar que a LGPD estabelece diversas hipóteses em que o tratamento de dados pessoais pelo advogado é condicionado ao consentimento do titular. Isso não exclui, entretanto, a possibilidade de o profissional da advocacia tratar dados pessoais independentemente da obtenção do consentimento em hipóteses específicas, tais como nos casos em que os dados se façam necessários para: i) a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular de dados; ii) o cumprimento de obrigação legal ou regulatória; iii) a proteção da vida ou incolumidade física do titular ou de terceiros ; e iv) exercício regular de direitos em processo judicial, administrativo ou arbitral.

Portanto, além de enquadrar as operações de tratamento nas bases legais anteriormente mencionadas, o advogado deverá adotar diversas providências de adequação, em que se incluem a revisão dos contratos de prestação de serviços e das políticas internas de coleta, armazenamento e descarte de dados, bem como a implementação de novas tecnologias e o treinamento de seu quadro de pessoal.

CAA DF

CAIXA DE ASSISTÊNCIA
DOS **ADVOGADOS** DO DF

60 ANOS

OAB

DISTRITO FEDERAL