Lei Geral de Proteção de Dados Pessoais: dos principais conceitos à implementação

Por Débora Minuncio[1], *Sandro Tomazele*[2]

Revisado por Carolina Vago[3]

1. Por que é preciso falar sobre proteção de dados pessoais?

O manuseio da informação alcança grande importância na sociedade digital, sendo o dado pessoal uma das mais importantes moedas de troca nos negócios modernos e que dita as regras da atual sociedade do consumo.

Inicialmente, dados são fatos não organizados que devem ser processados e, quando isso ocorre, originam a informação. Nas palavras de Laudon e Laudon (2004)[4] "dados são correntes de fatos brutos que representam eventos que estão ocorrendo nas organizações ou no ambiente físico, antes de terem sido organizados e arranjados de uma forma que as pessoas possam entendê-los e usá-los".

A informação, por sua vez, transmite significado e compreensão dentro de um determinado contexto, gerando conhecimento. Para Serra (2007)[5] a informação resulta do processamento, manipulação e organização de dados, assim representando uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano, animal ou máquina) que a recebe.

O acesso à informação e a esse conhecimento sobre a vida pessoal de um ser humano demandou a necessidade de direitos, garantias e proteção à privacidade desde 1890, com o artigo americano "*The Right to Privacy*", evoluindo com a Declaração Universal dos Direitos Humanos (1948) e o *Pacto de San José da Costa Rica* (1969).

Consequentemente, esse debate avançou também para a atenção imprescindível em relação aos dados pessoais, ou seja, as informações diretas e indiretas coletadas sobre uma pessoa física ou natural (titular de dados), como nome, sexo, CPF, RG, e-mail, endereço, filiação, profissão, data de nascimento, foto, placa de carro, currículo, carteira de trabalho, biometria, prontuário médico, hábitos de consumo, preferências, dentre outros.

---

[1] Advogada especialista em direito empresarial, digital, compliance e proteção de dados; Graduada em Direito pela Processus de Brasília/DF; Master of Laws (LLM) em Direito Empresarial pela FGV de Brasília/DF; Compliance Officer pela ABF; Certificação Privacy and Data Protection pela EXIN.

[2] Com 25 anos de experiência em TI, nas áreas pública e privada, é graduado em TI, Pós-Graduado em Redes de Computadores, Mestrando em Comércio Internacional pela Université d'Angers, França. Especialização em Advanced Project Management pela Positive Business Chair, Université de Paris, França. Professor convidado da Privacy Academy, Recife/PE. Professor do MBA em Privacidade de Dados (LGPD), Curitiba/PR. Foi membro dos comitês de governança das corporações e de gestão de riscos corporativos, ambos da ABNT – Associação Brasileira de Normas Técnicas. Coautor dos livros: LEI GERAL DE PROTEÇÃO DE DADOS - Estudos sobre um novo cenário de Governança Corporativa e LEI GERAL DE PROTEÇÃO DE DADOS NO SETOR PÚBLICO.

[3] Administradora especialista em melhoria de processos nos setores público e privado, com experiência em projetos de fusões e aquisições de empresas e padronização de operações e sinergia. Mestranda em Comércio Internacional pela Université d'Angers, na França, e especialização em Advanced Project Management pela Positive Business Chair, Université de Paris, França.

[4] LAUDON, K. C.; LAUDON, J. P. Sistemas de informação gerenciais: Administrando a empresa digital. São Paulo: Pearson Prentice Hall, 2004.

[5] SERRA, J. Paulo (2007). Manual de Teoria da Comunicação. Covilhã: Livros Labcom.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) implementou na Europa, entre 1970 e 1990, diversas diretrizes legislativas sobre dados pessoais, avançando para a conhecida Diretiva 95/46/CE da União Europeia, de 1995.

O *Safe Harbor*, de 2000, foi outro importante marco, sendo considerado um acordo entre Estados Unidos e Europa para facilitar a troca de informações e dados pessoais entres os dois continentes. Em 2015 foi revogado e renegociado em 2016 com o nome de *Privacy Shield*.

Ainda em 2016, a Europa adota o *General Data Protection Regulation* (GDPR) ou Regulamento Geral sobre a Proteção de Dados (RGPD), iniciado em 2012 e com entrada em vigência em 25 de maio de 2018.

No cenário brasileiro, desde 1993 o Código de Defesa do Consumidor (CDC) preceitua a detenção e a multa para quem impede ou dificulta o acesso a bancos de dados e cadastros de consumidores, e para aqueles que deixam de corrigir dados do consumidor e informações que sobre eles constem nesses locais.

Outras proteções relacionadas à informação, privacidade e regramento em ambiente digital vieram com a Lei de Acesso à Informação perante os órgãos públicos (Lei nº 12.527/2011), a Lei Carolina Dieckmann (Lei nº 12.737/2012), o Marco Civil da Internet (Lei nº 12.965/2014), a Lei do Usuário perante órgãos públicos (Lei nº 13.460/2017) e a Lei do Governo Digital (Lei nº 14.129/2021).

A lei cerne deste artigo é a Lei Geral de Proteção de Dados Pessoais, LGPD, Lei nº 13.709/2018, publicada em 14 de agosto de 2018, com entrada em vigência em 18 de setembro de 2020 e aplicação das sanções administrativas em 1º de agosto de 2021. Isso implica afirmar que desde setembro de 2020 todos devem estar em conformidade com ela.

Para compreender a relevância da proteção dos dados pessoais, recentemente foi promulgada a Emenda Constitucional 115, em 10 de fevereiro de 2022, colocando a proteção de dados pessoais no rol de direitos e garantias fundamentais e individuais da Constituição Federal (CF) e, portanto, como cláusula pétrea (que não pode ser alterado nem por emenda à CF).

Posto todo esse contexto, nota-se que o tema de proteção de dados pessoais vem evoluindo desde meados de 1970 e tem ganhado força política e econômica nos últimos 6 anos, alterando o modo como a sociedade lida com dados pessoais e dita padrões de consumo.

O mercado e as organizações movimentam a economia e seus lucros através dos dados pessoais dos cidadãos, analisando o mercado de compra, os padrões de seus consumidores, gerando e estudando estatísticas, vendendo informações e manipulando novos desejos e hábitos de consumo. Nas palavras de Andrew Lewis, retirada do filme "O Dilema das Redes" (disponível na Netflix e uma ótima recomendação para refletir sobre o tema): "Se você não está pagando pelo produto, você é o produto".

Diante deste cenário, um dos mais importantes princípios da LGPD é o da autodeterminação informativa. Significa garantir ao cidadão o controle dos seus próprios dados pessoais, ou seja, sempre que a escolha for possível, o titular pode decidir se os seus dados poderão ser coletados, tratados e compartilhados. É justamente onde reside a importância de legislações regulamentando os dados pessoais, impondo limites em seus tratamentos, aplicando sanções e penalidades em suas violações e garantindo direitos aos titulares, únicos donos dos dados pessoais.

2. Afinal, o que são dados pessoais?

É fato observável que as organizações tratam dados pessoais em suas operações rotineiras, em geral não importando seu segmento de atuação, nem sua constituição pública ou privada, tampouco seu tamanho ou seu volume de operações. Sejam dados pessoais relacionados a seus clientes, empregados, fornecedores, parceiros, acionistas ou a quaisquer outras partes interessadas, de alguma forma o tratamento de dados pessoais está presente.

O que vem a ser, então, tratamento de dados pessoais? A própria LGPD conceitua essa terminologia no inciso X do artigo 5º, afirmando que é *toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.*

Com este conceito em mente, uma organização trata dados pessoais sempre que, por exemplo:

- Cadastra um conjunto de dados pessoais (nome, CPF, RG, data de nascimento, por exemplo) de um cliente, parceiro, fornecedor, empregados etc.;
- Recebe ou repassa uma lista, ainda que em papel, de clientes, alunos, participantes em eventos etc.;
- Compartilha com outra entidade informações de negócio que contenham dados pessoais;
- Gerencia currículos para seleção e contratação de funcionários, colaboradores, instrutores, palestrantes, cumprimento de edital etc.;
- Faz anotações em post-it, agenda ou papel de recados de ligações e compromissos que contenham dados pessoais.

Entendido o que vem a ser o tratamento de dados pessoais, é necessário entender que ele só pode ser realizado se puder ser enquadrado em situações específicas, caracterizadas na Lei. São as chamadas hipóteses legais de tratamento, ou bases legais de tratamento, e estão descritas nos artigos 7º, 11 e 14 da LGPD. Antes, porém, de aprofundar nas bases legais, é preciso saber que os dados pessoais possuem três espécies: dados pessoais, dados pessoais sensíveis e dados pessoais de crianças e de adolescentes.

Dado pessoal é, segundo a Lei, a *informação relacionada a pessoa natural identificada ou identificável*. Isto quer dizer que toda e qualquer informação que possibilite a identificação direta de uma pessoa natural é um dado pessoal e, também, que é dado pessoal aquela informação que, embora não identifique diretamente um sujeito, permite identificá-lo quando associada a outra(s) informação(ões).

Dado pessoal sensível, por seu turno, é definido pela LGPD como sendo o *dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.*

Finalmente, dados pessoais de crianças e de adolescentes. O Estatuto da Criança e do Adolescente, Lei nº 8.069, de 13 de julho de 1990, aduz logo em seu artigo 2º: *Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade*. É esta a definição a ser adotada na LGPD, assim qualquer dado pessoal relacionados a esse público é considerado dado pessoal de crianças e de adolescentes.

Retomando as bases legais, a LGPD permite o tratamento de dados pessoais, desde que este tratamento se enquadre em alguma daquelas, ou seja, só pode ocorrer nas hipóteses abaixo:

- mediante o fornecimento de consentimento pelo titular;
- para o cumprimento de obrigação legal ou regulatória pelo controlador;
- pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Por sua vez, a hipótese seguinte soma-se às anteriormente elencadas, quando o tratamento realizado for o de dados pessoais sensíveis:

- garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Do outro lado, a realização do tratamento de dados pessoais de crianças e adolescentes só pode ocorrer com o *consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal* ou, excepcionalmente, sem consentimento quando for necessário para *contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento*.

3. Quem são os agentes de tratamentos e quais seus papéis de responsabilidades?

O artigo 5º da LGPD traz conceitos importantes e, dentre eles, a definição de que os agentes de tratamento são o controlador e o operador. Em uma simples leitura legislativa compreende-se que o controlador é responsável por tomar decisões referente aos tratamentos de dados pessoais, enquanto o operador realiza o tratamento de dados pessoais em nome do controlador.

O profissional que atua com proteção de dados entende a necessidade de aprofundar nesses conceitos para adequada implementação da LGPD, correlacionando-os

com as *guidelines* (diretrizes) europeias e os guias orientativos da Autoridade Nacional de Proteção de Dados (ANPD), os quais trazem ainda duas outras situações:

- Controladoria conjunta ou Co-controlador é quando, cumulativamente, mais de um controlador possui poder de decisão sobre o tratamento de dados pessoais; há interesse mútuo de dois ou mais controladores, com base em finalidades próprias, sobre um mesmo tratamento; e dois ou mais controladores tomam decisões comuns ou convergentes sobre as finalidades e elementos essenciais do tratamento;
- Sub-operador: é aquele contratado pelo operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador.

Ainda, a Seção III – Da Responsabilidade e do Ressarcimento de Danos – do CAPÍTULO VI que trata sobre os agentes de tratamentos, preceitua que:

> *Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.*
>
> *§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:*
>
> *I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;*
>
> *II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.*
>
> *[...]*
>
> *Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:*
>
> *I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;*
>
> *II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou*
>
> *III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.*

Isso implica dizer que uma organização, a depender do referencial a ser observado, ora pode assumir o papel de controlador e ora os demais papéis de controlador conjunto, operador e sub-operador. A definição correta, após analisado cada caso concreto, garante delimitar a responsabilidade da instituição em contratos, termos, políticas, dentre outros, mitigando riscos e prevenindo problemas.

4. Quem é e o que faz o Encarregado de Dados ou DPO? E o Comitê de Proteção de Dados?

A LGPD faz várias referências ao encarregado de dados em seu corpo (também conhecido como *Data Protection Officer* ou DPO, pela legislação europeia). A primeira delas conceituando-o:

> *Art. 5º Para os fins desta Lei, considera-se:*
>
> *[...]*
>
> *VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);*

A segunda referência ao encarregado é no CAPÍTULO IV - DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO, quando elenca regras específicas para o tratamento de dados pelo poder público:

> *Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:*
>
> *[...]*
>
> *III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;*

Por fim, a terceira referência ao operador é na Seção II – Do Encarregado pelo Tratamento de Dados Pessoais – do CAPÍTULO VI que trata DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS:

> *Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.*
>
> *§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.*
>
> *§ 2º As atividades do encarregado consistem em:*
>
> *I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;*
>
> *II - receber comunicações da autoridade nacional e adotar providências;*
>
> *III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e*
>
> *IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.*
>
> *§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.*

Juntando-se todas as referências acerca do encarregado, chegam-se às conclusões de que:

- o serviço público só pode tratar dados pessoais se, entre outras, indicar um encarregado;
- a identidade e as informações do encarregado devem ser divulgadas publicamente;
- o Encarregado tem, por atribuições:
  - "aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências";
  - "receber comunicações da autoridade nacional e adotar providências";
  - "orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais";
  - "executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares".

O rol de atribuições do encarregado pode parecer pouco, contudo, ao se desdobrar as responsabilidades elencadas, percebe-se o volume de conhecimentos e habilidades inerentes à função de encarregado de dados. O encarregado precisa "adotar providências" sobre as reclamações dos titulares e sobre as comunicações da ANPD, orientar sobre práticas de proteção de dados a serem adotadas em toda a organização e executar as atribuições do controlador ou estabelecidas em normas complementares.

Além disto, ele precisa acompanhar as comunicações da autoridade nacional, toda a legislação que trata do tema, incluindo as atualizações, as boas práticas aplicáveis à privacidade e à proteção de dados, planejar, implementar e monitorar as práticas a serem adotadas na organização e garantir que os terceiros estejam alinhados a essas práticas. Considere que isso será aplicado em todas as áreas da sua entidade e fica fácil observar a complexidade do trabalho do encarregado.

Há duas opções que a Lei permite, para ajudar neste caso específico de volume de trabalho do encarregado: a primeira possibilidade é a contratação do encarregado como serviço, ou DPO as a Service, como o mercado tem chamado. A segunda, é estabelecer um comitê de proteção de dados. Qual delas escolher? A que fizer mais sentido para o contexto da sua organização.

No caso do comitê, a recomendação é que seus integrantes sejam o encarregado de dados, os representantes das áreas de TI, do Jurídico e das principais áreas de negócio da instituição. A principal característica do comitê é ser multidisciplinar, agregando a visão de todas as áreas e servindo de apoio ao encarregado em suas atribuições, trazendo uma visão completa da organização e atuando de forma centralizada e coordenada.

5. Como o titular de dados exerce os seus direitos?

Conforme disposto no CAPÍTULO III – DOS DIREITOS DO TITULAR, em especial no artigo 18, o titular de dados pessoais tem direito de obter do controlador, a qualquer momento e mediante requisição:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no artigo 16 da LGPD;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogação do consentimento.

Para que o titular consiga exercer seus direitos, as organizações públicas e privadas precisam disponibilizar um canal de comunicação de fácil acesso, preferencialmente em seus sítios eletrônicos, devendo responder ao que foi solicitado no prazo de até 15 (quinze) dias, contados da data do requerimento do titular.

Caso as instituições não tenham eficácia nesse canal de comunicação ou não cumpram com a resposta à solicitação efetivada pelo titular, este pode fazer valer o seu direito por outras vias: denúncia perante a ANPD, reclamação nos órgãos de defesa do consumidor como PROCON e Consumidor.gov.br e acionamento da justiça.

A Autoridade Nacional de Proteção de dados (ANPD) é um órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD no Brasil. Ao receber uma denúncia, a ANPD procede com a apuração da adequação da entidade à LGPD e, caso seja constatada ausência de implementação ou irregularidades, as seguintes sanções administrativas podem ser aplicadas conforme gravidade da infração:

- advertência, com indicação de prazo para adoção de medidas corretivas;
- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- multa diária, observado o limite total a que se refere o inciso II;
- publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- eliminação dos dados pessoais a que se refere a infração;
- suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

A condenação administrativa pela ANPD não impede que o titular de dados também possa pleitear pela garantia do exercício de seus direitos perante o judiciário brasileiro. Um trabalho desenvolvido pelo CEDIS-IDP, intitulado de "Painel LGPD nos Tribunais" e disponível em https://www.jusbrasil.com.br/static/pages/lgpd-nos-tribunais.html , demonstra que entre setembro de 2020 a outubro de 2021 existiam 274 decisões fundamentadas na LGPD.

Essas decisões condenam baseadas nos seguintes temas: tratamento de dados nas investigações criminais; publicidade de dados pessoais em reclamações trabalhistas; coleta de dados para uso como prova em ações judiciais; compartilhamento e acesso a bases de dados do poder público; fraude nas relações de consumo decorrentes de uso indevido de dados; danos morais decorrentes de vazamentos ou uso indevido de dados pessoais.

Evidencia-se então que todo e qualquer negócio, público ou privado, de pequeno, médio ou grande porte, que de algum modo maneje dados pessoais, necessita estar em conformidade com a LGPD desde a data de sua vigência, qual seja, desde setembro de 2020, visando evitar sanções administrativas e condenações judiciais, proteger a imagem reputacional e propagar as boas práticas e seguranças institucionais.

6. Como funciona o processo de implementação e adequação à LGPD?

O mercado vende pílulas mágicas de adequações instantâneas, pacotes de modelos prontos para serem editados caso a caso, ou, ainda, que basta fazer cláusulas contratuais de LGPD e inserir políticas de cookies e de privacidade no site institucional para estar em conformidade. Infelizmente nada disso se procede para estar em compliance (conformidade) com a lei.

Observe que elaborar, logo no início dos trabalhos, cláusulas contratuais, políticas de privacidade e de cookies até pode ser o começo do trabalho de conformidade, desde que tais

ações estejam adaptadas ao contexto da sua instituição e desde que se tenha conhecimento de que estas atividades são apenas o início de uma longa jornada.

Conforme todo o discorrido, um projeto correto e eficaz de implementação e adequação à LGPD envolve tempo, etapas, planejamento, engajamento de toda a organização e checagem constante de todos os processos. Possui começo, meio e monitoramento constante, mas, em geral, não há fim. É um trabalho de melhoria contínua.

Não existe um *roadmap* padronizado a ser seguido por todas as consultorias, mas sim uma lógica equivalente que se verifica nos programas de implementação e adequação de qualidade em todo o mundo, principalmente na Europa, onde a proteção de dados encontra-se em fase mais avançada de consolidação e jurisprudência, servindo como norteadora para aplicação da lei nacional pelo judiciário brasileiro e pela ANPD.

Nas consultorias do Grupo JML, em geral, o primeiro passo da implementação envolve realizar o *gap analysis* (análise de lacunas) e uma conscientização da alta administração sobre a importância dos dados pessoais no seu negócio e da necessidade de proteção e garantia para os titulares de dados. Os sócios, diretores e gerentes são os detentores do poder de tomada de decisão e possuem acesso aos dados pessoais do negócio e suas finalidades, sendo fundamental estarem contextualizados entre a prática das atividades rotineiras e o que é permitido pela legislação e pelas boas práticas.

Em seguida, cabe disseminar o conhecimento básico sobre segurança da informação e proteção de dados dentro da organização, com o intuito de educar e nivelar todos os funcionários, colaboradores, parceiros e prestadores de serviços.

A nomeação do comitê e/ou do encarregado de dados é imprescindível desde o início para que eles possam acompanhar todo o trabalho, entender e consolidar a construção dos documentos probatórios, as justificativas para tomadas de decisões e a escolha fundamentada e respaldada de determinado modelo de negócio, além de reter o conhecimento produzido ao longo das etapas de consultoria.

Avançando, a próxima etapa envolve mapear os processos de trabalho a realizar (*data mapping*), analisar a documentação existente na instituição, confeccionar o inventário de dados pessoais e entender o fluxo de tratamento desses dados (*data flow*), fazer a gestão de riscos de privacidade e apresentar o relatório de diagnóstico com os gaps identificados e o registro de atividades de tratamento (ROPA) para, a seguir, elaborar um plano de ação e o relatório de impacto dos dados pessoais (DPIA).

A execução de fato do plano de ação, que consiste em uma penúltima fase, compreende elaborar ou atualizar os contratos da organização, contratos de processamentos de dados (DPA), política de segurança da informação, política de privacidade, política de cookies, termos e condições de uso, termos de consentimento, política de acesso remoto, plano de incidentes (DBN), implementar controles de segurança da informação ou melhorar os existentes, garantir os direitos dos titulares (DSARs), dentre outros.

Por fim, concluindo a metodologia de implementação e adequação à LGPD do Grupo JML, a última etapa consiste em nova apresentação do fechamento da conformidade para toda a organização, suporte para respostas às dúvidas das equipes, suporte para criação do canal de denúncias sobre violação de dados pessoais, diretrizes para o plano de comunicação e recomendações finais. Assim, ao término de todo esse percurso, é possível afirmar que a instituição está devidamente em conformidade com a LGPD.