7. Ponderações sobre a Lei Geral de Proteção de Dados Pessoais no poder público

(Autores)

MURILO JACOBY

Especialista em Direito Público. Presidente do Instituto Protege Escola Brasil e Diretor Jurídico da Jacoby Fernandes & Reolon Advogados Associados.

TATIANA CAMARÃO

Mestre em Direito Administrativo pela Faculdade de Direito da UFMG. Diretora Secretária do Instituto Mineiro de Direito Administrativo. Professora de Direito Administrativo.

1.Introdução

Em 14 de agosto de 2018, foi publicada a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), a qual dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Como disposto na própria Lei, ela passaria a vigorar em 24 (vinte e quatro) meses após a data de sua publicação.

Considerando o ambiente turvo e de instabilidade no qual se encontra o país [1] , impactado que está pela pandemia da Covid-19, foi editada a MP 959, de 29 de abril de 2020, prorrogando o prazo de entrada em vigor previsto no art. 65, II, da Lei nº 13.709/18 para o dia 3 de maio de 2021.

Contudo, estava em tramitação o Projeto de Lei nº 1.179, convertido, no dia 10 de junho de 2020, na Lei nº 14.010/2020 que prevê, no seu art. 20, que o art. 65 da Lei nº 13.309/18 seja acrescido do inciso I-A, que altera a *vacatio legis* dos arts. 52, 53 e 54 da LGPD, passando a data de sua vigência a partir, somente, do dia 1º. de agosto de 2021.

Com todas essas idas e vindas, temos, hoje, uma situação de insegurança jurídica com relação ao art. 65, II, da LGPD que trata da vigência dos artigos da Lei nº 13.709/18, visto que, nele, a vigência da Lei está regulamentada pelo art. 4º da MP 959/2020 e prevê a sua entrada em vigor para maio de 2021. Dessa forma, é importante que a MP 959/2020 seja convertida em lei sob pena de manter-se a vigência inicial prevista na Lei nº 13.709/18.

O cenário correto, portanto, é que as sanções previstas na LGPD tenham vigência fixada para 1º de agosto de 2021 e, se a medida provisória não for convertida em lei, permanece sua entrada em vigor para o dia 14 de agosto de 2020.

Não restam dúvidas, de que, mesmo diante desse imbróglio normativo [2] , é forçoso que as organizações se preparem, em especial os órgãos e entidades públicas.

Vale registrar que a LGPD tem inspiração no Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e estabelece os direitos dos titulares dos dados e a responsabilidade das organizações que coletam, armazenam, divulgam e eliminam os dados, bem como as sanções no caso de infração da Lei.

Com objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, a citada lei prescreve que as organizações devem adequar suas atividades às exigências da lei e promover melhorias na governança da organização.

A ausência de medidas técnicas e administrativas para estruturação de um programa de proteção de dados importará na violação das normas da LGPD pela organização [3] e poderá ensejar, a partir de 1 de agosto de 2021 [4] , a aplicação de sanções administrativas de enorme impacto financeiro e reputacional pela Autoridade Nacional de Proteção de Dados (ANPD). [5]

Por se tratar de norma de caráter sancionatório, há previsão na lei de circunstâncias que podem agravar ou atenuar a pena, pautada na ocorrência dos seguintes parâmetros e critérios: gravidade e a natureza das infrações e dos direitos pessoais afetados; a condição econômica do infrator; a reincidência; o grau do dano; a pronta adoção de medidas corretivas; a proporcionalidade entre a gravidade da falta e a intensidade da sanção; e a proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados.

Além dessas sanções, os responsáveis poderão sofrer as penas descritas em leis específicas, como a Lei de Improbidade Administrativa, Lei de Acesso à Informação e Estatutos Funcionais.

2.Programa de Proteção de Dados Pessoais

Percebe-se, neste contexto, a importância de as organizações adotarem medidas corretas de proteção de dados pessoais por meio de um programa de governança de privacidade efetivo e que observe os seguintes requisitos: [6]

> a) comprometimento do controlador dos dados obtidos em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
>
> b) aplicação do programa de proteção a todo o conjunto de dados pessoais que estejam sob a custódia do controlador,

independentemente do modo como se realizou sua coleta;

c) adaptação do programa à estrutura, escala e volume das operações da organização, bem como ao grau de sensibilidade dos dados tratados;

d) previsão no programa de políticas e salvaguardas adequadas de avaliação sistemática de impactos e riscos à privacidade;

e) previsão de relação de confiança da organização com o titular dos dados, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) previsão de que o programa esteja integrado à estrutura geral de governança da organização e que estabeleça e aplique mecanismos de supervisão internos e externos;

g) elaboração de planos de resposta a incidentes e para remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Como podemos ver, o programa de proteção de dados pessoais serve como motor de aperfeiçoamento dos procedimentos internos e fator de prevenção e redução dos riscos de desconformidades, levando à preservação da reputação da organização e ao abrandamento da responsabilização administrativa, civil e criminal dos agentes públicos responsáveis pelo processamento de dados.

2.1.Etapas de implantação do programa de proteção de dados pessoais

2.1.1.Comitê de LGPD – o envolvimento de grupo multidisciplinar

O primeiro passo é a constituição de um comitê, multidisciplinar [7] , ao qual será atribuída a competência para capitanear o diagnóstico atual da organização, elaborar a arquitetura do programa e implementar ações de

monitoramento [8] . Por óbvio, todas as decisões serão chanceladas pela alta direção da organização, a qual assume um papel de destaque no acompanhamento do processo de implantação e apoio necessários ao funcionamento do programa.

2.1.2.Diagnóstico – critério e atenção no levantamento de informações

A etapa de diagnóstico contempla a realização de levantamentos criteriosos de todos os dados pessoais tratados na organização, seu ciclo de vida, identificando ainda aqueles que exigem mais cuidado no tratamento, e a verificação se os procedimentos, operações e documentos estão amoldurados à lei. Nessa auto avaliação inicial, é importante, ainda, conhecer o ambiente regulatório no qual está inserida a organização, [9] analisar os sistemas, apurar os fluxos de negócios e documentos relacionados a cada tipo de dado pessoal. [10]

A identificação da maturidade dos processos dentro da instituição torna possível definir um espectro das ações e atividades que envolvem a utilização de dados pessoais e sensíveis e quais são as deficiências e lacunas existentes. Este procedimento de autoconhecimento pode ocorrer por meio de questionário enviado aos dirigentes de cada área de negócio responsáveis pelo tratamento de dados pessoais e que conhecem a organização. [11]

Prática melhor, e com impactos mais assertivos para a organização, é a aplicação deste questionário em um treinamento, durante o qual se pode tirar dúvidas dos participantes sobre as perguntas e, por meio das respostas e interação entre os dirigentes, aprofundar em temas que ainda são frágeis para a organização e obter de maneira objetiva as informações necessárias para estruturação do programa.

2.1.3.Riscos e tratamento dos dados

Superada a fase de diagnóstico, passamos para a depuração dos principais riscos dos processos e sistemas de tratamento de dados da organização. Somente com o mapeamento completo dos dados pessoais e mensuração dos riscos é possível estruturar e direcionar, de forma assertiva, o programa, inclusive com as medidas para revisão de processos e adequação às exigências da LGPD.

Para tal ação, mostra-se como boa prática a inclusão de riscos levantados por entidades internacionais [12] e outros entre similares, de forma a agregar a experiência alheia no processo.

No levantamento dos tipos de arranjos de trabalho, serão apuradas informações sobre o dado coletado, verificando sua sensibilidade ou não, os responsáveis por sua coleta e gerenciamento, sua utilização, o momento do seu registro, a existência do consentimento do proprietários dos dados, a justificativa para o levantamento desses dados, o processo de sua eliminação no momento adequado, a solução tecnológica utilizada para armazenamento, a seleção para compartilhamento e fundamentos, ações e medidas de proteção que são adotadas.

Com o mapeamento completo dos dados pessoais e mensuração dos riscos é possível estruturar e direcionar de forma eficiente e eficaz o programa, inclusive com as medidas para revisão de processos e adequação às exigências da LGPD [13] .

2.1.4.Política de proteção de dados – um norteador das ações

É essencial criar a política de proteção de dados pessoais, estabelecendo as diretrizes e condições que deverão ser observadas pela organização e que envolverão o regime de funcionamento, as formalidades enfeixadas nos procedimentos de reclamações e petições de titulares, as normas de segurança de dados pessoais e sensíveis, os padrões técnicos, o direito de acesso e outros aspectos relacionados ao tratamento de dados pessoais.

Faz-se necessário, também, pelas normas enredadas na lei, normatizar e implantar **procedimentos e documentos padronizados** para informar ao titular a finalidade e forma de utilização dos dados pessoais, [14] bem como para a formulação de pedidos, regras de acesso, formas de descarte, correção e atualização, portabilidade e anonimização. A isto se soma, a importância de se criar o procedimento para o formal consentimento do titular do dado, quando necessário sua utilização ou compartilhamento.

Ainda sobre o compartilhamento ou integração de dados coletados com terceiros, é imprescindível **regulamentar** esse processo, indicando o substrato legal ou contratual que amparam essa ação.

É imperioso, ainda, estabelecer a política acompanhada do **procedimento operacional padrão** a ser adotado no caso de incidentes de segurança, contemplando nestes a comunicação das contingências potenciais de violação.

A propósito, Rony Vainzof e Nuria Lopez sugerem regras de boas práticas que poderão ser formuladas no código de conduta [15] :

> Essas regras devem estabelecer:
>
> - as condições de organização;
>
> - o regime de funcionamento;
>
> - os procedimentos, incluindo reclamações e petições de titular;
>
> - as normas de segurança;
>
> - os padrões técnicos;
>
> - as obrigações específicas para os diversos envolvidos no tratamento;
>
> - as ações educativas;
>
> - os mecanismos internos de supervisão e de mitigação de riscos;
>
> - entre outros.

Enfim, é vital para a arquitetura do programa de proteção de dados que os órgãos e entidades públicas tenham **políticas** com diretrizes orientadas a preservar a conformidade da organização à LGPD. Por óbvio, todas estas medidas deverão ser acompanhadas por investimentos em sistemas de informação e soluções tecnológicas para proteção de dados pessoais e preservação da privacidade.

Ademais, e como medida indispensável, há que se promover políticas e ações relacionadas aos fornecedores e prestadores de serviços. Para tanto, deve-se realizar um levantamento das contrações que têm como objeto a prestação de serviços que envolvem ou estejam atreladas ao acesso e processamento de dados pessoais, adequando-se às exigências da LGPD.

Um exemplo clássico é o dos contratos de trabalhos com dados pessoais do empregado. Nestes deverão estar inclusa cláusula individualizada e devidamente destacada dando ciência à parte

interessada, ou titular do dado, da utilização dos seus dados e outra com o seu respectivo consentimento [16] .

Não obstante a isto, é importante, também, definir quais dados pessoais devem figurar na minuta contratual, buscando proteger os contratados e incluir cláusula contratual acerca das obrigações e deveres do contratado e subcontratado de observação da LGPD.

2.1.5.Política de Proteção de Dados Pessoais dos Contratados - Due Diligence

Após o desenvolvimento da política, uma medida que desponta diz respeito à necessidade de formalizar com o contratado e seus funcionários um acordo de confidencialidade e decantar nos contratos e nos sistemas de gerenciamento de dados o que é designado informação de livre acesso, de acesso restrito, sigilosa ou reservada.

Não se pode perder de vista que deverão ser realizadas gestão de riscos e diligências para verificação da **conformidade do contratado** em relação à LGPD. Sua inadequação influi diretamente no desenvolvimento dos negócios do órgão ou entidade pública contratante.

Nota-se, como mencionado acima, que os órgãos e as entidades deverão buscar expandir o alcance de seu Programa de Proteção de dados para os fornecedores e prestadores de serviços contratados.

Vale registrar que, no caso de órgãos e entidades públicas nas quais o tratamento de dados pessoais é realizado para o atendimento de sua finalidade pública e na persecução do interesse público, com fins de executar as competências legais ou cumprir as atribuições legais do serviço público, algumas premissas devem ser observadas nos programas de proteção de dados pessoais. São elas:

> a) Divulgar em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, que, no exercício de suas competências, serão realizados tratamento de dados pessoais e asseguradas informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessa atividade;

b) Indicar os responsáveis do órgão que ficarão com a atribuição de realizar operações de tratamento de dados pessoais e o encarregado [17] .

Toda implementação de uma nova política e ação, via de regra, demanda a realização de treinamentos para ensinar e reforçar as melhores práticas e, mesmo, a checagem do aprendizado ou retenção das informações. É um caso de mudança de comportamento, de comprometimento dos usuários e, portanto, demanda atenção, tempo e monitoramento dessa nova atitude que, neste caso, não se trata de um desejo e sim de um dever legal.

O treinamento ainda é essencial para sensibilizar a equipe no uso das ferramentas disponíveis (documentos padronizados, procedimentos operacionais padrão, política) e na interação com outros agentes (o titular dos dados, o controlador, o contratado).

Por esse motivo, no caso da LGPD, o conteúdo programático dos treinamentos deverá contemplar temas, como:

a) o atendimento dos usuários do serviço em relação ao vazamento de dados sensíveis, correção de informação e exclusão de dados pessoais;

b) a compreensão das regras de segurança e de custódia da informação;

c) as medidas a serem tomadas no caso de um incidente de segurança da informação;

Notadamente, para os treinamentos, é uma boa prática a elaboração de um **plano de capacitação** que garanta coerência entre as suas diversas fases de aprendizado, de acordo com a demanda de cada órgão ou entidade pública.

Ainda por se tratar de uma mudança na organização, ressoa como vital para eficácia do programa, o planejamento e execução de um plano estratégico de comunicação para os servidores, prestadores de serviços e usuários do serviço, com a finalidade de disseminar informações das ações implementadas e cultura de privacidade, mas, acima de tudo, fortalecer os comportamentos que devem ser adotados.

2.1.6.Monitoramento – sempre mensurando e aprimorando

Por fim, completando o ciclo de implantação do programa de proteção de dados, passa-se à etapa de **monitoramento contínuo** , com ações de supervisão, operacionalização e *loops de feedbacks* para melhorar a performance da organização.

Importante destacar que a autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado, e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.

3.Considerações finais

Como se percebe, a Lei nº 13.709/2018 é um marco regulatório e permite uma releitura do princípio da privacidade, estabelecendo um rol de direitos e obrigações para os órgãos e entidades públicas e privadas, que irão demandar a implantação de programa de proteção de dados pessoais.

Por se tratar de programa que envolve várias políticas e ações, é possível dizer que a jornada virtuosa tem início, mas não tem fim [18] . A despeito de muitos desafios que serão enfrentados para estruturação do programa, é inegável que este representa um grande passo para melhoria da governança quanto à privacidade dos dados e segurança da informação nas organizações públicas ou privadas.

Referências bibliográficas

BRASIL. Lei nº 13.709/2018, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 15 ago. 2018. Seção 1, p. 59.

ASPIS, Fábio Lara. Aplicações práticas da LGPD. Revista LEC – *Legal, Ethics, Compliance* , São Paulo, ano 7, nº 27, novembro/2019.

BRUNO, Marcos Gomes da Silva. Pandemia de Covid-19 e o adiamento da Lei Geral de Proteção de Dados. Disponível em: <https://opiceblumacademy.com.br/2020/04/adiamento-lgpd-covid-19/>. Acesso em 13 abr. 2020.

CHO, Tae Young. Aplicações práticas da LGPD. Revista LEC – *Legal, Ethics, Compliance* , São Paulo, ano 7, nº 27, novembro/2019.

JUNQUEIRA, Thiago; CHALFINS, Renato. Covid-19 e postergação da LGPD: histeria ou sabedoria?. Disponível em: <https://www.conjur.com.br/2020-abr-21/opiniao-covid-19-postergacao-lgpd-histeria-ou-sabedoria>. Acesso em 21 jun. 2020.

LEMES, Daniele. Como adaptar os contratos à Nova Lei Geral de Proteção de Dados. Disponível em: <https://danilemes.jusbrasil.com.br/artigos/801125986/como-adaptar-os-contratos-a-nova-lei-geral-de-protecao-de-dados>. Acesso em 13 abr. 2020.

PECK, Patrícia. Aplicações práticas da LGPD. Revista LEC – *Legal, Ethics, Compliance* , São Paulo, ano 7, nº 27, novembro/2019.

VAINZOF, Rony; LOPEZ, Nuria. Governança em privacidade: *compliance* à LGPD de dentro para fora. In: Andrade, Renato Campos; SOUZA, Fernanda Nunes Coelho Lana e; TOMAGNINI, Flávia Neves; UCHOA, Maria Raquel de Sousa Lima. *Compliance* em Perspectiva. Belo Horizonte: D´Plácido, 2019.

VAINZOF, Rony; LIMA, Caio César Carvalho; MORAES, Henrique Fabretti; FURTADO, Tiago Neves. O caminho que deve ser percorrido para adequação à LGPD. Disponível em: <https://https://opiceblumacademy.com.br/2020/01/lgpd-mitos-desafios/. Acesso em 21 jun. 2020.

1

A propósito, Thiago Junqueira e Renato Chalfins, registram: “Sem embargo de iniciativas prévias no Senado (PL nº 1.027/2020) e na Câmara dos Deputados (PL nº 5.762/2019), foi apenas com a evolução da Covid-19 que a proposta de adiamento da entrada em vigor da LGPD ganhou força. A prorrogação do prazo de vigência e das sanções administrativas foi inserida no designado Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (Projeto de Lei nº 1.179/2020). Originalmente correspondendo a 18 meses, após emendas, o Senado acolheu a

seguinte determinação: “adiar, em regra, a vacatio legis da Lei Geral de Proteção de Dados até 1º de janeiro de 2021, com a ressalva de que os artigos relativos às sanções só entrarão em vigor em agosto de 2021”.Entre os argumentos para o adiamento da LGPD, a serem, em um futuro próximo, escrutinados pelos deputados federais (e, possivelmente, pelo presidente da república), possuem destaque a ausência de criação da Autoridade Nacional de Proteção de Dados (ANPD) e a impossibilidade de adequação, caso seja mantida a entrada em vigor para agosto deste ano, de parte significativa das empresas — seja por dificuldades econômicas, muito agravadas pela pandemia, seja pela necessidade de encontros presenciais, ora impedidos, para a implementação de programas de conformidade à lei”. Disponível em: https://www.conjur.com.br/2020-abr-21/opiniao-covid-19-postergacao-lgpd-histeria-ou-sabedoria.

2

Sugerimos a leitura do artigo de autoria de Rodrigo Pironti Aguirre de Castro, LGPD e a MP 959/20: O início de uma pandemia normativa sobre proteção de dados. Disponível em: https://www.cafecompliance.com.br/?area=artigo&c=f4d83289b95746bdc7fd1ffbf34eaba3.

3

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - 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;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

(...)

X - 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; (Incluído pela Lei nº 13.853, de 2019)

XI - 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;

(Incluído pela Lei nº 13.853, de 2019)

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.(Incluído pela Lei nº 13.853, de 2019)

4

Com relação a aplicação de sanção, considerando o horizonte mais alargado de entrada em vigor previsto na Lei nº 14.010/2020, cumpre citar ensinamentos de Marcos Gomes da Silva Bruno, que muito embora tenha feito essa análise baseado em outro cenário de alteração de vigência da lei, serve para compreensão mais abrangente da necessidade das organizações se adequarem a LGPD: a Autoridade Nacional de Proteção de Dados (ANPD) não poderá aplicar sanções às empresas que de alguma forma infringirem a LGPD, mas a LGPD servirá de fundamento para todas as outras demandas e discussões envolvendo tratamento de dados pessoais, em especial aquelas oriundas dos Titulares de Dados, Ministérios Públicos, Órgão de Proteção e Defesa do Consumidor, entre outros. O mesmo autor ilustra, ainda, as situações que as empresas serão cobradas quanto à sua adequação à LGPD, embora sobrestada o prazo de entrada em vigor das sanções administrativas para 1º de agosto de 2021: indenizações em ações individuais e coletivas, multas em processos administrativos como os da SENACON – Secretaria Nacional do Consumidor, e outros. (BRUNO, Marcos Gomes da Silva. Pandemia de Covid-19 e o adiamento da Lei Geral de Proteção de Dados. Disponível em: https://opiceblumacademy.com.br/2020/04/adiamento-lgpd-covid-19/).

5

A autoridade nacional é o órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

6

Art. 50, § 2º, da Lei nº 13.709/2018.

7

Na mesma perspectiva Tae Young Cho destaca a importância da participação de representantes de todas as áreas da organização durante a fase de implantação do programa de LGPD: “O engajamento da alta administração da empresa é muito importante, mas, sozinho, não garante o sucesso na implementação. É fundamental o engajamento da alta direção aliado (ao de representantes das áreas impactadas pela LGPD) para criar um ambiente de colaboração e de mudança de cultura na empresa, porque é disso, também, que se trata a implantação da LGPD” (Aplicações práticas da LGPD. Revista LEC – *Legal, Ethics, Compliance* , São Paulo, ano 7, nº 27, novembro/2019, P. 41).

8

Sugerimos a criação do Comitê, mas o órgão ou entidade pública, que vai implantar o programa, pode definir a área de acordo com sua estrutura e finalidade. A respeito escreve Rony Vainzof e Nuria Lopez: “Por isso, fez sentido para muitas organizações

absorver a Lei Geral já bem estruturada a área de *compliance* como seu ponto focal. Outras empresas, em setores muito regulamentados elegeram o jurídico como ponto focal do *compliance* de dados. Outas, muito ligadas à segurança, elegeram a Segurança da Informação ou a Tecnologia da Informação.

Outras, ainda, mantiveram o *compliance* de dados vinculados às áreas de negócios ou às áreas de risco. Não há resposta correta. Cada empresa precisa olhar para sua própria estrutura e readequá-la a esse *compliance* , que é muito particular" (Governança em privacidade: *compliance* à LGPD de dentro para fora. In: Andrade, Renato Campos; SOUZA, Fernanda Nunes Coelho Lana e; TOMAGNINI, Flávia Neves; UCHOA, Maria Raquel de Sousa Lima. *Compliance* em Perspectiva. Belo Horizonte: D´Plácido, 2019. P. 306).

9

Podemos citar as seguintes leis que devem ser analisadas em consonância com os ditames da LGPD: A Lei de Acesso à Informação, Marco Civil da Internet, Segurança Cibernética.

10

De acordo com o art. 5º da Lei nº 13.709/2018, considera-se:

I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II– dado pessoal sensível: 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;

III– dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

11

Podemos citar seguintes setores que deverão ser envolvidos na implantação da política: TI, recursos humanos, escolas, financeiro, planejamento, jurídico, controladoria.

12

Cita-se, a título de exemplo, o levantamento feito pela União Europeia, por meio do Supervisor de Proteção de dados. Disponível em <https://edps.europa.eu/data-protection/data-protection/reference-library/information-security_en>. Acesso em: 13 abr. 2020.

13

De acordo com Patrícia Peck: O maior desafio neste momento é o de entender o diagnóstico atual, ou seja, ter um cenário real e consistente de Gap Analysis para poder

então focar na priorização da execução do Plano de Ação, sabendo quais as medidas mais urgentes que precisam ser realizadas até a entrada em vigor dos dispositivos da lei. A autora, ainda, esclarece que a LGPD é uma lei de partida e não de chegada, e vai precisar haver manutenção da conformidade (Aplicações práticas da LGPD. Revista LEC – Legal, Ethics, Compliance, São Paulo, ano 7, nº 27, novembro/2019, P. 42).

14

Os titulares dos dados poderão exercer seus direitos perante o Poder Público considerando os prazos e procedimentos previstos em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

15

Governança em privacidade: *compliance* à LGPD de dentro para fora. In: Andrade, Renato Campos; SOUZA, Fernanda Nunes Coelho Lana e; TOMAGNINI, Flávia Neves; UCHOA, Maria Raquel de Sousa Lima. *Compliance* em Perspectiva. Belo Horizonte: D ´Plácido, 2019. p. 302-303.

16

De acordo com Daniele Lemes: “os contratos deverão carregar uma cláusula especificando onde e como serão utilizados os dados pessoais contidos naquele contrato, descrevendo onde esses dados serão armazenados (local físico, adição dos dados em sistemas, etc.), vez que a Lei prevê a necessidade de se demonstrar como os dados coletados serão tratados” (LEMES, Daniele. Como adaptar os contratos à Nova Lei Geral de Proteção de Dados. Disponível em: https://danilemes.jusbrasil.com.br/artigos/801125986/como-adaptar-os-contratos-a-nova-lei-geral-de-protecao-de-dados).

17

De acordo com Fábio Lara Aspis é recomendável que o encarregado tenha independência e reporte ao nível mais alto de gestão do controlador ou operador (C-level ou board). Ainda, é aconselhável que este tipo de profissional não acumule cargos, como por exemplo, executar simultaneamente as funções de Diretor de TI e DPO, de forma a não impactar em sua principal incumbência, que deverá ser a proteção de dados pessoais (Data Protection Officer ou Encarregado. Revista LEC – *Legal, Ethics, Compliance* , São Paulo, ano 7, nº 27, novembro/2019, p. 39).

18

No artigo “Dia Internacional da Proteção de Dados e a jornada de conformidade com a LGPD no ano de sua eficácia – Desvendando mitos e desafios, sem reinventar a roda”, Rony Vainzof, Caio César Carvalho Lima, Henrique Fabretti Moraes e Tiago Neves Furtado, o caminho que deve ser percorrido para adequação à LGPD. Disponível em: https://opiceblumacademy.com.br/2020/01/lgpd-mitos-desafios/