CAPACITAÇÃO DA ADVOCACIA

Lei Geral de Proteção de Dados Pessoais

Material de Apoio

ARTIGOS

Ana Amelia Menna Barreto
DIREITO DIGITAL E PROTEÇÃO DE DADOS

SUMÁRIO

Autoria de Ana Amelia Menna Barreto

A PROTEÇÃO JURÍDICA DE DADOS PESSOAIS NO BRASIL

Introdução

Acompanho o movimento europeu na regulamentação sobre a proteção de dados pessoais e a privacidade, a aplicação de sua Diretiva, seus reflexos mundiais, assim como a atualização trazida pelo Regulamento Geral de Proteção de Dados.

Enquanto mais de uma centena de países promoviam a necessária proteção da privacidade e dos dados pessoais dos indivíduos, o Brasil adormecia em berço esplêndido. Sua tardia regulação foi fruto de idas e vindas de arremedos legislativos, invariavelmente movidas ao sabor de interesses políticos de todos os segmentos envolvidos.

Na economia digital a informação é seu ativo mais importante. Nossos dados revelam tudo sobre cada um de nós são capturados e rentabilizados a nossa revelia. A mercadoria é você, seus hábitos de consumo, preferência, geolocalização. Rastros de nossas pegadas digitais que marcamos a cada navegação. Daí a importância da efetiva tutela jurídica de proteção dos direitos e garantias individuais.

Nesse cenário de proteção não somos exatamente um exemplo a ser seguido. O rompimento desse paradigma se realizará por uma profunda mudança cultural voltada ao respeito, proteção e ética quanto à guarda segura de nossos dados pessoais identificáveis.

Escrevo essas linhas em janeiro de 2019 na interseção temporal entre a promulgação da lei de proteção de dados, após a criação e antes da instalação da Autoridade e o do Conselho nacional de dados e de privacidade. Antes da vigência desse novo normativo legal, até 2020 muita água ainda passará por debaixo dessa ponte imaginária.

A proteção de dados pessoais na União Européia

A Carta dos Direitos Fundamentais da União Europeia datada de 2012 estabeleceu que todos os cidadãos do bloco têm direito à proteção dos seus dados pessoais[1].

A Diretiva nº 46 do ano de 1995[2] tornou-se uma referência internacional por cuidar da proteção das pessoas singulares no que se refere ao tratamento de dados pessoais,

---

[1] Disponível em <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt> Acesso em 01 fev. 2019

[2] Disponível em<https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:pt:HTML> Acesso em 01 fev. 2019

assim como sua livre circulação. Os Estados-membros devem assegurar a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais.

Após anos de discussão no Parlamento Europeu essa Diretiva foi reoxigenada pelo Regulamento Geral de Proteção de Dados 2016/679[3], com o objetivo de reforçar os direitos fundamentais dos cidadãos na era digital e facilitar a atividade comercial através da simplificação das normas aplicáveis às empresas no mercado único digital. Todas as empresas que armazenassem dados pessoais de cidadãos europeus - mesmo as não estabelecidas na UE - tiveram o prazo de dois anos para ficar em conformidade com as novas regras, vigentes desde maio de 2018.

A proteção de dados pessoais no Brasil

A proteção legal dos dados pessoais no Brasil estava dissolvida esparsamente em vários mandamentos legais.

Em 1984 a Política Nacional de Informática teve como princípios o estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas, assim como o direito ao acesso e à retificação de informações sobre ele existentes em bases de dados públicas ou privadas[4].

Nossa Constituição Federal garantiu entre as cláusulas pétreas a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação[5]. Também recebeu status constitucional o direito de retificação de dados de todo cidadão brasileiro - através do remédio constitucional do habeas data - para conferir o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, assim como para a retificação de dados[6].

Também ficou consagrado constitucionalmente o direito de todos receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo

---

[3] Disponível em <https://eurlex.europa.eu/legalcontent/PT/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC> Acesso em 01 fev. 2019

[4] Lei 7.232/1984, art. 2º, VIII e IX

[5] Art. 5º, X

[6] Art. 5º, LXXII, a e b, regulado pela Lei 9.507/97

sigilo seja imprescindível à segurança da sociedade e do Estado. É permitido o acesso dos usuários a registros administrativos e a informações sobre atos de governo, cabendo a administração pública, a gestão da documentação governamental, assim como as providências para franquear sua consulta a quantos dela necessitem[7].

O Código de Defesa do Consumidor faz referência literal sobre banco de dados e cadastros de consumidores, concedendo aos titulares o direito de acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes[8].

A Lei de Acesso a Informação regulou o acesso previsto na lei do habeas data[9] sendo posteriormente regulamentada pelo Decreto 7.724/2012 para disciplinar a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

A chamada Lei do Cadastro Positivo regulamentou a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito[10].

Em 2014 emergiu o chamado Marco Civil da Internet, Estabelecendo princípios, garantias, direitos e deveres para o uso da Internet no Brasil, ressaltou a necessidade da proteção de dados pessoais na forma da lei, até então inexistente[11].

Em 2018 a Política Nacional de Segurança da Informação da administração pública federal - instituída pelo Decreto 9.637 - teve como objetivo assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional. Entre seus princípios gerais destacam-se o respeito e a promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação. Além de prever a ampla participação da sociedade e dos órgãos e das entidades do Poder Público na criação da Estratégia Nacional de Segurança da Informação, estabelece o dever de criar ações estratégicas para proteção contra vazamento de dados[12].

---

[7] Arts. 5º, inciso XXXIII, art. 37, § 3º, II e art. 216, § 2º
[8] Lei 8.804/1990, art. 43, §§ 1º e 2º
[9] Lei 12.527/2001, art. 38

[10] Lei 2.414/2011, regulamentada pelo Decreto 7.829/2012
[11] Lei 12.965/2014, art. 7º
[12] Art. 3º, II e art. 6º, V e parágrafo único.

A LEI DE PROTEÇÃO DE DADOS PESSOAIS BRASILEIRA

Com um *delay* de algumas décadas finalmente o Brasil se incluiu no ecossistema mundial de regulação da proteção de dados em 2018.

Em apertada síntese os primeiros passos a caminho da regulação se iniciaram em 2005 em discussões internas no âmbito do Poder Executivo. Em 2010 o Ministério da Justiça submeteu a consulta pública um Anteprojeto de lei que, após cinco anos de hibernação, foi reapresentado sob nova roupagem e igualmente submetido ao debate público. Também o Poder Legislativo trafegava em suas próprias iniciativas regulatórias.

Finalmente em 14 de agosto de 2018 emergiu a Lei 13.709 dispondo sobre o tratamento de proteção de dados pessoais, inclusive nos meios digitais. Poucos meses após sua edição, o texto veio a ser alterado pela Medida Provisória 869, de 27 de dezembro de 2018.

A norma protege de forma ampla os dados pessoais, cria direitos do titular, enumera as hipóteses autorizadas para tratamento, além de prever responsabilidades e sanções de ordem administrativa e pecuniária de ressarcimento de danos por vazamentos.

Tem por objetivo a proteção dos direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural, tendo como fundamentos da proteção de dados o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais[13].

Os direitos e princípios expressos na norma não excluem os outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte[14].

Por suas definições o dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. O dado pessoal sensível se relaciona a aquele que revela a origem racial ou étnica, a convicção religiosa, a opinião política, a filiação a sindicato ou a organização de caráter religioso, filosófico ou político, o dado referente à saúde ou à vida sexual, o dado genético ou biométrico, quando vinculado a uma pessoa natural.

[13] Art. 2º
[14] Art. 64

Existe ainda a classificação do dado anonimizado, que se caracteriza pela não identificação de seu titular[15].

O escopo alcança qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: a operação de tratamento seja realizada no território nacional; quando a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional, assim considerado quando coletados os dados pessoais cujo titular nele se encontre no momento da coleta[16].

Entende-se por tratamento toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração[17].

A atividade deve observar os princípios da boa fé, da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação, da responsabilização e da prestação de contas[18].

Elencadas as hipóteses permitidas para o tratamento, ressalta que o consentimento do titular, quando necessário, deve ser fornecido por escrito e constar de cláusula destacada ou outro meio idôneo de manifestação. Além do consentimento existem outras nove outras hipóteses de autorizações legais elencadas no art. 7º.

O tratamento de dados pessoais sensíveis somente pode ocorrer com o consentimento específico e destacado do titular ou responsável legal. Quando desnecessário o consentimento as hipóteses se circunscrevem as previsões contidas no art. 11.

Em se tratando de crianças e adolescentes o tratamento deve ser realizado com o consentimento específico - e em destaque - por pelo menos um dos pais ou pelo responsável legal[19].

O término do tratamento dos dados ocorre após ter sido alcançada sua finalidade ou quando deixarem de ser necessários ou pertinentes ao alcance da finalidade específica

[15] Art. 5º
[16] Art.3º
[17] Art. 5º
[18] Art.6º
[19] Art. 14

almejada, ou pelo fim do período de tratamento, pela comunicação do titular, ou por determinação da autoridade nacional em caso de violação legal[20].

Autoriza-se a eliminação dos dados pessoais após o término de seu tratamento e no âmbito e nos limites técnicos das atividades. Sua conservação está autorizada apenas para o cumprimento de obrigação legal ou regulatória pelo controlador; de estudo por órgão de pesquisa, sempre eu possível garantida sua anonimização; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei ou, uso exclusivo do controlador, vedado seu acesso por terceiro e desde que anonimizados os dados[21].

A pessoa natural titular dos dados pessoais tem assegurados os direitos fundamentais de liberdade, de intimidade e de privacidade, além de poder obter uma série de informações do controlador - por requerimento expresso dirigido ao agente de tratamento.[22]

A Lei alcança as pessoas jurídicas de direito público, a saber: órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, Judiciário e Ministério Público, assim como as autarquias, fundações e empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios[23].

Também se enquadram os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, as empresas públicas e as sociedades de economia mista, quando operacionalizem políticas públicas e no seu âmbito da execução[24]. O tratamento deve ser realizado para o atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público e desde que seja indicado um encarregado.

Por padrão está vedada a transferência de dados pessoais a entidades privadas, sujeitas ao consentimento do titular a comunicação ou o uso compartilhado de dados pessoais[25].

Os agentes de tratamento são responsáveis por adotar medidas de segurança, técnicas e administrativas para proteção dos dados pessoais, de acessos não autorizados e de

[20] Art. 8, § 5º e art. 15 e incisos

[21] Art. 16

[22] Arts. 17, 18 e §§

[23] Art. 23

[24] Art. 23, § 4º e 24, parágrafo único

[25] Art. 26, § 1º e art. 27

situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito[26].

Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obrigam-se a garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término. O 'controlador' tomará as decisões relativas ao tratamento, deve indicar a figura do 'encarregado', assim como comunicar à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares[27].

O 'operador' é responsável por realizar o tratamento segundo as instruções do controlador e o 'encarregado'- indicado pelo controlador - atuará como canal de comunicação entre o controlador, o titular dos dados e a Autoridade Nacional de proteção de dados[28].

É responsabilidade do controlador, ou do operador, o ressarcimento de dano patrimonial, moral, individual ou coletivo por violação à legislação de proteção de dados pessoais. A excludente de responsabilidade somente ocorre caso os agentes de tratamento provem que não realizaram o tratamento de dados pessoais, que não houve violação à legislação no tratamento ou que o dano decorreu de culpa exclusiva do titular dos dados ou de terceiros[29].

Todos os agentes de tratamento se obrigam a adotar medidas de segurança, técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito[30].

No âmbito das competências dos controladores e operadores cabem a esses formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais[31].

---

[26] Art. 46
[27] Arts. 47 e 48

[28] Arts. 5º, VI a VIII e 37 a 41
[29] Art. 42 e 43
[30] Arts. 46 e seguintes
[31] Art. 50

As sanções[32] de ordem administrativa - aplicáveis pela autoridade nacional - levarão em conta a gravidade e a natureza das infrações e dos direitos pessoais afetados, além de um elenco de condicionantes.

As penalidades de ordem pecuniária dividem-se em: advertência, multa simples de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, limitada, no total, a cinquenta milhões de reais por infração; multa diária, observado o limite total referido; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais até a sua regularização e a eliminação dos dados pessoais a que se refere a infração. O valor da sanção de multa diária deve observar a gravidade da falta e a extensão do dano ou prejuízo causado.

Assim como previsto na norma europeia permite-se a transferência internacional de dados pessoais a países estrangeiros, somente quando assegurarem um nível de proteção considerado adequado pelo regramento brasileiro.

Autoridade nacional de proteção de dados[33]

A criação da autoridade nacional de proteção de dados e do conselho nacional de proteção de dados pessoais e da privacidade - inicialmente constante da Lei 13.709/2018 -foi vetada pelo Poder Executivo[34].

Posteriormente a Medida Provisória 869 - editada em 27 de dezembro de 2018 – recriou a autoridade e o conselho nacional[35].

A Autoridade nacional teve sua genética transmutada pela MP. Inicialmente concebida como integrante da administração pública federal indireta, se submetia ao regime autárquico especial, estava vinculada ao Ministério da Justiça e regida pela Lei 9.986/2000. Sua então natureza de autarquia especial se caracterizava pela independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira. Mas ressurgiu na Medida Provisória como órgão da administração pública federal integrante da estrutura da

---

[32] Art. 52 e seguintes

[33] Arts. 55 e seguintes

[34] Afronta aos arts. 61, § 1º, II, 'e', e ao art. 37, inciso XIX da Constituição Federal. Mensagem de veto 451/2018. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm> Acesso em 03 fev. 2019

[35] Exposição de Motivos MP 869/2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Exm/Exm-MP-869-18.pdf>. Acesso em 03 fev. 2019

Presidência da República[36], com cargos alocados em estruturas já vigentes de órgãos e entidades do Poder Executivo[37], instalada sem aumento de despesa e com autonomia técnica[38].

A Autoridade é composta pelo Conselho Diretor, pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, pela Corregedoria; pela Ouvidoria; por órgão de assessoramento jurídico próprio e unidades administrativas e especializadas necessárias ao seu funcionamento. Sua estrutura regimental ainda pendente receberá por ora apoio técnico e administrativo da Casa Civil da Presidência da República para o exercício de suas atividades.

O Conselho Diretor ocupa a figura de órgão máximo de direção, composto por cinco diretores, escolhidos dentre brasileiros, de reputação ilibada, com nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados pelo Presidente da República, com mandato de quatro anos.

A Autoridade atuará como órgão central de interpretação da Lei cabendo-lhe estabelecer as normas e procedimentos sobre proteção de dados pessoais e diretrizes para a sua implementação, fiscalizar e aplicar sanções, articular sua atuação com o Sistema Nacional de Defesa do Consumidor do Ministério da Justiça e com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais. Detém a competência privativa de aplicar sanções, prevalecendo estas as sanções aplicáveis por outras entidades ou órgãos da administração pública

Conselho nacional de proteção de dados e da privacidade[39]

A gênese do Conselho Nacional não sofreu alterações relevantes pela Medida Provisória 869/2018. Tem por atribuições propor diretrizes estratégicas, fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD, além de sugerir ações e realizar debates e audiências públicas e disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população em geral.

Seus membros serão designados pelo Presidente da República, considerada a participação como prestação de serviço público, não remunerada. O mandato dos integrantes será de dois anos, permitida a recondução. Será composto por 23 membros, assim distribuídas as representações: 6 do Poder Executivo federal; 1 do Senado Federal;

---

[36] MP 870/2019, art. 2º

[37] Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Exm/Exm-MP-869-18.pdf>
Acesso em 04 fev. 2019

[38] MP 869/2018, arts. 55-A a 55-K.

[39] Art. 58 e seguintes

1 da Câmara dos Deputados; 1 do Conselho Nacional de Justiça; 1 do Conselho Nacional do Ministério Público; 1 do Comitê Gestor da Internet no Brasil; 4 de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais; 4 de instituições científicas, tecnológicas e de inovação; e 4 de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais.

Considerações Finais

Concluída a apresentação do novo marco legal devemos tecer alguns comentários pontuais, sempre ressaltando esse momento de interseção entre a publicação e a vigência da Lei, entre a criação e a instalação da autoridade e do conselho.

A Medida Provisória 869/2018 deve ser aprovada pelo Congresso Nacional e convertida em lei até abril de 2019.

Na composição do Conselho Nacional de Proteção de Dados causa estranheza a ausência de representação do Conselho Federal da Ordem dos Advogados do Brasil.

É necessário fixar os parâmetros e limites para o consentimento expresso pelo titular dos dados, assim como definir se a autorização deve ser única e definitiva ou será necessária uma autorização para cada tipo de informação.

Outra questão se dirige as sanções: seriam elas cumulativas por informação? Deve ser esclarecida a definição de responsabilidade individual no caso de compartilhamento de informações entre empresas, no que tange a questão da territorialidade devem os dados permanecer no território brasileiro.

Para garantia do cumprimento das regras estabelecidas é indispensável a independência da autoridade nacional. Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a implementação da proteção de dados pessoais depende fortemente do estabelecimento de autoridades de fiscalização e execução da lei com recursos e expertise técnica para exercer seus poderes e tomar decisões de forma objetiva, imparcial e consistente. Há ainda pouca clareza, entretanto, sobre qual seria a natureza de uma autoridade desse tipo no Brasil[40].

Nesse momento de grave crise econômica e financeira pelo qual sobrevive nosso país, um órgão sem dotação orçamentária poderia estimular a gestão punitiva para sua

[40] FGV Direito Rio. Respostas às perguntas-chave sobre os debates públicos do Ministério da Justiça.
Disponível em <https://direitorio.fgv.br/cts/marcocivil-dadospessoais/pergunte> Acesso em 03 fev. 2019

sobrevivência, deixando de exercer seu primordial papel educativo e incentivador de boas práticas.

Fato gravíssimo se relaciona ao surgimento de leis estaduais e municipais sobre proteção de dados, inaugurando a malsinada competência concorrente, que tanta insegurança jurídica causa em matéria ambiental.

Os alicerces da fundação dessa grande obra devem ser firmes por fundamentais para a indispensável segurança jurídica de todos aqueles alcançados pela Lei, que dela se espera seja justa e imune aos nefastos percalços de interpretação. Devemos estar atentos e vigilantes nesse momento crucial de implantação das diretrizes para elaboração da política nacional de proteção de dados. O momento nos reserva uma interrogação, mas nos incentiva a observação atuante. Vamos ao futuro!

IMPACTOS DA LEI DE PROTEÇÃO DE DADOS PARA O EMPRESARIADO

A recém aprovada 'Lei de Proteção de Dados Pessoais' finalmente inseriu o Brasil no cenário mundial de regulação da privacidade dos cidadãos. Estamos diante de uma mudança radical de paradigma, aplicável aos setores público e privado e que alcança todos os setores da economia.

A informação é o ativo mais importante da economia digital, considerada o petróleo da atualidade. Nossos dados - capturados e rentabilizados sem que tenhamos sequer conhecimento - revelam tudo sobre cada um de nós. A mercadoria é você, seus hábitos de consumo, preferência, localização, além de outras várias pegadas digitais que deixamos a cada navegação.

A Lei 13.709/2018 aplica-se a qualquer operação de tratamento de dados pessoais, inclusive os armazenados em meio digital, com o objetivo de assegurar proteção aos direitos fundamentais de liberdade e de privacidade. Funda-se nos princípios da boa fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

A norma protege de forma ampla os dados pessoais, cria direitos do titular, elenca as hipóteses autorizadas para tratamento e prevê responsabilidades e sanções de ordem administrativa e pecuniária de ressarcimento de danos por vazamentos, que podem chegar a 50 milhões de reais, além de outras de ordem civil e penal.

As empresas obrigam-se ainda a eleger agentes de tratamento de dados, responsáveis por adotar medidas de segurança, técnicas e administrativas para proteção dos dados pessoais, de acessos não autorizados e de situações acidentais ou ilícitas. O 'controlador' tomará as decisões relativas ao tratamento, o 'operador' realizará o tratamento em nome do controlador e o 'encarregado' atuará no canal de comunicação entre o controlador e o titular dos dados.

Ocorrendo violação à legislação de proteção de dados pessoais, os agentes de tratamento que causarem danos ao titular - de ordem patrimonial e moral, individual ou coletiva -, serão obrigados a repará-lo.

A adaptação às regras da LPDP pelas micro e pequenas empresas certamente será um grande desafio que exigirá igualmente grande esforço, especialmente para aquelas cuja atividade fim não é o mercado de dados. O modelo de negócio deverá ser totalmente reprogramado, iniciando-se com o mapeamento do uso de dados pessoais. É preciso prever regras da captação, armazenamento e destinação dos dados pessoais, segundo a finalidade do serviço ou negócio. Será necessário registrar as operações de tratamento de dados, adotar ferramentas de controle, governança e gestão de dados, criar políticas

de privacidade e termos de uso, obter autorização do titular, além de medidas de segurança e gestão de risco para casos de incidentes como vazamentos inclusive de seus parceiros e fornecedores.

A criação da indispensável 'Autoridade Nacional de Proteção de Dados', apesar de exaustivamente citada na norma, ainda não ocorreu. E sem a Autoridade a Lei perde eficácia e eficiência, já que é responsável pela regulamentação, fiscalização e aplicação de sanções administrativas. O mesmo ocorre em relação ao 'Conselho Nacional', a quem caberá elaborar a política nacional de proteção de dados e da privacidade.

Diante do absoluto e generalizado desconhecimento sobre se adaptar a Lei, será vital a atuação das associações de classe visando estabelecer regras de segurança da informação, de boas práticas, de governança e de códigos de condutas setorizados, estabelecendo nortes, normas de segurança e padrões técnicos.

A Lei alcança tanto um condomínio que coleta informações cadastrais, biométricas ou faciais dos visitantes, a um consultório médico que armazena dados de saúde, quanto uma empresa de telecomunicação que terceiriza seu atendimento técnico. Todos, sem exceção, serão atingidos pela tsunami regulatória.

O prazo é extremamente curto para as empresas ficarem em conformidade com a Lei de Proteção de Dados Pessoais.

A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

E SUA AGENDA REGULATÓRIA

Cronograma de trabalho da ANPD estabeleceu as fases e temas a serem regulados prioritariamente

O marco legal da privacidade e proteção de dados nacional nasceu com a Lei Geral de Proteção de Dados, que criou a Autoridade Nacional de Proteção de Dados - a ANPD - com o objetivo de proteger os direitos fundamentais de liberdade e privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural.

Com a competência macro de zelar pela proteção de dados pessoais e regulamentar a LGPD, é responsável por fiscalizar e aplicar sanções nos tratamentos realizados em descumprimento à Lei e promover a conhecimento, estudos e cultura da proteção de dados, entre outras atribuições.

Com as dificuldades de ter sido criada sem aumento de despesas o Conselho Diretor formado por cinco membros empossados em novembro, trabalha na organização da estrutura básica de trabalho. O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias.

Sua estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança está disposta no Decreto 10.474/2020.

Sua agenda regulatória foi publicada na semana comemorativa da proteção de dados, através da Portaria 11/2021.

O cronograma de trabalho estabeleceu 10 temas prioritários a serem regulados no prazo de dois anos e classificados em 3 fases:

Na **fase 1** o processo regulatório acontecerá em até 1 ano, com as seguintes metas: publicação do regimento interno e planejamento estratégico da ANPD, a definição de sanções administrativas a infrações, as metodologias que orientarão o cálculo do valor-base das sanções de multa, os prazos de notificação e forma de encaminhamento de Comunicação de incidentes, regulamentar os procedimentos da apresentação de relatório de Impacto à Proteção de Dados Pessoais; a regulamentação de normas diferenciadas para pequenas e médias empresas, startups e pessoas físicas que tratam dados pessoais com fins econômicos.

Na **fase 2** o processo regulatório acontecerá em até 1 ano e 6 meses, abrangendo a transferência internacional de dados, definição e atribuições do encarregado.

A **fase 3** deve acontecer em até 2 anos a elaboração de documento orientador ao público sobre as bases e hipóteses legais de aplicação da LGPD sobre diversos temas, incluindo as hipóteses legais descritas no art. 7º, mas não restritas a ele.

Publicado no meu Linkedin em 2 de fevereiro de 2021

LGPD - TEMAS PENDENTES DE REGULAMENTAÇÃO PELA ANPD

Buscamos na Lei Geral de Proteção de Dados os **temas que carecem de regulamentação** pela Autoridade Nacional de Proteção de Dados e localizamos os seguintes artigos: 9º, 13 - § 3º, 18 - V e § 5º, 19 - § 3º, 27 - parágrafo único, 34 - IV, 48 - § 1º, 53 e § 2º, 58-A - § 3º - I, 55/J - V - X - XIII - XVIII - XX - XXIV e 62.

As **sanções administrativas** a serem definidas por meio de regulamento serão objeto de consulta pública [Art. 53].

Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório *[art. 55/J, § 2º].*

De **forma mandatória** a Autoridade Nacional: **deve estimular** a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais [a*rt. 51*]. Deve emitir opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais [art. 4, § 3º]

As hipóteses de **atuação facultativa** da ANPD estão contidas nos seguintes artigos: 10 - § 3º, 11 - §3º, 12 - § 3º, 19 - §4º, 20 - § 2º, 23 - § 1º, 29, 30, 31, 32, 35 - §§ 2º, 3º e 4º, 38, 40, 41 - § 3º, 46 - § 1º, 48 - §§ 1º e 2º, 50 - § 3º, 52, §§ 3º e 4º, 55/J - V - § 6º.

Importante ressaltar a **competência exclusiva** da Autoridade na aplicação das sanções previstas na LGPD - prevalecendo sobre as competências correlatas de outras entidades ou órgãos da administração pública, no que se refere à proteção de dados pessoais. **Deve atuar como o órgão central de interpretação da Lei** e do estabelecimento de normas e diretrizes para a sua implementação. **Deve** a Autoridade articular sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais [55/K, parágrafo único].

Os primeiros passos dessa longa caminhada começaram a ser trilhados pela ANPD. A disciplina da privacidade e da proteção de dados no Brasil terá um longo caminho em busca de uma mudança cultural até que atinja a esperada maturidade por parte de todo o ecossistema que perpassa a matéria.

Por tais motivos foi muito bem recebida a afirmação do Presidente da ANPD ao **que o principal foco de atuação da ANPD nesse primeiro momento de existência será educativo e não punitivo.**

A LEI DO GOVERNO DIGITAL E A LGPD

A recém editada Lei 14.129/2021 instituiu os princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, sendo aplicáveis:

1. aos órgãos da administração pública direta federal, abrangendo os Poderes Executivo, Judiciário e Legislativo, incluído o Tribunal de Contas da União, e o Ministério Público da União;

2. às entidades da administração pública indireta federal, incluídas as empresas públicas e sociedades de economia mista, suas subsidiárias e controladas, que prestem serviço público, autarquias e fundações públicas; e

3. às administrações diretas e indiretas dos demais entes federados, nos termos dos incisos I e II do caput deste artigo, desde que adotem os comandos desta Lei por meio de atos normativos próprios.

Destacam-se entre os princípios e diretrizes adotados a proteção de dados pessoais e conceitos trazidos pela Lei 13.709/2018 - a Lei Geral de Proteção de Dados.

O compartilhamento de dados pessoais - quando indispensável para a prestação do serviço - deve acontecer em ambiente seguro na atuação integrada entre os órgãos e entidades envolvidas na prestação e no controle de serviços.

As **Plataformas de Governo Digital** devem dispor de ferramentas de transparência e de controle do tratamento de dados pessoais - de forma clara e facilmente acessível - visando permitir ao cidadão o exercício dos direitos previstos na LGPD.

Tais ferramentas devem garantir o acesso as fontes dos dados pessoais, informar a finalidade específica do seu tratamento pelo respectivo órgão ou ente, indicar os órgãos com os quais compartilha dados pessoais, incluindo o histórico de acesso ou o uso compartilhado, excetuadas as hipóteses de não aplicação da LGPD (*inciso III, do art. 4º*).

Deve-se permitido ao cidadão obter da entidade controladora de seus dados, os direitos previstos no art. 18 da LGPD, podendo a Autoridade Nacional de Proteção de Dados editar normas complementares com a finalidade de regulamentar essa requisição.

O conceito de transparência ativa na gestão pública - **positivado na Lei de Acesso à informação** - consiste na liberação do maior número de informações e dados de interesse geral ou coletivo em portal da transparência, independente de solicitação.

A abertura de dados do governo como plataforma se sustenta na disponibilização de qualquer informação de transparência ativa, de livre utilização pela sociedade, observados os princípios da LGPD e os seguintes requisitos: garantia de acesso irrestrito aos dados, os quais devem ser legíveis por máquina e estar disponíveis em formato aberto, respeito à privacidade dos dados pessoais e dos dados sensíveis, intercâmbio de dados entre órgãos e entidades dos diferentes Poderes e esferas da Federação, respeitado o disposto no art. 26 da LGPD.

Os órgãos gestores de dados poderão disponibilizar em transparência ativa dados de pessoas físicas e jurídicas para fins de pesquisa acadêmica e de monitoramento e de avaliação de políticas públicas, desde que anonimizados antes de sua disponibilização os dados protegidos por sigilo ou com restrição de acesso prevista, obedecida a LAI.

Os dados pessoais tratados por mecanismos de interoperabilidade devem seguir as diretrizes da LGPD.