
A ANPD
PONTOS A SEREM REGULADOS!
LGPD
ACADÊMICO

LGPD ACADÊMICO

Esse e-book foi desenvolvido a partir de uma iniciativa (sem fins lucrativos) que começou em agosto/2018, o grupo LGPD Acadêmico, o qual é composto por voluntários do Brasil inteiro, apaixonados pelo mundo da privacidade e com objetivo comum – aprender e compartilhar.

Diante da publicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709 de 2018), que entrará em vigor em 16 de agosto de 2020, foi identificada uma necessidade direta da sociedade civil, entidades privadas e públicas (independente do seu porte), profissionais, dentre outros, por conhecimento e acesso à informações relevantes sobre a temática privacidade e proteção de dados pessoais.

Assim, o LGPD Acadêmico decidiu reunir o conhecimento e experiência prática de cada autor neste material através de uma linguagem simples, evitando-se o famoso "juridiquês", recorrendo a termos técnicos somente quando absolutamente necessário e claro, acessível a todos de maneira gratuita.

Boa Leitura!

Das Autoras

Aline Fuke Fachinetti

Fernanda Maia

Maria Angela Mendes Nascimento Martins

Rachel Gonzaga

Remilina Yun (Remi)

Sumário

INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais ("LGPD") entrará em vigor em 16/08/2020 e, com menos de 6 meses para sua entrada em vigor ainda não temos a Autoridade Nacional de Proteção de Dados ("ANPD") devidamente constituída.

Dentre suas atribuições a ANPD tem a competência de regular sobre privacidade e proteção de dados pessoais e, em razão disto, a LGPD estabelece, em diversos artigos, a necessidade de regulamentação da ANPD para endereçamento de questões específicas (a serem abordadas adiante).

Apesar da LGPD ter uma base sólida e ser uma legislação robusta e que permite o desenvolvimento de um programa de proteção de dados pessoais, os aspectos que restam pendentes de definição, além de gerar insegurança jurídica, deixam, por diversos momentos, as organizações que precisam se adequar em situação de incerteza, aguardando até que tais pontos sejam regulamentados para poderem se sentir seguros do trabalho realizado (ou que façam a sua implementação correndo o risco de incorrer em retrabalho sobre alguns quesitos).

Considerando o cenário acima, entendemos extremamente necessário que as nomeações do Conselho Diretor da ANPD pelo Presidente da República (após devida aprovação pelo Senado Federal, que somente poderá ocorrer após arguição pública) sejam realizadas o quanto antes e que, tão logo seja devidamente constituído, inicie a realização de suas diversas atribuições, inclusive a tão necessária atribuição regulamentar, especialmente considerando que a legislação estabelece que os regulamentos e normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório, o que pode retardar ainda mais a existência de regulamentos e recomendações aprovados.

Necessária, também, a devida finalização da formação do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (que, esperamos, sejam indicados com o mesmo grau de sabedoria e tecnicidade que envolveu a escolha dos que já foram indicados até o momento), já que essa diretoria será essencial para a realização de ações pela ANPD e para, dentre outras relevantes atribuições, disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade no Brasil.

Importante lembrar que além dos pontos específicos que serão aqui abordados, a ANPD tem diversas outras tarefas, listadas no art. 55-J da lei, de forma que precisará também se incumbir de esclarecer conceitos abertos (que, muitas vezes, foram importados de legislações estrangeiras), estabelecer um canal efetivo para comunicação com os titulares e desempenhar suas diversas e importantes funções como a de estabelecer cooperação com autoridades de proteção de dados pessoais de outros países, editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais, editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos,

para que microempresas e empresas de pequeno porte, bem como startups ou empresas de inovação e muitas outras atribuições que dependem desse importante órgão.

Por fim, destacamos que não é recomendado ou salutar que se aguarde esclarecimentos explícitos sobre os temas abaixo para iniciar o programa de compliance, isso porque os problemas atuais existentes e decorrentes da sociedade movida à dados, que a LGPD veio para resolver, já precisam ser endereçados e serão, cada vez mais, exigidos pela sociedade.

A ANPD terá um grande e relevante trabalho a fazer ao ser constituída de forma completa, mas os agentes de tratamentos precisam buscar, desde já, estabelecer um programa de proteção de dados robusto, valendo-se dos fundamentos já existentes na lei e, principalmente, dos princípios trazidos pela LGPD, visando construir uma relação de confianca e transparência com os titulares, mesmo sem todos os pormenores regulamentados.

No presente material, abordaremos brevemente quais são os principais aspectos pendentes de regulamentação e os possíveis impactos da ausência de regulamentação para as organizações e para os titulares de dados pessoais, até para eventualmente apoiar a vindoura ANPD na priorização de suas tarefas regulamentares.

Tratamento de dados pessoais por pessoas de direito privados para fins de segurança pública, defesa nacional, segurança do estado e atividades de investigação e repressão de infrações penais, bem como as opiniões técnicas

Por: Maria Ângela Mendes

A LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais segundo seu art. 4º, inciso III. Logo, nestas hipóteses, o tratamento de dados pessoais não será regido pela LGPD, devendo ser editada legislação específica sobre este tema, conforme determina o §1º do Art. 4º da LGPD.

Contudo, a LGPD estabelece alguns parâmetros para tal situação, dentre eles a vedação, em regra, às pessoas de direito privado no tratamento dos dados pessoais para referidas finalidades. De acordo com o §2º do art. 4º da LGPD, somente em procedimentos sob tutela de pessoa jurídica de direito público, as pessoas de direito privado poderão tratar os dados pessoais nas hipóteses acima.

Além disso, o §4º também do art. 4º da LGPD determina que, em nenhum caso, a totalidade dos dados pessoais poderá ser tratada por pessoa de direito privado, para os fins mencionados, salvo se esta possuir capital integralmente constituído pelo Poder Público.

Posto isto, a LGPD, na parte final do §2º do art. 4º, dispõe que os procedimentos de tratamento de dados para fins de segurança pública e demais matérias acima mencionadas, nas hipóteses permitidas à pessoa de direito privado, deverão ser informadas à ANPD.

Nesse sentido, é de extrema relevância que a ANPD estabeleça o trâmite a ser adotado pelas partes envolvidas, no que diz respeito ao informe específico estipulado pelo citado art. 4º, §2º da LGPD. Para a devida regulamentação, é fundamental que os seguintes aspectos sejam abordados:

- O sujeito que terá o dever de informar à ANPD o procedimento de tratamento de dados pessoais na situação ora especificada: A quem caberá este dever? À pessoa de direito privado ou à pessoa jurídica de direito público?
- Forma que deverá ser adotada para a devida comunicação: Quais serão as formalidades a serem atendidas? Quais informações deverão constar obrigatoriamente do informe? Qual documentação deverá ser apresentada? Qual será o meio oferecido pela ANPD para apresentação do informe?
- Fiscalização do cumprimento das obrigações relativas a este tratamento, estabelecidas pela LGPD e legislação específica: A quais órgãos da ANPD caberá a fiscalização? Quais poderes serão atribuídos a estes órgãos? Quais os limites da autoridade administrativa no exercício desta fiscalização? Quais os meios de defesas àqueles sujeitos à fiscalização?

Nota-se que os pontos acima tratados orientarão os atores envolvidos neste tratamento de dados pessoais, como também estabelecerão algumas premissas para atribuição de responsabilidade no caso de descumprimento da respectiva legislação e regulamentação. Além de que, garantirá o devido processo legal àqueles sujeitos à fiscalização da ANPD, bem como viabilizará a proteção destes em caso de eventual abuso de autoridade.

Outrossim, as atividades de segurança pública, defesa nacional, segurança do Estado e de investigação e repressão de infrações penais compreendem interesse da sociedade que, por sua relevância, se sobrepõem às necessidades individuais. Consequentemente, no exercício destas atividades, direitos individuais, incluindo àqueles relativos ao tratamento de dados pessoais, podem ser mitigados com o fim de garantir necessidades coletivas. Por este motivo é imprescindível que a legislação específica seja editada de modo a permitir, também, a devida regulamentação do tema pela ANPD.

Em complementação ao tema acima, dispõe o art. 4º §3º da LGPD que a ANPD emitirá opiniões técnicas ou recomendações referentes ao tratamento de dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais.

Tais opiniões técnicas ou recomendações, na verdade, caracterizam um parecer técnico. Portanto, trata-se de ato administrativo que compreende um pronunciamento opinativo de órgão ou agente público especializado na matéria sobre determinado conteúdo de ordem técnica.

Como ato administrativo, tais opiniões e recomendações exigem que os seguintes elementos ainda sejam especificados:

- Motivo: situação de fato e de direito que ensejará a emissão da opinião técnica.
- Competência: definição do órgão ou agente público da ANPD responsável pela emissão da opinião técnica.
- Forma: definição dos elementos essenciais do ato, bem como modo de sua materialização e publicização.

Em razão da especificidade da matéria, a opinião técnica ou recomendação emitida não se subordinará à hierarquia administrativa, ou seja, deverá ser observada por todos os órgãos e agentes da ANPD, bem como pelos agentes de tratamento de dados pessoais e titulares.

Nesse sentido, não existindo regulamentação que delimite a atuação da ANPD, haverá dificuldade no controle de casos de abuso de autoridade, má-fé ou erro grosseiro.

Além disso, também haverá repercussão na esfera jurídica dos titulares, uma vez que o tratamento de dados pessoais estará relacionado a atividades que podem importar na mitigação de seus direitos, devido à aplicação do princípio da supremacia do interesse público, como acima exposto.

Regulamentação sobre o uso compartilhado de dados pessoais sensíveis com objetivo de obtenção de vantagem econômica (poderá ser regulado)

Por: Aline F. Fachinetti

Durante as discussões legislativas envolvendo a regulamentação de proteção de dados pessoais no Brasil, um dos pontos amplamente debatidos foi o compartilhamento de dados pessoais (especialmente considerando a necessidade de se garantir a autodeterminação informativa[1] do titular, que é um dos fundamentos da LGPD), sendo definida a obrigatoriedade do controlador facilitar o acesso ao titular acerca do uso compartilhado de seus dados e a sua finalidade. Além do direito de acesso mencionado, definiu-se que normas complementares poderão ser estabelecidas pela ANPD para as atividades de comunicação e de uso compartilhado de dados pessoais (art. 30, LGPD).

Maior preocupação ainda surgiu para endereçar a comunicação e uso compartilhado dos dados considerados *sensíveis* (isto é, todo *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*).

Como esses dados notadamente exigem maior grau de zelo em seu tratamento, considerando que seu conteúdo, mais vulnerável, usualmente oferece maior potencial de lesividade ou discriminação ao titular, foi necessário traçar regras mais rígidas para o seu compartilhamento, especialmente quando o objetivo desse compartilhamento consistir na obtenção de vantagem de cunho econômico.

Assim, o art. 11, § 3º da LGPD estabeleceu que a comunicação ou o uso compartilhado desses dados entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da ANPD, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

Importante destacar que, não obstante o que vier a ser regulamentado (ou vedado) pela ANPD, a redação atual da LGPD já veda expressamente o compartilhamento de dados pessoais referentes à saúde com objetivo de obter vantagem econômica (exceto nas hipóteses, em benefício dos interesses dos titulares, relacionadas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluindo serviços auxiliares de diagnose e terapia, sendo também será permitido o compartilhamento de dados de saúde para realizar a portabilidade dos dados quando solicitada pelo titular, e para permitir as transações financeiras e administrativas relacionadas aos referidos serviços). Há, também, restrição expressa na lei ao compartilhamento com terceiros de dados pessoais que órgãos de pesquisa acessem durante estudos em saúde pública.

Essas provisões específicas para dados de saúde foram motivadas, principalmente, pelo fato de que o uso comercial de dados pessoais de saúde poderia orientar a venda de

[1] Autodeterminação informativa significa dar o controle dos dados pessoais ao seu titular, ou seja, o titular deverá ter meios (direitos) de controlar o uso e compartilhamento de seus dados pessoais.

produtos e serviços, impactar relações entre os titulares e possíveis empregadores, planos de saúde e até mesmo agências de adoção, por exemplo.

No que tange ao compartilhamento de dados, conforme abordaremos com mais detalhes adiante, também serão objeto de regulamentação questões relativas à comunicação e uso compartilhados de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado.

Percebe-se, portanto, que a ANPD terá um papel primordial na regulamentação desse aspecto da lei, de forma que os controladores deverão acompanhar as atividades da autoridade, bem como regulamentações específicas setoriais para balizar o uso compartilhado de dados pessoais.

Regulamento sobre segurança da informação na realização de estudos em saúde pública e regulamento quanto o acesso aos dados pessoais sobre saúde para fins de pesquisa (art. 13, caput e §3º.) e acesso dos órgãos de pesquisa a dados de saúde

Por: Aline F. Fachinetti

A LGPD estabelece que, quando órgãos de pesquisa estiverem realizando estudos envolvendo saúde pública e tiverem acesso a bases de dados pessoais, deverão realizar o tratamento exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas, devendo os dados serem mantidos em ambiente controlado e seguro.

Para tanto, deverão atuar conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. A necessidade da anonimização, sempre que possível, também é ressaltada no art. 7º, IV, da lei.

O parágrafo 3º do art. 13 da LGPD incumbiu à ANPD e às autoridades de saúde e sanitárias, no âmbito de suas competências, nesses casos, o dever de regulamentar o acesso aos dados pelos órgãos de pesquisa.

Essa previsão legal enaltece a necessidade da ANPD, quando devidamente formada, exercer a sua tão necessária competência de articulação com as autoridades reguladoras públicas para exercer suas competências em setores específicos, como prevê o art. 55º-J, XXIII. É primordial que o relacionamento entre a ANPD e tais entidades seja feito forma coordenada, visando assegurar o cumprimento de suas atribuições com a maior eficiência, bem como promover o adequado funcionamento dos setores regulados, devendo ser estabelecido um fórum permanente de comunicação entre os entes, conforme estabelece a lei.

Padrões e técnicas de anonimização

Por: Maria Ângela Mendes

Para fins de aplicação da LGPD, segundo dispõe o art. 12 da lei, em regra, os dados anonimizados não são considerados dados pessoais. Dado anonimizado é aquele relativo a titular que não pode ser identificado.

Assim, para que o dado pessoal se torne anonimizado, ele deve ser submetido a adequado processo de anonimização. Ou seja, é necessária a utilização de meios técnicos razoáveis, disponíveis no momento do tratamento, a fim de que o dado perca a possibilidade de associação, direta ou indireta, ao titular.

Nesse sentido, a LGPD em seu art. 12 § 3º estabelece que a ANPD poderá dispor sobre os padrões e técnicas utilizados em processos de anonimização, afinal, existem diferentes técnicas e práticas de anonimização, tais como a generalização e a aleatorização, cada uma com suas especificidades, aplicabilidade e efeitos.

Consequentemente, é necessário que, através da estipulação de padrões e técnicas, seja formulado um processo eficaz que garanta a anonimização, bem como minimize o risco residual de identificação do titular. Assim, ao regular o tema, a ANPD terá que definir requisitos e objetivos claros e determinados, de forma a atender aos seguintes critérios, extraídos da experiência europeia no assunto[2]:

- **Identificação: É possível identificar o titular?**

Deve-se considerar a possibilidade de isolar alguns ou todos os registros que identifiquem uma pessoa num conjunto de dados.

- **Possibilidade de ligação: É possível estabelecer ligação entre registros relativos àquele titular?**

Deve-se considerar a capacidade de ligar pelo menos dois registros sobre o mesmo titular ou um grupo de pessoas, tanto na mesma base de dados como em duas bases de dados diferentes.

- **Inferência: Podem ser deduzidas informações relativas a um titular?**

Deve-se considerar a possibilidade de deduzir o valor de um atributo a partir dos valores de um conjunto de outros atributos.

Nota-se, portanto, que estabelecer um processo de anonimização adequado e eficaz, com ferramentas possíveis de anonimização, não é uma tarefa simples.

[2] Grupo de Trabalho de Proteção de Dados do Artigo 29º da Diretiva 95/46/CE.Parecer 05/2014 sobre técnicas de anonimização, adotado em 10 de abril de 2014. Disponível em: https://www.gpdp.gov.mo/uploadfile/2016/0831/20160831042518381.pdf

Como mencionado, uma vez que não haja possibilidade de associação, direta ou indireta, a um indivíduo, os dados serão anonimizados não serão considerados dados pessoais para fins da LGPD, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Logo, em regra, não caberá qualquer proteção como a aplicada aos dados considerados pessoais. Por essa razão é de fundamental importância que exista um processo de anonimização eficiente, que viabilize a conservação dos dados sem permitir a reidentificação do respectivo titular.

Isto posto, a regulamentação deve ser editada justamente para auxiliar as organizações na construção de um processo de anonimização eficaz, bem como garantir aos titulares a proteção de seus dados pessoais.

Portabilidade

Por: Rachel Gonzaga

O artigo 18, V da LGPD concede ao titular o direito de solicitar a portabilidade de seus dados,nos termos de regulamentação da ANPD, observados os segredos comercial e industrial:

> *Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:*
>
> *V - 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;*

Esse direito busca garantir, além da efetivação da autodeterminação informacional, que o titular não fique preso a determinado fornecedor ou que sofra custos altos de troca (que decorreriam da perda dos dados existentes no fornecedor anterior)[3].

Nesse sentido, para que o titular possa exercer tal direito, é necessária à sua devida regulamentação, para que as organizações se preparem para o atendimento deste direito, com o devido conhecimento do âmbito de aplicação da portabilidade e a forma de operacionalização.

Para tanto, devemos considerar alguns aspectos sobre a portabilidade que impactam diretamente na forma como as organizações deverão se preparar e na eficácia da interoperabilidade dos dados entre os controladores:

- Em qual formato os dados pessoais devem ser transmitidos?
- Haverá um padrão de interoperabilidade (razoável e economicamente viável para diversos *players*)?
- Quais dados pessoais estão sujeitos à portabilidade? Apenas os dados pessoais fornecidos diretamente pelo titular, como estabelece o GDPR? Os dados observados a partir do uso de tecnologias, como, por exemplo, o cookie de tracking? Dados inferidos ou derivados, como por exemplo, o resultado da análise de seus dados[4]?
- Dados pseudoanonimizados também seja objeto de portabilidade?
- Os dados tratados sob qualquer base legal serão objeto de portabilidade?
- E se houver dados de terceiros?

[3] Carl Shapiro and Hal R. Varian, Information Rules, A strategic guide to the network economy (1999) Boston, MA.

[4] Em ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on the right to data portability., o WP29 estabeleceu que todos os dados gerados de forma ativa e consciente pelo titular estariam abrangidos, excluindo apenas os dados inferidos ou derivados pelo controlador por seus instrumentos (exceto nos casos de decisão automatizadas, que, expressamente, estão incluídas no GDPR no direito à portabilidade).

- Como afastar a responsabilidade do Controlador sob o tratamento posterior destes dados por terceiros?
- Como será definido o limite do segredo comercial e industrial?
- Qual o prazo para cumprimento do pedido?

Note-se que as definições acima, gerarão para as empresas mudanças internas, tanto de tecnologia e forma de armazenamento de dados, quanto de processos e procedimentos internos, razão pela qual, a demora na regulamentação poderá ensejar em dificuldades de adequação e possibilidade de cumprimento da obrigação de garantir o exercício deste direito pelos titulares.

É de se destacar que o direito a portabilidade de dados pessoais é algo inovador nas legislações de proteção de dados pessoais, tendo sido inclusive uma das inovações trazidas pelo *General Data Protection Regulation* nº 2016/679 da União Europeia ("GDPR") em relação a Diretiva nº 1995/46, sendo que na União Europeia o antigo *Article 29 Working Party* publicou *Guidelines on the right to data portability adotada em 13/12/2016*, ratificada pelo atual *European Data Protection Board*, em que definiu todos os parâmetros para o exercício do direto à portabilidade, bem como seus limites.

Durante a ausência de previsão específica sobre a portabilidade, é de se esperar que se aplique as regras previstas para direito de acesso (pois, conforme se verá adiante, existe certa proximidade entre os dois direitos)[5]. No entanto, é de suma importância que as complexas questões acima sejam endereçadas pela ANPD para que o direito à portabilidade seja implementado pelas organizações de forma efetiva (e razoável) e para que os titulares possam exercer esse direito sem entraves.

[5] FRAZÃO, Ana. Direitos básicos dos titulares de dados pessoais. Revista do Advogado (AASP), São Paulo, n. 144, p. 33 – 46, 2020.

Cópia eletrônica integral de dados pessoais e Prazos sobre fornecimento de informações solicitadas pelo titular

Por: Fernanda Maia

Em relação aos itens pendentes de regulamentação pela ANPD, um dos que trazem maior preocupação é a efetivação dos direitos dos titulares.

Dada a importância do tema, a LGPD dedica o Capítulo III ao regime dos direitos dos titulares e elenca, em seu artigo 18, os principais direitos que os titulares dos dados pessoais passarão a ter com a LGPD, de forma que os controladores precisam ter meios e mecanismos adequados para cumprir esses direitos.

Sobre o direito de confirmação de existência e direito de acesso, o artigo 19 versa:

> *Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular:*
>
> *I - em formato simplificado, imediatamente; ou*
> *II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.*
> *§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.*
> *§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:*
> *I - por meio eletrônico, seguro e idôneo para esse fim; ou*
> *II - sob forma impressa.*
>
> *§ 3º Quando o tratamento tiver origem no consentimento do titular ou em contrato, o titular poderá solicitar cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.*
>
> *§ 4º A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.*

O parágrafo 3º cita que a cópia eletrônica integral dos dados pessoais do titular será regulamentada pela ANPD e o parágrafo 4º cita que a ANPD poderá *"dispor de forma diferenciada acerca dos prazos"*. Esses dois cenários são exemplos de medidas que diversas empresas estão tomando e que podem precisar de reformulação após essas diretrizes. Note-se que para atender tais direitos é necessária a contratação de tecnologias, reformulação de processos internos e, caso haja alterações ajustes podem ser necessários como decorrência da regulamentação dessa questão.

Além dos mencionados problemas da ausência imediata dessas regulamentações, o conteúdo em si delas é problemático. Empresas como hospitais, plano de saúde, multinacionais que realizam operações em sua maioria B2C poderão sofrer enormes impactos ao tentar cumprir o prazo de 15 dias para uma entrega "completa" dos dados, considerando as diversas medidas – anteriores à entrega dos dados pessoais – que deverão ser adotadas para que o envio desses dados não configure em vazamento de dados pessoais (por exemplo, ao solicitar acesso completo aos seus dados, aquele titular deverá ser identificado pela empresa como sendo de fato o "dono" dos dados discutidos em questão, de forma que tais medidas analíticas poderão impactar o prazo de entrega).

Nesse sentido, até o GPDR possui um prazo mais razoável de resposta. Em linhas gerais, pela regulamentação europeia, o controlador deve atender a uma solicitação sem demora injustificada e, o mais tardar, um mês após o recebimento da solicitação. Ainda, é possível estender o tempo de resposta por mais 2 meses se a solicitação for complexa ou se o controlador receber diversas solicitações do titular.

Diante do cenário apresentado, cabe à ANPD regulamentar os pontos relativos aos direitos dos titulares, em especial ao prazo de entrega e os meios dele, para as empresas possam, além de se adequar, orçar os valores que essas ações terão e conseguir, em um tempo hábil, testar os seus sistemas e procedimentos envolvendo o exercício desse direito para garantir a sua efetividade.

Normas complementares para a comunicação e uso compartilhados de dados pela administração pública

Por: Maria Ângela Mendes

A LGPD dedica um capítulo exclusivo ao tratamento de dados pessoais pelo Poder Público. Trata-se do Capítulo IV, o qual estabelece, em suma, que o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas na Lei de Acesso à Informação deverá ser realizado para o atendimento de sua finalidade pública, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, observadas certas condições.

No que tange ao uso compartilhado de dados pessoais pelo Poder Público, dispõe o §1º do art. 26 da LGPD que é vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso.

Contudo, o mesmo §1º do art. 26 da LGPD prevê algumas exceções, de modo a permitir o compartilhamento de dados pela Administração Pública com entidades privadas nas seguintes situações:

- Execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado;
- Dados forem acessíveis publicamente;
- Houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; e
- Transferência dos dados com o objetivo exclusivo de prever fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

Portanto, o acesso a base de dados da Administração Pública pelas empresas e organizações que destes necessitam para a execução de suas atividades fundamenta-se no art. 26 § 1º da LGPD.

Não obstante, o "caput" do art. 27 da LGPD determina dois requisitos para a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado: (i) a ANPD deverá ser informada sobre o uso compartilhado; e (ii) a necessidade de consentimento do titular.

Ainda, o art. 27 da LGPD relaciona em seus incisos algumas exceções ao seu caput, dentre elas, as exceções constantes do §1º do art. 26 acima tratado, quais sejam, as hipóteses em que o compartilhamento de dados pessoais pelo Poder Público a entidades privadas é permitido.

Isto posto, depreende-se da leitura do art. 27 da LGPD que, quando permitido o compartilhamento de banco de dados pelo Poder Público a entidades privadas, não será necessário o consentimento do titular, tampouco a ANPD deverá ser informada sobre o uso compartilhado.

Assim, ao compararmos o art. 26 com o art. 27 da LGPD, notamos uma aparente incompatibilidade, haja vista que o art. 26 estabelece como regra geral a vedação ao Poder Público de transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, enquanto o art. 27 dispõe sobre os requisitos para o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado.

Nota-se que, apesar de utilizarem expressões diferentes ("Poder Público X "´pessoa jurídica de direito público" e "entidades privadas X pessoa de direito privado"), ambos artigos convergem para o mesmo tema, o uso compartilhado de dados pessoais pelo Poder Público. Logo, a interpretação em conjunto destes artigos pode ocasionar insegurança jurídica às empresas e organizações quanto à possibilidade ou não de utilizar banco de dados do Poder Público.

Uma possível solução para este impasse é o art. 30 da LGPD que autoriza a ANPD estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

Fazendo uma analogia ao direito tributário, segundo art. 100 do Código Tributário, normas complementares são atos normativos expedidos por autoridades administrativas, decisões administrativas, práticas reiteradas das autoridades administrativas e convênios que entre si celebram os entes da Federação. Tais normas poderão exercer o papel de orientar de forma adequada o cumprimento da LGPD no que diz respeito ao uso compartilhado de dados pessoais pelo Poder Público, elucidando o sentido que referidos dispositivos legais não conseguiram delinear de modo preciso e contundente.

Transferência Internacional

Por: Rachel Gonzaga

A LGPD apresenta regras para que a Transferência Internacional de Dados Pessoais seja legítima, conforme descrito nos artigos 33 e seguintes da LGPD:

> *Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:*
> *I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;*
> *II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:*
> *a) cláusulas contratuais específicas para determinada transferência;*
> *b) cláusulas-padrão contratuais;*
> *c) normas corporativas globais;*
> *d) selos, certificados e códigos de conduta regularmente emitidos;*
> *III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;*
> *(...)*
> *V - quando a autoridade nacional autorizar a transferência;*
> *(...)*
> *Parágrafo único. Para os fins do inciso I deste artigo, as 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) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.*
>
> *Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:*
> *(...)*
> *Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência,*

> *normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.*
> *(...).*
> *Art. 36. As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional.*

Note-se que, dentre as 09 hipóteses autorizativas para a transferência internacional de dados pessoais, 06 delas dependem de regulamentação pela ANPD.

Assim, se não houver a devida regulação, a LGPD entrará em vigor com hipóteses autorizativas que muitas vezes, ou não são aplicáveis a determinadas transferências, ou são inviáveis operacionalmente, como pode ser o caso da obtenção do consentimento expresso do titular.

Ou seja, na prática, as organizações não possuem todos os meios necessários a possibilitar que haja a transferência internacional de dados de forma efetiva, o que, em última instância, pode até ferir a observância de um dos fundamentos da LGPD, o desenvolvimento econômico e tecnológico e a inovação.

Isto porque, a ausência de regulamentação destes pontos pode ser bastante sensível não apenas para as organizações que dependem da transferência internacional de dados pessoais para suas operações, mas para a própria evolução da economia digital.

Tal fato é tão relevante que a *Organisation for Economic Co-operation and Development* ("OECD") em suas *Guidelines on the Protection of Privacy and Transborder Flow of Personal Data* trouxe como princípios básicos a garantia de facilitação da transferência internacional de dados pessoais observadas as garantias de sua efetiva proteção, a saber:

> *PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS*
> *15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.*
> *16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.*
> *17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.*

> *18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.*

Além destes princípios a OECD publicou em abril de 1985 a *Declaration on Transborder Data Flows* em que declara a importância da transferência de dados entre países diversos para o desenvolvimento econômico e tecnológico e a necessidade dos países membros em possibilitar este fluxo de dados de forma facilitada observadas as garantias de proteção dos dados.

No mesmo sentido se posicionou o *Council of Europe* na *Convention 108* em seu artigo 14 e o GDPR em seus artigos 44 e seguintes.

Assim, verifica-se que o Brasil, ao não possuir a devida regulamentação de pontos essenciais para a viabilidade jurídica de transferências internacionais de dados pessoais está na contramão das regulações de proteção de dados pessoais e sujeito a impactos econômicos em razão disto.

Sob o ponto de vista das organizações, a ausência de tal regulamentação gera enorme insegurança jurídica pois, muitas organizações ou realizam operações internacionais, ou simplesmente possuem dados armazenados em outros países e dependem da transferência internacional para a manutenção de seus negócios e operações.

Ademais, dos pontos que demandam regulamentação, sua aplicação, à exceção da decisão de países adequados demandam tempo de implementação e mudança de processos, procedimentos e documentos.

Para as organizações que forem adotar as **Cláusulas contratuais padrão, Cláusulas especificas ou Normas corporativas globais**, será necessária adequação de procedimentos e adequação de todos os contratos e instrumentos cujo objeto envolva o fluxo internacional de dados pessoais, ações que muitas vezes demandam tempo, negociação e organização de processos dentro das organizações, o que por sua vez, demandam tempo, esforços e recursos financeiros.

Já aquelas que pretendem utilizar-se de **certificações, selos ou códigos de conduta**, será necessário obter tais certificados, selos e códigos de condutas e ainda, após a devida regulamentação, demandará das empresas certificadoras o tempo necessário para a estruturação de como serão conferidos tais certificados, selos e códigos de conduta.

Diante disso, entendemos que a regulamentação destes itens é medida urgente e imprescindível para a segurança jurídica das organizações que no tratamento de dados pessoais envolva o fluxo internacional de dados pessoais e para a efetiva proteção dos dados pessoais, uma vez que tais hipóteses não apenas autorizam a transferência internacional de dados pessoais, mas provêm a adequação da estrutura de proteção destes dados.

Regulamentação do relatório de impacto a proteção de dados pessoais
Por: Remi Yun

Ao contrário do GDPR, a LGPD não dispôs sobre alguns aspectos relevantes na elaboração do Relatório de Impacto à Proteção de Dados Pessoais – "RIPD", incumbindo assim, a responsabilidade para a ANPD em regular e/ou preencher essas lacunas.

Essas lacunas seguem tanto na própria definição do art. 5º, inciso XVII da LGPD, como em outros pontos que serão apresentados a seguir.

Na sua definição, o RIPD é referenciado como uma "documentação" do controlador, restando ausente qualquer orientação ou direcionamento sobre seu formato ora "*template*", cabendo assim à ANPD regular sobre tal tema, a fim de assegurar maior segurança jurídica para as organizações que exercem o papel de controlador, uma vez que sua conformidade será atestada quando requerida pela ANPD (além de facilitar a atuação da própria ANPD durante a análise dos relatórios, caso sejam realizados de forma homogênea ou tenham um padrão mínimo a ser seguido).

Sabemos hoje que, na União Europeia, as organizações submetidas ao GDPR tem apresentado o *Data Protection Impact Assessment* - DPIA no formato de tabela (excel ou word), petição inicial, resposta a notificação, entre outros, ou seja, sem uma padronização adequada.

Outro ponto a ser regulamentado está relacionado ao próprio conteúdo do RIPD, já que no artigo supracitado faz referência apenas ao conteúdo mínimo, porém sem maiores detalhamentos:

- Descrição dos processos de tratamento de dados pessoais;
- Identificar riscos que impactem as liberdades civis e aos direitos fundamentais;
- Identificar as medidas, salvaguardas e mecanismos de mitigação de risco adotados;

Quanto à descrição dos processos de tratamento, a ANPD precisa determinar o nível de detalhamento a ser apresentado.

Em relação aos riscos, a ANPD precisa determinar qual o nível de risco a ser considerado à luz do RIPD, pois todo risco tem atrelado à si a sua probabilidade de ocorrência e seu nível de impacto, independentemente de ser em relação às liberdades civis e aos direitos fundamentais, não restando dúvidas sobre a necessidade de sua regulamentação.

Na Europa, o GDPR determinou em seu dispositivo como requisitado para o DPIA "*qualquer tipo de processamento com probabilidade de resultar em alto risc*o", no entanto, resta questionar o conceito de "*alto risco*", ou seja, qual o parâmetro a ser considerado, uma vez que cada organização e/ou segmento tem sua metodologia e critério

próprio? O que é alto risco para um pode não ser para outro, já que organizações podem ter apetite de risco diverso.

Além disso, o GDPR, taxativamente estabelece alguns tipos de tratamento que exigem a elaboração do DPIA. No entanto, de forma diversa, a LGPD não fez tal especificação, gerando mais uma insegurança jurídica, pois, cumulada com a ausência de definições e/ou conceito sobre a criticidade de riscos *versus* impacto, as organizações, para buscar sua conformidade, poderão adotar linhas de frentes distintas, uma conservadora, elaborando RIPD para todo e qualquer tipo de tratamento ou independente, criando premissas próprias através de *benchmarking* com mercado interno e/ou com práticas das autoridades europeias.

Adicionalmente, cabe a ANPD regulamentar ou não sobre uma boa prática apresentada pelo GDPR frente a consulta prévia para tratamento de dados, cujo DPIA resulta em alto risco. E, se assim o decidir fazer, estabelecer parâmetros para tanto, já considerando as lições aprendidas pelas autoridades europeias (na Europa, percebeu-se que diversos DPIAs que não dependiam de submissão prévia eram submetidos às autoridades, mergulhando-as em trabalho desnecessário, o que culminou na elaboração de listas por diversas autoridades sobre atividades que dispensam a elaboração de DPIA).

Regulamentação de padrões de interoperabilidade
Por: Aline F. Fachinetti

O artigo 40 da LGPD prevê a faculdade da ANPD dispor, dentre outros aspectos, sobre os padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança.

Como já mencionado no item que discorre sobre a portabilidade de dados pessoais, a atuação da ANPD nesse aspecto é extremamente relevante para que se estabeleça regras mínimas, de ampla aceitação, às empresas, viabilizando o cumprimento dos deveres dos agentes de tratamento, bem como o exercício de direitos pelos titulares de dados pessoais, como o direito à portabilidade, previsto no art. 18, inciso V da lei.

Como se denota, a própria eficácia desse direito depende da resolução pragmática da interoperabilidade com o novo receptor dos dados pessoais, ou seja, à funcionalidade dos sistemas de informação para trocar dados e permitir o compartilhamento de informações, em formato estruturado. Considerando que os Controladores serão solicitados à realizar a portabilidade (além de existir a possibilidade de receberem dados de outros controladores, à pedido dos titulares), é de suma importância, para que se permita que essa "troca informacional" ocorra em larga escala e baixo custo, que se adote critérios uniformes (e, claro, razoáveis para todos os agentes envolvidos nesse ecossistema).

Na Europa, entende-se que os dados pessoais devem ser fornecidos em formato que seja (i) estruturado; (ii) comumente utilizado; e (iii) legível por máquina. Ainda, o GDPR indica que interoperabilidade não necessariamente significa "compatibilidade", não sendo razoável se exigir que uma empresa utilize determinado sistema.

Ainda no contexto Europeu, sobre a questão de formatos para interoperabilidade, o *Article 29 Working Party* nas *Guidelines on the right to data portability* entendeu que cada setor poderá ter formados diferentes, adequados às especificidades do seu ramo/setor.

Existem outros aspectos que poderão ser esclarecidos pela ANDP durante a sua elucidação sobre os padrões de interoperabilidade, por exemplo, o alcance do exercício desses direitos (ou seja, qual a limitação dos dados a serem fornecidos/portados - se se limitam apenas ao que foi fornecido pelo titular, à exemplo do que estabelece o art. 20 da GDPR), bem como a elucidação de até que ponto uma empresa poderia arguir que determinadas informações seriam segredo industrial ou comercial (isto é, orientações gerais sobre como "traçar a régua" dentre o que é revelável e o que é classificado como secreto).

Tempo de guarda dos registros de tratamento de dados pessoais
Por: Remi Yun

Esse tema é um dos pontos que mais gera discussão dentro das organizações, pois, além das particularidades e necessidade de cada negócio, segmento, setor, entre outros, nos deparamos com controvérsias legais dentro do ordenamento jurídico brasileiro, pois temos Marco Civil da Internet, Lei de Acesso à Informação, dentre outras e, agora, a LGPD.

Na LGPD, por entender sobre as particularidades decorrentes de cada tratamento de dados pessoais, não se estabeleceu um prazo ou período de guarda dos dados pessoais pelos agentes de tratamento, já que inexiste uma solução ou resposta pronta e padronizada ao se falar em dados pessoais. No entanto cabe à ANPD regular sobre esse ponto com o objetivo de entender suas expectativas quanto ao tempo de guarda à luz da LGPD.

Importante ressaltar que se considerarmos o princípio da necessidade ou minimização, a LGPD busca que os tratamentos de dados pessoais sejam realizados com base naquilo que é realmente necessário, colando em xeque o volume de dados pessoais, e, consequentemente seu tempo de retenção.

No mesmo sentido, segundo Comissão Europeia, *"os dados devem ser conservados durante o mínimo de tempo possível"*. Esse mínimo deve ser estabelecido levando em conta a finalidade do seu tratamento dos dados pessoais, bem como as eventuais obrigações legais, interesse público, entre outros, desde que sejam adotadas medidas técnicas e organizativas adequadas.

Além disso, estabelecer uma política de prazo de retenção considerando os princípios mencionados e executá-la de forma efetiva pode gerar verdadeiro ganho operacional e redução de riscos ao se reduzir a base de dados existentes nas organizações.

Indicação e função do encarregado de proteção de dados pessoais
Por: Remi Yun

O encarregado de proteção de dados pessoais, popularmente conhecido como *Data Protection Officer* – DPO, é uma figura estabelecida na LGPD, o qual terá um papel de guardião sobre aspectos da proteção de dados pessoais dentro das organizações, sendo também aquele que conduzirá toda e qualquer comunicação junto aos seus titulares de dados e à ANPD.

Ao contrário da GDPR, a LGPD não especificou em quais condições o encarregado deve ser indicado, por exemplo, setor, atividade principal, escala de dados, tipos de dados, finalidade de tratamento ou até mesmo à possibilidade da não indicações em situações excepcionais como dispõe o artigo 41,§ 3º da LGPD.

Essa lacuna caberá à ANPD regular (espera-se, com urgência), pois, na conjuntura atual, até mesmo o controlador de uma empresa de pequeno porte (ex. padaria) deve adotar as mesmas exigências direcionadas à multinacionais pela lei. Dessa forma, consideramos importante que o nível de criticidade e complexidade sejam considerados quando da definição da estrutura e requisitos na indicação do encarregado de proteção de dados pessoais.

Padrões técnicos mínimos de segurança e boas práticas
Por: Remi Yun

Neste tópico, resta destacar sobre a possiblidade da ANPD regulamentar e criar orientações quanto às medidas de segurança, técnicas e administrativas que sejam minimamente necessárias e esperadas para assegurar os dados pessoais dos titulares de dados, bem como atender à conformidade das obrigações previstas na LGPD.

Atualmente existem diversas boas práticas tais como ISO 27001, ISO 27701, COBIT, ITIL e outros frameworks para segurança de informação, enquanto isso para boas práticas de governança temos as orientações e cadernos do Instituto Brasileiro Governança Corporativa - IBGC, metodologias de gestão de riscos como COSO ERM e ferramentas para identificação de riscos para preencher as lacunas existentes. A possibilidade de regulação segue no artigo 46, § 1º da LGPD, sendo importante que a ANPD, para elaborar as suas orientações, considere a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios da LGPD.

Prazo de notificação de incidentes de segurança
Por: Remi Yun

A LGPD estabelece que o controlador deverá comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, visando, além de permitir que tenham o devido conhecimento do que acontece com seus dados pessoais, mitigar riscos àqueles que tiveram seus dados expostos.

No entanto, esse é um ponto que a ANPD precisa regulamentar com urgência, pois no artigo 48, § 1º da LGPD determina que caso o controlador identifique um incidente de segurança que possa acarretar risco ou dano relevante aos titulares, a sua comunicação deve ser feita em "*prazo razoável*".

Se considerarmos seu conceito, a razoabilidade está atrelada aos sinônimos, aceitável, admissível, racional, entre outros, levando para interpretações diversas e até mesmo certo subjetivismo, reforçando assim, a urgência na adoção de um prazo específico, como foi, por exemplo, estabelecido no GDPR (que estabelece que a notificação deve ser realizada sem demora injustificada, mas o mais tardar 72 horas contadas do conhecimento do fato e, se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso).

A ausência de regulamentação nesse sentido é um risco para os próprios titulares de dados pessoais e faz com que as organizações impactadas pela LGPD tenham incertezas quando da elaboração de seus planos de respostas à incidentes e procedimentos correlatos.

Regulamento sobre sanções administrativas com metodologia de cálculo do valor da multa e regras de multa diária e simples

Por: Aline F. Fachinetti

Como se sabe, uma das sanções que poderá ser aplicada pela ANPD é a de multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada a 50 milhões de reais por infração.

No entanto, para definir o valor exato da multa, a ANPD deverá, antes de sancionar os agentes de tratamento com tal penalidade, preparar um regulamento de sanções e metodologias correspondentes que orientarão o cálculo do valor-base das sanções de multa, por força do art. 53 da LGPD. Dentre outros aspectos, o regulamento deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Para o cálculo da multa simples, a ANPD poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.

Sobre as metodologias a serem estabelecidas pela ANPD, estas devem ser previamente publicadas (para devida ciência dos agentes de tratamento) e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos na LGPD.

Sobre as condições para a adoção entre multa simples ou diárias, historicamente no Brasil multas diárias são utilizadas para garantir o cumprimento de uma decisão anterior, mas, as especificidades para tanto deverão ser regulamentadas pela autoridade, assim que constituída.

Analisando o direito comparado, destaca-se que a GDPR traz dispositivo semelhante, ao definir, em seu artigo 70 (1), (k), que a *European Data Protection Board* ("EDPB") possui competência para emitir guidelines, recomendações e boas práticas para as autoridades relativas à aplicação das medidas das autoridades e à fixação de multas administrativas, o que resultou na publicação das *Guidelines on the application and setting of administrative fine*. No entanto, como a metodologia de cálculo de multa não foi ainda abordada de forma específica pela EDPB, algumas autoridades emitiram regulamentos próprios para tal cálculo (por exemplo, a autoridade alemã e holandesa) enquanto aguardam um posicionamento mais específico da EDPB sobre a dosimetria dessa penalidade pecuniária.

Apenas a título de conhecimento, a metodologia alemã consiste em 5 passos para o cálculo, que incluem (i) classificar a entidade violadora, definindo uma categoria para a

entidade, de acordo com o seu faturamento anual/tamanho; (ii) definir o volume médio de faturamento anual da entidade violadora; (iii) definir valor diário da multa, determinando um valor diário de multa dividindo o faturamento médio anual por 360 dias como base para o cálculo da multa real; (iv) avaliar a gravidade da infração, dentre gravidade baixa, média, grave e muito grave, com cada grau possuindo multiplicadores que são aplicados ao valor diário de multa definido na etapa anterior; e (v) ajustar às circunstâncias especiais, acordo com a dosimetria estabelecida na GDPR e também em casos específicos, como insolvência ou duração do processo.

Regulamento específico para tratamento de dados pela União para cumprimento da Lei de diretrizes e Bases da educação infantil e Sistema nacional de avaliação da educação superior

Por: Aline F. Fachinetti

A LGPD estabelece, em seu art. 62, que a ANPD e o INEP (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira) deverão editar regulamento específico sobre o acesso a dados tratados pela União para o cumprimento da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), que estabelece que a União terá acesso a todos os dados e informações necessários de todos os estabelecimentos e órgãos educacionais para cumprir algumas de suas atribuições relativas à educação nacional (incluindo, por exemplo, o ENEM) e aos dados pessoais referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004.

Esse artigo havia sido vetado da LGPD, por tratar de base de dados de caráter geral (não sensíveis), mas foi reinstaurado em sua redação final, após se pugnar pela necessidade de regulamentação, que decorreu de questão envolvendo antigo diretor do INEP e sua intenção, na época, em permitir acesso a informações do INEP para emissão de carteira estudantil.

Regulamento quanto a indicação dos membros do conselho
Por: Rachel Gonzaga

Dentre a composição da ANPD, temos o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, cuja indicação dos membros de (i) entidades da sociedade civil, (ii) instituições científicas, tecnológicas e de inovação, (iii) confederações sindicais representativas das categorias econômicas do setor produtivo, (iv) entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais e (v) entidades representativas do setor laboral, dependem de regulação da ANPD.

De início cumpre-nos ressaltar que a temática objeto de regulamentação da LGPD não é algo simples, e permeia por diversos setores públicos e privados do Estado, cuja regulamentação impacta de forma ampla e escalonada diversos segmentos e setores.

Além disso, é claro que a proteção de dados pessoais não envolve única e exclusivamente o dado em si, mas seu uso nas mais diversas tecnologias que vêm sendo desenvolvidas a partir da revolução digital, podendo o dado ser considerado o insumo e, porque não, a mola propulsora de diversas inovações e criações de modelos de negócio.

É fácil de se constatar tal fato a partir da história em que se iniciou a discussão quanto à necessidade de uma legislação que regulasse a proteção de dados pessoais, que se tornou cada vez mais necessária e relevante com o advento da internet e desenvolvimento de tecnologias capazes de processar de forma mais rápida e barata uma grande quantidade de dados, que, por sua vez geraram diversos reflexos na vida privada e nos direitos e liberdades das pessoas, demandando assim que o direito regulasse os limites e salvaguardas para o uso dos dados pessoais.

Note-se que internacionalmente a regulamentação não é tão nova, a Declaração Universal de Direitos Humanos, em 1948 já garantia o direito à privacidade, a Alemanha possui regulação desde 1970, sem contar com a *Convention* 108 de 1981, as *Guidelines* da OECD de 1981, dentre diversos outros normativos.

Contudo, no Brasil, apesar de já possuirmos em nossa Constituição Federal consagrado o direito à privacidade e existirem diversas legislações esparsas que tratam de alguma forma o tema, a ideia de um regulação geral de proteção de dados pessoais é nova e portanto, é necessário um diálogo entre a sociedade civil e as autoridades, no sentido de garantir a proporcionalidade e razoabilidade na interpretação de seus dispositivos.

Nesse sentido, o Conselho Nacional de Proteção de Dados Pessoais e Privacidade, órgão que compõe a ANPD em conjunto com o Conselho Diretor, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas e unidades especializadas necessárias à aplicação do disposto na lei, é peça fundamental para garantir tal equilíbrio.

Dentre suas atribuições previstas no art. 58 da LGPD, verifica-se que o Conselho Nacional irá ser um órgão consultivo da ANPD fornecendo os *insights*, parâmetros e

estudos necessários à uma aplicação da lei equilibrada e dentro dos padrões que permitam a avaliação de todos os âmbitos, setores e negócios impactados.

Face a esta atribuição que sua composição é heterogênea, possuindo representantes do setor público e privado. Contudo, a indicação dos representantes do setor privado depende de regulamentação e a demora em definir como se dará a eleição de tais membros poderá impactar sobremaneira no desenvolvimento dos estudos e pareceres a serem apresentados ao Conselho Diretor, bem como, nos diversos pontos que precisam ser regulamentados conforme aqui descrevemos (uma vez que o Conselho Diretor pode regulamentar tais pontos sem que o Conselho Nacional tenha se manifestado, o que poderá a levar a uma regulamentação ineficiente, que impacte desnecessariamente setores da economia ou que sejam inviáveis operacionalmente).

Regulamento bases legado
Por: Aline F. Fachinetti

É notório que a LGPD é uma lei complexa, ainda mais para um país que não possui o histórico cultural de proteção de dados pessoais (a despeito dos regimes setoriais e leis esparsas existentes no país, conforme mencionamos anteriormente). Assim, a LGPD consiste em verdadeiro e paradigmático marco regulatório, introduzindo diversos novos requisitos no ordenamento jurídico brasileiro.

Nesse cenário, definiu-se que, além do *vacatio legis*, haveria uma disposição para assegurar que o período de transição social e adequação fosse promovido de forma mais justa e com maior segurança jurídica, notadamente através do artigo 63 da LGPD, que estabelece que a ANPD "*estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor* da lei [no jargão popular, a famosa base legado], *consideradas a complexidade das operações de tratamento e a natureza dos dados".*

Muito embora isso não seja, de forma alguma, uma isenção do cumprimento da lei no que se refere a tais bancos de dados ou um abrandamento da aplicabilidade da mesma para a base legado, existirá um verdadeiro *regime de transição*, cujas regras para adequação no período deverão ser regulamentadas pela autoridade.

Importante destacar que a avaliação e adequação dos dados pessoais já existentes na estrutura das entidades pode ser extremamente valiosa para aqueles que passam por um programa de conformidade com a LGPD, já que essa avaliação possibilitará a revisão de bases legados que não são mais úteis e, inclusive, a revisão de procedimentos, de forma a gerar melhorias em processos e oportunidades.