Passa a Passar: A LGPD e a inevitável prorrogação da sua vacatio (2)

Continuação da Parte 1: A lei também cuida de maneira taxativa do tratamento de dados pessoais sensíveis (art. 11), seja quando o titular ou seu representante legal consentir, de forma específica e destacada, para finalidades específicas (I), seja independentemente de consentimento, quando, *v.g.*, for indispensável para o cumprimento de obrigação legal ou regulatória pelo controlador (II, a). O § 4º veda "*a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica*", exceto nos casos de portabilidade de dados consentida pelo titular (I) ou "*necessidade de comunicação para a adequada prestação de serviços de saúde suplementar*" (II).

Igualmente mereceu atenção da LGPD o tratamento de dados pessoais de crianças e adolescentes, que "*deverá ser realizado em seu melhor interesse*" (art. 14), contando com o consentimento específico e em destaque por pelo menos um dos pais ou pelo responsável legal (§ 1º).

O art. 15 da lei estipula que o término do tratamento de dados pessoais se dará quando (I) a finalidade tiver sido alcançada ou os dados tiverem deixado de ser necessários; (II) se der o fim do período do tratamento; (III) houver comunicação do titular, "*inclusive no exercício de seu direito de revogação do consentimento*"; e (IV) a autoridade nacional assim determinar, quando houver violação ao disposto na LGPD.

Muito embora o art. 16 estabeleça que os dados pessoais serão eliminados após o término de seu tratamento, ele permite a sua conservação para os seguintes fins: (I) cumprimento de obrigação legal ou regulatória pelo controlador; (II) estudo por órgão de pesquisa, "*garantida, sempre que possível, a anonimização dos dados pessoais*"; (III) transferência a terceiro, uma vez observados os requisitos legais para tanto; e (IV) "*uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.*"

Nos arts. 17 e seguintes, a LGPD cuida dos direitos do titular dos dados pessoais, garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, bem como, a qualquer momento (art. 18), (I) o direito de obter do controlador a confirmação da existência de tratamento; (II) o acesso aos dados; (III) a correção de dados incompletos, inexatos ou desatualizados, como visto; (IV) a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em dissonância com a lei,

dentre outros.

O tratamento de dados pessoais também poderá ser feito por pessoas jurídicas de direito público (art. 23), tendo os serviços notariais e de registro o mesmo tratamento dispensado àquelas pessoas (§ 4º), tais como os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público, além de autarquias, fundações e empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, pelos Estados, Distrito Federal e Municípios.

Interessante notar que a lei em comento permite a transferência internacional de dados pessoais observadas determinadas circunstâncias (art. 33), como (I) "*para países ou organismos internacionais que proporcionem grau de proteção de dados adequado ao previsto nesta Lei*"; e (II) o controlador oferecer e comprovar garantias de cumprimento dos princípios dos direitos do titular e do regime de proteção de dados constantes da norma, na maneira de (a) cláusulas contratuais específicas para determinada transferência; (b) cláusulas-padrão contratuais; (c) normas corporativas globais; e (d) selos, certificados e códigos de conduta regularmente emitidos.

No cenário legal, são figuras que merecem destaque o titular, o controlador, o operador, o encarregado pelo tratamento de dados pessoais, o órgão de pesquisa e autoridade nacional. Reiterem-se aqui, porquanto pertinentes, os respectivos conceitos, constantes do art. 5º da LGPD:

"V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII – encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados; (…)

XVIII – órgão de pesquisa:órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

XIX – autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei." (Grifou-se.)

Mas os agentes de tratamento também estão sujeitos a duras sanções administrativas (art. 52), que vão desde advertência à multa simples de até 2% (dois por cento) do faturamento de pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Inequivocamente relevante que se adotem as melhores práticas para que não haja a aplicação das

referidas penalidades, observando-se as normas dispostas nos arts. 46 a 51, que tratam da segurança e do sigilo de dados e das boas práticas e da governança.

O mencionado art. 46 impõe aos agentes de tratamento a obrigação de se adotarem medidas de segurança, técnicas e administrativas, para proteger os dados pessoais de acessos não autorizados, inclusive evitando-se qualquer forma de tratamento inadequado ou ilícito. O parágrafo primeiro relega à autoridade nacionaldispor sobre padrões mínimos para tornar aplicável o disposto no artigo, enquanto o parágrafo segundo determina que as medidas sejam observadas desde a fase de concepção do produto ou do serviço até a sua execução, devendo os agentes de tratamento garantir a segurança da informação e o controlador comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (arts. 47 e 48).

Quanto às boas práticas e à governança, os sistemas utilizados para o tratamento de dados pessoais devem atender a essas condições, juntamente com os requisitos de segurança, observando-se, ainda, os princípios gerais previstos na lei e as demais normas regulamentares pertinentes (art. 49).

A LGPD permite, ainda, aos controladores e operadores que formulem regras a esse respeito, estabelecendo "*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*" (art. 50).

Quanto à criação, sem aumento de despesa, da Autoridade Nacional de Proteção de Dados – ANPD pela Medida Provisória nº 869, como órgão da administração pública federal, integrante da Presidência da República (art. 55-A), foi-lhe assegurada, como não poderia deixar de ser, autonomia técnica (art. 55-B), sendo ela composta por (I) Conselho Diretor, órgão máximo de direção; (II) Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; (III) Corregedoria; (IV) Ouvidoria; (V) órgão de assessoramento jurídico próprio; (VI) unidades administrativas e unidades especializadas necessárias à aplicação do disposto na lei.

Como se percebe, estar preparado para o cumprimento da norma demandará um minucioso trabalho por parte de todos os envolvidos no processo. Desde o modelo a ser adotado para regular as relações entre o controlador e o titular dos dados pessoaisaté a elaboração do ato que cuidará da estrutura regimental da ANPD, um longo caminho deverá ser percorrido para que a LGPD atinja os seus devidos fins.

No país, estima-se que um número ainda pequeno estava pronto ou estaria pronto até agosto para o cumprimento da norma. Neste grupo, incluem-se as multinacionais e empresas com contratos internacionais com terceiros já sob a tutela do *General Data ProtectionRegulation*, o GDPR europeu, fonte de inspiração da nossa LGPD.

Fora a pendente criação da ANPD, o país – nem o mundo! – contava com a pandemia que viria a ser causada pelo Coronavírus (COVID-19). Os números, a escalada, de infectados e mortos são impressionantes, tudo a impor o fechamento de quase todos os estabelecimentos e o isolamento pessoal para se evitar o contágio de mais e mais indivíduos.

Além das vidas humanas, o cenário econômico que se instaurou é assustador. Por exemplo, com o comércio fechado – apenas atividades essenciais estão autorizadas a funcionar, como farmácias e mercados –, a quantidade de empresas que se encontrarão em situação de insolvência é relevantíssima, cabendo ao Estado, aqui em sentido *lato* – dispor e aprovar medidas, com velocidade, para minimizar esse caos.

Dentre essas ações, é de se indagar: deve a lei ser mais uma vez postergada diante do quadro atual? A mim meparece que não haverá alternativa, sobretudo considerando a necessidade de interação pessoal entre a equipe escolhida para traçar o plano de trabalho e o cliente, não sendo suficiente o contato apenas por meios digitais. E esse parece ser o caminho natural que se seguirá, com a aprovação, nesta data, pelo Senado, do Projeto de Lei nº 1.179/2020, que suspende normas de Direito Privado enquanto perdurar a epidemia no país.

Como destacado pela **ConJur**, "*[um] dos pontos centrais do projeto é o artigo 65, que trata do adiamento da vigência da Lei Geral de Proteção de Dados (LGPD). Pelo texto aprovado nesta sexta, a lei passa a viger apenas a partir do dia 1º de janeiro de 2021. As multas e sanções para as empresas que não consigam se adequar à lei passam a valer em 15 de agosto de 2021 (…)*". A proposta, fruto de trabalho entre o Judiciário e Legislativo em regime de emergência, aprovada por unanimidade, agora segue para votação na Câmara dos Deputados.

Contudo, isso não quer dizer que a atividade de adequação deva ficar esquecida até o fim deste cenário. Não e não. Muito pelo contrário, o momento é profícuo para se aprofundar no tema e, no que for possível, adiantar a missão virtualmente, sendo vários os meios hoje disponíveis para tanto.

Nesse diapasão, temos que falar em como se preparar para a lei o quanto antes, considerando ou não eventual alteração na sua *vacatio*. Pelo que vimos até aqui, podemos utilizar como exemplo de sua plena aplicação a relação existente entre o empregador e o seu colaborador. Quando da contratação ou para fins de atender ao disposto na LGPD, o empregador deverá disponibilizar em cláusula destacada no contrato de trabalho ou em documento suplementar autorização específica, jamais genérica, para o tratamento de dados pessoais ou dados pessoais sensíveis.

O conceito de tratamento é amplo: "*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*" (art. 5º, X).

Feito o instrumento adequadamente, haverá, se for o caso, uma integração entre as figuras acima, ainda mais considerando que o descumprimento de qualquer disposição da lei ensejará, ao controlador ou ao operador, até mesmo em caráter solidário, a obrigação de reparar o dano causado ao titular, seja ele

patrimonial ou moral, individual ou coletivo, na linha dos arts. 42 e seguintes, que também permitem a inversão do ônus da prova no processo civil, havendo verossimilhança da alegação e hipossuficiência para fins probatórios (§ 2º).

Mas eu diria que o passo principal a ser tomado é o de se estabelecer, caso ainda não estabelecido, uma comissão, um grupo, para estudar as peculiaridades da norma, que, a meu ver, deverá ser formada por pessoas ligadas às áreas de recursos humanos, tecnologia da informação e jurídica.

Esse grupo ficaria encarregado de dividir as tarefas de cada qual, as suas atribuições e o controle do tratamento das informações, sobretudo no que diz respeito ao operador e ao encarregado.

A sociedade deverá ter um contrato ou termos específicos em um contrato de trabalho, por exemplo, que cuide do tratamento dos dados, na parte em que trate da confidencialidade e do uso responsável das informações profissionais.

Cabível alertar que a lei fez uma distinção entre dados e dados pessoais sensíveis, os quais podemos citar como informações de saúde, raça, política, religião, orientação sexual e por aí vai. As informações sobre a saúde do indivíduo, vejam só, encontram-se em voga por conta do Coronavírus.

Como se vê, as empresas terão um novo enfoque quanto à sua responsabilidade, preservando o consentimento do seu colaborador, os seus direitos, zelando pela segurança das informações que lhes são prestadas no âmbito de um contrato de trabalho ou de prestação de serviços.

Nessa linha, sugere-se a atribuição a determinado indivíduo da missão de protetor desses dados, o chamado *Data Protection Officer*, o DPO, que funcionará como um canal entre a sociedade e os seus empregados, para tomar as medidas que forem cabíveis, inclusive comunicando-se com a ANPD no caso de violação das obrigações legais.

Essa pessoa será encarregada, ainda, de treinar o pessoal envolvido no processamento de dados, conduzindo auditorias a fim de evitar qualquer problema relacionado ao assunto, que, eventualmente, poderá levar a pesadas sanções à empresa. Ressalte-se que o encarregado poderá ser uma pessoa natural ou jurídica, ou, ainda, um grupo de pessoas.

Para pontuar de uma forma mais clara, destacam-se, enfim, as seguintes orientações:

1. Conhecer a lei a fundo;

2. Identificar as principais lacunas para interpretar a LGPD, tanto no que diz respeito ànorma quanto à própria empresa;

3. Envolver todas as equipes – Jurídico, *Compliance*, Negócios, RH, TI, Risco e outras – para que se comprometam a compartilhar a responsabilidade pelo plano de implementação e pela adequação a? nova lei – criação de grupos de estudo;

4. Nomear os técnicos do time: controlador, operador e DPO, que poderá não ser exigido, mas é recomendado;

5. Definir o escopo do programa LGPD e determinar com clareza o que devera? estar pronto ate? junho de 2020, eis que ainda não sabemos se a sua vigência será adiada – adaptação de contratos de trabalho, criação de termos específicos etc.;

6. Construir um registro de cada atividade de processamento de dados pessoais na organização, para garantir a sua conformidade e rastreabilidade;

7. Identificar quais informações gerenciar; quais são os dados pessoais; verificar se os dados são compartilhados ou não; se há dados sensíveis para posteriormente permitir o enquadramento dessas operações em uma das hipóteses de tratamento permitida pela lei;

8. Analisar os contratos da empresa e adequá-los para que contenham disposições que protejam a empresa nos termos da lei;

9. Adotar tecnologias que garantam maior segurança contra o vazamento de dados. A anonimização, a criptografia e o controle de acesso são as mais indicadas. Em 2017, apenas 3% dos dados que vazaram em incidências divulgadas estavam criptografados adequadamente. No Fórum Econômico Mundial de Davos 2019, foi apresentado um gráfico de gestão de riscos indicando que os riscos cibernéticos e a fraude ou o furto de dados aparecem como de alto impacto e alta probabilidade de ocorrência nas empresas. Ou seja, segurançaé fundamental neste momento;

10. Envolver advogados para garantir que a interpretação legal seja pragmática e realista, com o profundo conhecimento da lei;

11. Criar um caminho claro para comunicar e classificar incidentes, incluindo o Departamento Jurídico, de TI e de Relações Públicas;

12. Eliminar os dados não utilizados pela empresa, mas que acabam circulando entre as áreas internas. Cuidado especial com as informações não estruturadas, guardadas em planilhas físicas ou eletrônicas;

13. Retirar do banco de dados as informações que não sejam necessárias à finalidade;

14. Criar um programa de gerenciamento para a perda de dados. O que fazer em caso de vazamento? Errou? Assuma e corrija com rapidez; e

15. Monitorar as respostas dos indivíduos, isto é, dos titulares que contratam um serviço ou compram um produto.

Em linhas gerais — e como pôde ser visto —, há muito a ser feito, mas nada que não possa ser organizado desde logo, através de e-mails, vídeo conferências, telefonemas, deixando aquilo que exija contato pessoal para breve, assim torcemos – nem poderia ser diferente.

Date Created
03/04/2020