A LGPD nas sociedades de advogados

Juliana Abrusio
Alexandre Atheniense
Bruna Borghi Tomé

Passada a polêmica quanto ao adiamento da vigência da Lei Geral de Proteção de Dados (LGPD), ela finalmente entrou em vigor na data de 18 de setembro de 2020. Com menos de três meses de sua vigência, já foi proferido o primeiro *leading case* sobre o tema envolvendo suposta venda de dados cadastrais de dados de clientes de construtora para empresas parceiras. E antes mesmo dessa vigência já havia sido instaurados inúmeros procedimentos administrativos pela Secretaria Nacional do Consumidor (Senacon), Ministérios Púbicos e Procons.

Para além desses casos, chamou a atenção o julgamento ocorrido em maio do corrente ano das Ações Diretas de Inconstitucionalidade contra a Medida Provisória 954. Nele, o Supremo Tribunal Federal (STF) entendeu por suspender os efeitos da citada Medida Provisória, evitando que as operadoras de telefonia compartilhassem com o IBGE dados pessoais (nome, número de telefone e endereço) de todos os seus clientes com o intuito de auxiliar na produção de estatística oficial durante a situação de emergência decorrente da COVID-19. Vencido apenas o Ministro Marco Aurélio, firmou-se a posição de que a ausência de finalidade adequada dos dados a serem compartilhados transformaria essa transferência em ato desarrazoado, desproporcional e em "atropelo de garantias fundamentais consagradas na Constituição", segundo a relatoria da Ministra Rosa Weber.

Mais recentemente, em 05 de Novembro a Comissão de Juristas da Câmara dos Deputados nomeada para confecção da chamada "LGPD Penal" entregou seus trabalhos ao Presidente da Casa, anunciando que novos importantes debates em torno do assunto ocuparão a pauta do Legislativo. Um dia depois, em 06 de Novembro, foi publicado ato de nomeação dos Diretores da Autoridade Nacional de Proteção de Dados (ANPD).

Portanto, vê-se, claramente, que o assunto está efervescente e o próximo ano de 2021 promete ser ainda mais intenso e profícuo no campo da disciplina da proteção de

dados pessoais no Brasil. Nesse sentido, muitos escritórios de advocacia têm se voltado ao atendimento para adequação de seus clientes à LGPD, mas a pergunta que não quer calar é: e as sociedades de advogados propriamente ditas estão adequadas à nova lei?

Vale lembrar que a situação dos escritórios de advocacia é *sui generis* pois já existe a sua sujeição ao sigilo profissional. Segundo teor dos artigos 25 a 27 do Código de Ética e Disciplina da Ordem dos Advogados do Brasil (OAB) é imposto aos advogados o sigilo profissional dos dados e comunicações de seus clientes. O que muda com a LGPD, no entanto, é a forma com a qual se deve proteger referidos dados, bem como se deve dar transparência a esse respeito, tudo em prol da proteção da pessoa do titular dos dados, mediante a adoção de todas as práticas de *accountability* envolvidas.

Estamos diante de uma grande mudança cultural, em todos os níveis dos profissionais dentro do universo da advocacia. A realidade da prática aponta que o advento da LGPD não foi suficiente para que a grande maioria da sociedade de advogados tenha se sensibilizado para efetivar o início da adequação às obrigações legais. Daí nossa intenção de contribuir com este artigo para destacar quais são as principais medidas a serem tomadas pelos sócios.

Importante ter presente que um plano de adequação à LGPD demanda uma abordagem multisetorial, sobretudo para gerar em todos os colaboradores a cultura de zelo com as operações de dados, que vão desde currículos para processos seletivos até lista de experiência para fins institucionais a contratos com clientes e fornecedores de serviços. Há, sem dúvida, uma imensa variedade de dados pessoais que circulam em escritórios.

Tal mudança cultural operacional deve ser encarada como uma jornada, cujos resultados não se alcançam de um dia para o outro. Não é uma mudança rápida, por esse motivo o escritório deve envidar esforços para que haja meios de criar uma campanha interna para conscientizar todas as pessoas envolvidas, por meio de cartilhas, reuniões, vídeos, webinars, para que seja possível alcançar uma capacitação mais breve sobre as mudanças operacionais trazidas pela LGPD, especialmente para o ambiente do escritório.

Antes de mencionar os passos, propriamente ditos, para um plano de adequação, recomenda-se que a sociedade de advogados, como ponto de partida dessa jornada, destaque e nomeie um comitê interno para se ocupar do assunto. O mais recomendado é que referido grupo tenha em sua composição, no mínimo, um sócio patrimonial gestor, um representante do setor jurídico do contencioso, e um representante do setor administrativo, incluindo as áreas de tecnologia da informação, de recursos humanos e do financeiro. O objetivo é discutir assuntos e tomar decisões acerca dos temas de privaci-

dade e proteção de dados pessoais e aprovar eventuais mudanças operacionais que possam configurar fator de risco e penalidades. Ademais, o comitê sugerido terá a missão de orquestrar todas as atividades operacionais relacionadas ao diagnóstico via inventário de dados pessoais, bem como o plano de ação para executar as medidas corretivas e verificar sua eficácia continuamente.

Dito isso, cumpre sistematizar quais são os passos para o cumprimento de um plano de adequação: (i) mapeamento dos fluxos de dados pessoais no dia a dia do escritório, bem como de bases legadas (arquivadas) de todas as áreas (jurídico e administrativas); (ii) classificação dos tratamentos de dados com base nas hipóteses legais (arts. 7º e 11 da LGPD); (iii) classificação da criticidade dos dados de acordo com sua natureza (dado pessoal, dado financeiro, dado pessoal sensível); (iv) definição dos prazos possíveis de retenção; (v) revisão dos contratos e políticas relacionadas; (vii) nomeação de um Encarregado; (vii) elaboração das documentações pertinentes para estruturação da governança de proteção de dados pessoais voltadas a um escritório de advocacia; (viii) revisão dos contratos do escritório (com clientes, empregados, fornecedores, etc); (ix) elaboração de documentos e processos aptos ao atendimento dos direitos dos titulares dos dados; e, sobretudo (x) treinamentos frequentes.

Detalharemos alguns dos passos mencionados acima, dando realce, inicialmente, ao Encarregado, também chamado de DPO (*Data Protection Officer*). É de suma importância que a sociedade de advogados, após escolher esse profissional, confira publicidade de seu contato para atuar como canal de comunicação com os clientes e titulares de dados em geral, bem como com a ANPD (art. 5º, VIII, LGPD). O atendimento a esta obrigação legal vale – até que a ANPD disponha de outra forma – para escritórios de advocacia de todos os tamanhos.

A lei faculta que a sociedade de advogados posso escolher entre nomear uma pessoa física ou jurídica para exercer esse *munus* (art. 41, LGPD). No último caso trata-se do chamado "*DPO As A Service*" (DPOaaS).

Quando ocorrer a escolha do encarregado, deve-se ter em mente que ele não pode ser equiparado a mais um colaborador do setor operacional do escritório. Trata-se de um cargo com atuação e conhecimento específicos, com independência e autonomia dos sócios gestores, sem submissões hierárquicas aos demais setores operacionais.

Esta condição é imprescindível, pois o DPO deve agir com autonomia e liberdade para apontar erros operacionais, buscar soluções, bem como sugerir, validar e adotar decisões estratégicas para enfrentar os incidentes prontamente após a sua ciência, além

de cobrar dos sócios respostas breves na tomada de decisões. Desse modo, não poderá ocorrer conflitos de interesses com chefes de setores, no momento da análise dos fatos.

Outro detalhamento a ser colocado em evidência é sobre a necessidade de um olhar cuidadoso para os prestadores de serviço do escritório de advocacia. Infelizmente, não são todas as empresas parceiras dos escritórios que estão sensibilizadas para as adequações necessárias. É importante ter em mente que a adequação à LGPD significa uma reação em cadeia, ou seja, não basta que a sociedade de advogados faça sua parte, se os seus parceiros de negócio estiverem alheios à necessidade de adequação. Caso esse cenário de informalidade permaneça, o terceiro poderá colocar em risco a sociedade de advogados. Sabe-se que muitos dos incidentes de segurança da informação ocorrem no ambiente do parceiro de negócio, muito embora o arranho de imagem e a responsabilidade legal recaiam sobre a figura do Controlador, esse entendido com o agente de tratamento que toma a decisão sobre os dados pessoais, tal qual um escritório de advocacia.

E ao mencionar esse assunto, é oportuno discorrer sobre a necessidade de um plano de contingenciamento de incidentes de segurança da informação para os escritórios de advocacia, incluindo incidentes que afetem sua reputação digital.

Todo escritório pode ser alvo de incidentes cibernéticos. Se até o STJ o foi recentemente, não se pode imaginar que as sociedades de advogados estariam ilesas. O que faz a diferença para o enfrentamento destes problemas está diretamente relacionado à adoção de um plano de contingenciamento prévio, selecionando as pessoas com talentos adequados para executar no menor tempo possível as medidas necessárias para colocar em prática o enfrentamento desses problemas.

Sabe-se que o enfrentamento tardio e desordenado, nesse quadrante, pode gerar sérias consequências para a sociedade de advogados. Este plano deverá ser executado como se fosse uma brigada de incêndio para agir rápido diante dos incidentes. Quanto mais rápida e assertiva for a reação, melhor será.

Nessa seara, vale dizer, o cuidado deve ir além da atenção aos ataques ‘de fora para dentro’. É salutar ter consciência que muitos incidentes ocorrem ‘de dentro para fora’, ou seja, são cometidos por colaboradores que, por vezes, agem de forma negligente frente aos cuidados e padrões que deveriam ter e assumir dentro de um escritório de advocacia.

Sobre esse ponto, essencial frisar que é função e dever da própria sociedade de advogados capacitar seus colaboradores, bem como instituir regras internas visando impor procedimentos para diminuir o risco da ocorrência de vazamento de dados e outros incidentes envolvendo dados pessoais.

Nesse panorama, pode ser citado como exemplo o hábito comum de muitos colaboradores divulgarem dados pessoais por meio de WhatsApp ou outras formas de comunicação afins, sem nenhum critério e facilitando o vazamento de informações, que deveriam estar sob maior proteção. Isto acontece porque o escritório não dispõe de uma política de gestão documental, que determine em qual canal cada tipo de informação deveria ser tratada.

Da mesma forma, percebe-se que muitos escritórios não possuem políticas formalizadas para descarte de dados pessoais, quando o tratamento já atingiu a sua finalidade, e inexiste dever legal para sua guarda. Os escritórios de advocacia são, por excelência, acumuladores (sem necessidade) de dados pessoais. Isto passa a ser fator de elevado risco. É, portanto, necessária a adoção de medidas e cuidados efetivos nesse sentido.

Além do mais, a adoção de uma política de segurança da informação é mandatória pois a inexistência dará margem a argumentação do colaborador que não tinha orientações sobre os limites do seu procedimento quanto ao uso da infraestrutura de tecnologia da informação e não sabia se sua atividade era (i)lícita.

A caminho do encerramento desse artigo, repise-se que de nada adiantam os relatórios, as novas cláusulas contratuais ou mesmo as novas políticas e regulamentos se os integrantes do escritório não estiverem devidamente treinados a esse respeito. Nesse sentido, palestras e cartilhas ilustrativas podem ser um bom caminho para incentivar o comportamento zeloso de todos.

Assim, se a adaptação ainda não teve início, é chegada a hora de fazê-lo para evitar maiores prejuízos e conceder o exemplo. É preciso, ainda, manter-se otimista e ter em mente que as adequações legais nas sociedades de advogados podem resultar em oportunidades. Dessa feita, o percurso dessa jornada não deve ser encarado como um ônus, mas como um diferencial de mercado que se transformará em valor, o qual passará a ser cada vez mais exigido em cartas-convites, editais de contratação, e concorrência em clientes da iniciativa privada.

Artigo publicado no Anuário CESA 2020, pg. 91 /95. Para baixar a versão digital do Anuário acesse: http://www.cesa.org.br/media/files/Anuario2020.pdf