ARTIGOS ACEITOS PARA PUBLICAÇÃO
DIREITO DIGITAL E SETOR PÚBLICO - 2020.2

ITS RIO

Pós-Graduação em Direito Digital

CEPED UERJ ITS

Primeiras Reflexões sobre os Impactos da Lei Geral de Proteção de Dados (LGPD) em Operações de Fusão e Aquisição (M&A) no Brasil

Rogério Soler Junior

Primeiras Reflexões sobre os Impactos da Lei Geral de Proteção de Dados (LGPD) em Operações de Fusão e Aquisição (M&A) no Brasil

Aluno: **Rogério Soler Junior**

Introdução

O objetivo deste artigo é propor um exame não exaustivo dos impactos da Lei Federal nº 13.709, de 14 de agosto de 2020, cf. alterada ("Lei Geral de Proteção de Dados" ou "LGPD") em operações de compra e venda de empresas – seja de participação societária (quotas ou ações), seja de ativos ou unidades de negócios –, também referidas como operações de fusão e aquisição ou, simplesmente, "M&A" (*mergers and acquisitions*).

Abordagens doutrinárias sobre a LGPD tendem a focalizar o tratamento de dados pessoais por agentes de tratamento (controladores e operadores) sob uma perspectiva estática, considerando tais agentes como entes estáveis, sujeitos às obrigações e aos limites impostos pela legislação. O artigo pretende apresentar uma breve contribuição para a ampliação desse foco.

A análise de operações de M&A implica, por essência, observar empresas (que se qualifiquem como controladores ou operadores) sob uma perspectiva dinâmica. Por um lado, a aquisição de uma empresa ou unidade de negócios que realiza tratamento de dados por outra empresa tem o potencial de modificar as relações estabelecidas entre a empresa original (adquirida) e os titulares, com impactos para todos os envolvidos (adquirente, adquirida e os próprios titulares). Por outro lado, o processo que culmina na consumação de uma operação de M&A pode representar, por si só, uma operação específica de tratamento de dados pessoais, que deve, como qualquer tratamento de dados, sujeitar-se às exigências normativas da LGPD.

Por ser uma matéria de interesse eminentemente prático (e econômico), operações de M&A não costumam ser objeto de tratamento particularizado pela academia, o que não tem sido diferente no que diz respeito à análise dos impactos das leis de proteção de dados em tais operações. Tal análise, no entanto, vem motivando advogados que atuam em operações de M&A (como o autor) a publicarem reflexões e materiais institucionais em veículos próprios de escritórios de advocacia ou na imprensa. O artigo procura conjugar material acadêmico e/ou produzido por organizações de proteção de dados reconhecidas com as reflexões de advogados

sobre os impactos das normas de proteção de dados sobre suas atividades e os interesses de seus clientes.

O artigo está dividido em três seções, além desta introdução e da conclusão. As seções são divididas seguindo a ordem cronológica convencional das etapas principais de uma operação de M&A: (i) a precificação (ou *valuation*) da empresa ou dos ativos que o adquirente pretende adquirir, (ii) o processo de auditoria (*due diligence*) realizado pelo adquirente na empresa ou ativo-alvo, e (iii) a negociação dos contratos de compra e venda de participação societária ou de ativos que estruturam a operação.

1. Impactos sobre a precificação *(valuation)*

Um primeiro impacto a ser considerado envolve uma etapa preliminar ao início das tratativas referentes a uma operação de M&A: a precificação (*valuation*), pelo potencial adquirente, da empresa ou dos ativos em consideração. Como regra (e de modo bastante simplificado), essa precificação se dá a partir do estabelecimento de premissas que permitam estimar o potencial de geração de valor futuro da empresa ou dos ativos – seja de lucro operacional, para negócios já estabelecidos e capazes de gerar lucros, seja de receita, comumente para negócios em fase de maturação ou escalada, cujos custos operacionais ou necessidade de investimento ainda excedam a sua capacidade de geração de caixa[1] –, descontando-se do valor calculado o endividamento da empresa e/ou a necessidade de investimentos específicos que tornem parte do caixa da empresa indisponível para seus sócios ou acionistas, a ser aferida antes ou após o processo de auditoria (cf. Seção 2, abaixo).

A novidade trazida pelas legislações e regulações de proteção de dados – em particular, para os fins deste artigo, pela LGPD – em diferentes jurisdições é a necessidade de consideração, nos processos de *valuation*, do custo de adequação (ou não adequação) das empresas ou ativos em consideração aos padrões legais de tratamento de dados, segurança da

[1] A decisão pelo método de avaliação mais adequado é altamente contextual e, em última análise, subjetiva. A utilização da receita bruta (*e.g.* total de vendas) ou da receita recorrente (*e.g.* pagamentos periódicos de assinaturas por usuários de serviços de *SaaS – Software as a Service*) como métrica de análise tem se tornado usual em operações envolvendo empresas do meio digital, sobretudo em negócios inovadores e em fase inicial de maturação, em detrimento da consideração tradicional do *Ebitda* (lucros antes do pagamento de impostos, depreciação de ativos e amortização), em especial quando é necessário um alto investimento (i.e., custo) para consolidar ou expandir o uso do produto ou serviço desenvolvido pela empresa adquirida.

informação e governança. Essa avaliação específica é tanto mais necessária quanto mais intenso for o tratamento de dados pessoais pela empresa-alvo, e especialmente relevante para empresas cuja atividade principal implique tratamento intensivo de dados pessoais.

Shah, Bacal e Forester (2019) indicam três fatores específicos e interconectados a serem levados em conta por potenciais adquirentes: (i) a consistência do modelo de *valuation* com os usos aventados de dados pessoais após a aquisição da empresa-alvo; (ii) os custos potenciais de adequação da empresa-alvo às exigências da(s) legislação(ões) de proteção de dados aplicáveis, sob as perspectivas operacional, contratual e de governança; e (iii) os custos financeiros associados à não adequação da empresa-alvo às normas de proteção de dados.

Sobre o fator (i), uma aquisição pode ser justificada pelo potencial de uma determinada tecnologia desenvolvida pela empresa-alvo de expandir a capacidade de coleta, análise, ou outras modalidades de tratamento de dados pessoais pela empresa adquirente, ou pela relevância das bases de dados pessoais mantidas pela empresa-alvo para o incremento ou expansão dos negócios da empresa adquirente. Caso a adquirente tenha o interesse de, após a aquisição, expandir o escopo do tratamento de dados realizado pela empresa adquirida, é necessário atentar para os constrangimentos impostos pela LGPD, que podem impor custos adicionais à operação ou mesmo tornar instável o tratamento pretendido dos dados pessoais, impactando as premissas do *valuation*.

Um exemplo hipotético é a situação em que adquirente tem interesse em utilizar as bases de dados da empresa adquirida de modo compartilhado para fins de elaboração de perfis comportamentais dos titulares (*e.g.* potenciais novos clientes[2]) ou fazer com que a adquirida, após a operação de aquisição, passe a coletar, analisar e compartilhar com a adquirente dados pessoais sensíveis (art. 5º, II, LGPD), como dados referentes à raça ou etnia de titulares de dados. No primeiro caso, a conjugação de informações da adquirente e da adquirida gera perfis legalmente qualificados como dados pessoais (art. 12, §2º, LGPD), o que pode exigir, no mínimo, adaptações das políticas e procedimentos internos da adquirente e da adquirida para

[2] Pense-se, por exemplo, na aquisição da Netshoes pela Magazine Luiza (Magalu), justificada pela adquirente como "*aquisição representa um passo significativo na estratégia de crescimento exponencial do Magalu, aumentando a base de clientes online e a frequência de compra*" (cf. Fato Relevante divulgado pela Magalu em 14 de junho de 2019, disponível em https://ri.magazineluiza.com.br/list.aspx?idCanal=dirZ4d6pdWtBlllUu+9ejg==&ano=2019, último acesso em 12.12.2020).

dar transparência aos titulares quanto à realização do tratamento e sua finalidade, bem como a criação de canais de comunicação adequados com tais titulares (art. 9º, LGPD). No segundo caso, sob a perspectiva de uma empresa privada, que pretende utilizar tais dados pessoais sensíveis com fins lucrativos, é quase certo que tal tratamento dependerá de consentimento expresso e específico dos titulares (art. 11, I, LGPD)[3], consentimento esse que fica sujeito à revogação pelo titular a qualquer momento (art. 8º, §5º, LGPD). Nesses cenários, o *valuation* deve considerar as exigências da LGPD para dar robustez às premissas adotadas, em especial no segundo caso, em que a geração de valor estimada decorrente do tratamento de dados pessoais sensíveis fica sujeita à determinação do próprio titular dos dados pessoais.

Sobre o fator (ii), o grau de adequação da empresa-alvo às exigências da LGPD pode ser um fator relevante e complexo para o *valuation*. A entrada em vigor "súbita" da LGPD em agosto de 2020 fez com que inúmeras empresas se encontrassem, repentinamente, em desconformidade com a lei. O investimento necessário para a adequação pode ser expressivo a depender de quão atrasada esteja a empresa adquirida em relação à exigência normativa e, sobretudo, da intensidade e profundidade das operações de tratamento de dados realizada pela empresa.

Tal investimento pode envolver tanto (a) custos operacionais relevantes, como os necessários à readaptação de procedimentos internos de armazenamento e acesso de colaboradores a dados pessoais[4] e, em especial, de medidas de segurança da informação (art. 46, *caput*), (b) custos associados à revisão de contratos celebrados pela empresa adquirida com clientes e fornecedores que envolvam tratamento de dados pessoais, e (c) custos associados à estruturação de uma equipe interna responsável pela elaboração e gestão das políticas de privacidade e tratamento de dados, comunicação com titulares e com a Agência Nacional de Proteção de Dados (ANPD), com a nomeação de um encarregado e uma equipe de suporte, que podem implicar novas contratações ou readequações de funções de colaboradores já contratados. Todas essas medidas importam custos que tornam parte do caixa gerado pela empresa indisponível aos seus sócios ou acionistas, impactando o valor "final" da empresa atribuído pelo *valuation*.

[3] A leitura das hipóteses de tratamento de dados pessoais sensíveis que não dependem de consentimento do titular (art. 11, II, alíneas a) a g)), restritas e específicas, permite chegar a essa conclusão.
[4] Em decorrência da interpretação do princípio da necessidade (art. 6º, III, LGPD), que justifica a limitação do acesso aos dados pessoais apenas às pessoas diretamente responsáveis pelo tratamento de dados em questão, observada a finalidade de tal tratamento.

Os custos associados à adequação à LGPD também podem decorrer das características do próprio adquirente e de seu interesse específico nas bases de dados da empresa adquirida. Um exemplo hipotético mais evidente é o caso de uma empresa estrangeira que adquire uma empresa brasileira e tem interesse em transferir as bases de dados da empresa adquirida para armazenamento em servidores e tratamento fora do Brasil. Com a ANPD ainda em fase de constituição, há uma insegurança quanto a transferências internacionais de dados realizadas sem o consentimento expresso e específico (e revogável) dos titulares de dados pessoais, dado que (a) não há certeza sobre quais jurisdições terão suas legislações de proteção de dados consideradas como equivalentes à legislação brasileira, e (b) não há mecanismos que permitam desde logo a aprovação de normas corporativas globais, cláusulas-padrão contratuais ou reconhecimento de certificações de proteção e privacidade de dados (cf. art. 33, II, "b", "c" e "d", LGPD).

Sobre o fator (iii), a progressiva atenção dada à temática da proteção de dados pessoais na agenda do debate público brasileiro, em especial com a entrada em vigor da LGPD, torna o cumprimento das exigências legais de proteção de dados um fator decisivo para que as empresas se protejam de eventuais sanções legais, considerando-se uma maior pressão pública pela atuação das autoridades (seja da ANPD, seja do Ministério Público ou do PROCON) e uma tendência de crescimento de litígios judiciais relacionados a tratamentos de dados ilegais ou incidentes de segurança. Para fins de *valuation*, a identificação do grau de adequação da empresa-alvo à LGPD e das lacunas referentes ao tratamento e à segurança de dados pessoais tratados – possível apenas mediante a realização de auditoria, conforme detalhado na Seção seguinte – é relevante para a identificação de possíveis contingências, como sujeição a multas pela ANPD ou risco de perdas decorrentes de processos judiciais. Trata-se de uma avaliação necessária, mas ainda bastante difícil no contexto brasileiro, não havendo um histórico consolidado de decisões da autoridade ou do judiciário que permitam quantificar e expressar tais riscos em termos monetários com precisão razoável[5].

[5] O montante das sanções pecuniárias aplicáveis pela ANPD pode chegar a 2% do faturamento líquido de tributos da "pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício", limitada ao teto de R$50 milhões (art. 52, II, LGPD). A própria LGPD estabelece que a dosimetria deverá observar, dentre outros fatores, a proporcionalidade (art. 52, §1º, XI), a condição econômica do infrator (art. 52, §1º, IV) e o nível de governança e a agilidade na correção de eventuais incidentes de segurança (art. 52, §1º, IX e X). Nesse sentido, há uma variabilidade esperada no valor das multas aplicáveis pela ANPD, que torna mais complexa a quantificação *a priori* das sanções a que a empresa-alvo pode vir a estar sujeita em virtude de violações da LGPD.

2. Impactos sobre a auditoria (*due diligence*)

As leis e regulações de proteção de dados, incluindo a LGPD, impactam especialmente os processos de auditoria (*due diligence*) realizados por potenciais adquirentes em empresas-alvo. Nessa etapa, a empresa-alvo divulga para a potencial adquirente informações sensíveis sobre seus negócios e contingências associadas a ele, como forma de dar conhecimento ao adquirente sobre a empresa ou ativo a ser adquirido, reduzir (ainda que parcialmente) a assimetria informacional entre os atuais "donos" do negócio e o investidor ou comprador e confirmar (ou forçar o ajuste) das premissas do *valuation* preliminar elaborado por ele.

Por um lado, uma noção mais geral de privacidade está no radar de advogados e assessores empresariais responsáveis pela organização de processos de auditoria. Pela própria sensibilidade da abertura de informações estratégicas da empresa-alvo a um terceiro, bem como pelo caráter sigiloso atribuído a aquisições de empresas, com vistas a inibir o assédio de concorrentes, é comum que os documentos preliminares ao início da auditoria e das negociações da operação celebrados pelas partes envolvidas (como memorandos de entendimentos, *term sheets* ou cartas de intenções) prevejam cláusulas vinculantes de confidencialidade, ou mesmo que acordos de confidencialidade específicos sejam celebrados. Também é comum que a disponibilização de documentos e informações da empresa-alvo seja realizada por meio de plataformas virtuais seguras (*virtual data rooms*), como forma de limitação do número de assessores que terá acesso a tais informações e de proteção contra eventuais vazamentos e incidentes de segurança.

Por outro lado, as exigências específicas da LGPD ultrapassam, e potencialmente conflitam, com a preservação da confidencialidade no compartilhamento de informações qualificadas como dados pessoais e, sobretudo, dados pessoais sensíveis. Um ponto central de preocupação é que, caso envolva o compartilhamento de determinadas bases de dados referentes a pessoas naturais da empresa-alvo (que podem se referir a colaboradores, clientes, fornecedores, consumidores ou parceiros de negócios), o processo de auditoria configura um tratamento de dados pessoais, que demanda, nos termos da LGPD, justificação adequada e, em especial, *transparência aos titulares de dados* – observada a preservação do "segredo comercial" (art. 6º, VI, LGPD).

Ainda, como indicado na Seção anterior, o grau de adequação da empresa-alvo às exigências da LGPD pode ter impacto relevante no *valuation*, em especial para empresas do meio digital, cuja geração de receita esteja diretamente associada ao tratamento de dados pessoais. Assim, a entrada em vigor da LGPD força a inclusão de questionários referentes à proteção de dados nos processos de auditoria, como meio para testar as premissas de avaliação do valor da empresa-alvo e identificar possíveis contingências que possam reduzir o preço final a ser pago pelo adquirente[6].

Nesse sentido, a adequada observância da LGPD impacta os processos de auditoria em operações de M&A em pelo menos duas dimensões: (i) uma dimensão procedimental, referente às precauções que devem ser tomadas por ambas as partes na condução do processo de auditoria, e (ii) uma dimensão substantiva, que diz respeito à necessidade de aferição, pelo adquirente, do grau de adequação da empresa-alvo à LGPD.

Quando à dimensão procedimental, passa a ser relevante a inserção de cláusulas, nos documentos preliminares assinados pelas partes para início do processo de auditoria, referentes aos procedimentos relativos à proteção dos dados pessoais que venham a ser compartilhados pela empresa-alvo ao potencial adquirente, bem como à uma eventual regulação de responsabilidades válida entre as partes. Isso porque, a despeito de manifestações em contrário, parece claro que tanto a empresa-alvo quanto a potencial adquirente configuram-se, para fins da LGPD, como controladores a fazer uso compartilhado de dados pessoais[7], o que implica, como regra geral, responsabilidade solidária perante os titulares de dados por eventuais danos causados por uso ilegal ou incidentes de segurança (art. 42, §1º, II, LGPD). Tais cláusulas devem detalhar (i) a finalidade e a hipótese legal que justificam o compartilhamento das bases de dados pessoais, e (ii) as medidas técnicas a serem adotadas pelas partes como forma de preservar os direitos dos titulares e a segurança dos dados compartilhados.

---

[6] Fachinetti e Poggio (2020) mencionam estudo internacional elaborado pela *Forescout Technologies, Inc*, segundo o qual "53% dos entrevistados relataram que sua organização encontrou problemas ou incidentes críticos de segurança durante uma transação, resultando em risco para o negócio. O estudo também constatou que cerca de 40% das compradoras envolvidas em uma operação de M&A relataram problemas de segurança cibernética durante a integração pós-aquisição da empresa-alvo (o que poderia, no cenário ideal, ter sido constatado antes da transação)".

[7] Liberman e Eulálio (2020) entendem que o adquirente se qualifica como operador, e não controlador. Não parece adequado esse entendimento, uma vez que o adquirente não realiza o tratamento de dados (análise) recebidos da empresa-alvo *em nome* da empresa-alvo, mas sim em nome e benefício próprio.

Quanto à finalidade do compartilhamento, é intuitiva a associação dos procedimentos associados a uma operação de M&A ao interesse legítimo das empresas envolvidas (art. 7º, IX, LGPD), seja porque a possibilidade de compra e venda de empresas ou ativos configura-se como estratégia empresarial lícita e, em princípio, fundamentada pela liberdade econômica dos agentes, seja porque a utilização de outras bases legais previstas na LGPD não parece adequada às suas características. Em particular, a obtenção de consentimento prévio de titulares de dados pessoais que serão compartilhados pela empresa-alvo (cf. art. 7º, §5º, LGPD) pode inviabilizar a operação – seja pelo tempo necessário à obtenção desse consentimento, seja pela possibilidade de o titular não consentir ou revogar o consentimento a qualquer tempo.

É razoável a fundamentação do compartilhamento de dados pessoais em auditorias em operações de M&A pelo legítimo interesse das empresas envolvidas. No entanto, a adequada utilização do legítimo interesse como base legal exige cautela. Em primeiro lugar, pelo fato de o legítimo interesse não ser uma hipótese legal que autoriza o compartilhamento de dados pessoais sensíveis. Nesse sentido, tais dados devem ser segregados e não apresentados ao adquirente caso não seja obtido consentimento prévio específico dos titulares (ou caso o consentimento inicialmente fornecido pelos titulares já contemple a possibilidade de compartilhamento com terceiros em casos de auditoria legal).

A doutrina e a prática internacional apontam para a importância de se promover um "teste" sequencial para a aplicação do legítimo interesse, o qual exige (i) identificação do interesse do(s) controlador(es) dos dados na situação concreta, (ii) verificação da necessidade de utilização do interesse como base legal *vis-à-vis* outras bases legais, (iii) balanceamento do interesse identificado com os impactos à privacidade dos titulares (em especial, *a expectativa razoável* de tais titulares quanto ao tratamento de seus dados), e (iv) previsão de salvaguardas aos interesses dos titulares, como *transparência* e mecanismos de mitigação dos riscos envolvidos[8]. Enquanto as duas primeiras etapas são razoavelmente atendidas nas circunstâncias de uma operação de M&A, conforme exposto acima, as duas últimas impõem medidas adicionais àquelas comumente empregadas nas fases preliminar e de negociação das operações, em especial para a empresa-alvo.

[8] Com base no guia de recomendações do Information Commissioner's Office (ICO) do Reino Unido (disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/#ib4, último acesso em 13.12.2020), em Maia (2020) e nas aulas do curso de Lei Geral de Proteção de Dados.

É de se verificar que a venda ou alteração de controle (societário) de uma empresa é um evento relevante e relativamente raro em seu ciclo de existência. Assim, é contestável a noção de que o compartilhamento de dados por uma empresa com um potencial adquirente atende as "expectativas razoáveis" dos titulares dos dados compartilhados. Como forma de atendimento ao princípio da transparência, é recomendável que as políticas de privacidade da empresa-alvo, divulgadas aos titulares, bem como os termos de consentimento específicos firmados pelos titulares (quando o consentimento for a base de tratamento) prevejam a possibilidade de compartilhamento dos dados com terceiros para fins de avaliação do interesse na aquisição da empresa controladora (dos dados). Trata-se de uma possibilidade de conciliação entre a transparência necessária aos titulares e a preservação da confidencialidade – ou do "segredo comercial" – sobre o interesse da empresa em envolver-se em uma operação de M&A.

Uma segunda salvaguarda é a limitação, pela empresa-alvo, do compartilhamento de dados ao mínimo possível e necessário para a avaliação do potencial adquirente. Esse é um ponto relevante para as negociações dos documentos preliminares ao início da auditoria, uma vez que é comum que potenciais adquirentes (e seus advogados) façam uso de listas padrão e genéricas de solicitação de documentos e informações. A indicação e negociação prévia de quais dados são efetivamente necessários pode minimizar o risco de compartilhamento desnecessário de dados, em atenção ao princípio da necessidade (art. 6º, III, LGPD).

Adicionalmente, é de se aventar a possibilidade de pseudonimização das bases de dados a serem compartilhadas pela empresa-alvo[9], como forma de preservar informações desnecessárias para a avaliação do adquirente. Vale notar que a pseudonimização não descaracteriza os dados compartilhados como dados pessoais, sendo uma técnica menos protetiva do que a anonimização, e oferece uma garantia menos robusta do que anonimização no que diz respeito à possibilidade de reversão e identificação dos titulares. No entanto, caso associada a uma obrigação contratual imposta à empresa adquirente que lhe proíba de intentar

[9] Sugestão aplicável às bases de dados não anonimizadas (dado que, para bases de dados anonimizadas, nem mesmo o próprio controlador original teria capacidade de identificar os respectivos titulares). A pseudonimização envolve a utilização de técnicas que "mascarem" parte dos dados para terceiros, sendo que a reversão e recomposição dos dados originais depende de informação adicional mantida apenas pelo controlador (*e.g.* mediante uso de criptografia com chave privada ou funções *hash*), cf. art. 13, §4º, LGPD. A diferença entre anonimização e pseudonimização é bem explicada pela *Opinion 05/2014* do Working Party (EU) (disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, último acesso em 13.12.2020).

a reversão do processo (*e.g.* por meio de força bruta), a pseudonimização pode configurar uma salvaguarda adicional à preservação da privacidade dos titulares de dados.

Ainda, a fundamentação do compartilhamento de bases de dados no legítimo interesse torna recomendável a elaboração de um relatório de impacto à proteção de dados pessoais, dada a faculdade conferida pela LGPD à ANPD de exigir tais relatórios, em especial nas situações em que se utiliza o legítimo interesse como base jurídica do tratamento (cf. art. 10, §3º, LGPD). Tal relatório deverá descrever os tipos de dados compartilhados e a adoção dos procedimentos indicados acima, como salvaguardas à proteção de dados pessoais dos titulares (cf. art. 38, *caput*, LGPD).

Quanto à dimensão substancial, o início das atividades da ANPD e a provável atenção especial conferida por autoridades como o Ministério Público e os próprios titulares no que diz respeito à proteção de dados pessoais torna ainda mais relevante uma auditoria cuidadosa, pelo adquirente, que questione a empresa-alvo sobre sua adequação (ou, ao menos, os passos dados em direção à adequação) à LGPD. Vale ressaltar que precedentes internacionais indicam que o adquirente, mesmo após a consumação da operação, pode vir a ser responsabilizado por incidentes de segurança da empresa adquirida ocorridos *antes* da aquisição, em função de não ter realizado uma auditoria intensiva o suficiente para identificar tais incidentes e possibilitar a adoção de medidas corretivas o mais rápido possível[10].

Advogados com experiência em auditorias jurídicas têm indicado que bons pontos de partida para a investigação do adquirente são o último mapeamento de dados tratados elaborado pela empresa-alvo, as políticas de privacidade compartilhadas com titulares de dados e as políticas internas referentes ao manejo e segurança de dados implementadas pela empresa-alvo (Shah, Bacal e Forester, 2019; Pessoa, 2019). A inexistência desses documentos, por si só, configura indício de uma abordagem pouco preocupada com a proteção de dados por parte da empresa-alvo.

[10] Em outubro de 2020, o Information Commissioner's Office (ICO) do Reino Unido multou a rede hoteleira Marriott em £18,4 milhões por um incidente de segurança que implicou vazamento de dados pessoais de mais de 300 milhões de hóspedes. A falha foi detectada em 2018, mas se estendeu desde o ano de 2014, e envolvia os sistemas de informação da rede Starwood, adquirida pela Marriott em 2016. Na notificação de imposição da multa, consta que a Marriott declarou não ter tido "tempo hábil" para conduzir uma auditoria completa na Starwood que incluísse revisão de seus procedimentos de segurança da informação, tendo confiado nas informações fornecidas apenas pela administração da Starwood. Notificação disponível em https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf, último acesso em 13.12.2020.

Ainda que tais documentos existam, recomenda-se uma abordagem não formalista, que procure identificar o efetivo cumprimento das medidas previstas nas políticas e a consistência do mapeamento de dados. Entrevistas com os responsáveis internos pela gestão e *compliance* de políticas de dados – em especial os encarregados, quando nomeados – podem ser um caminho de confirmação ou identificação de lacunas e inconsistências nos procedimentos adotados pela empresa-alvo. Adicionalmente, é recomendável que as auditorias não se restrinjam aos aspectos jurídicos, mas também adentrem, com a assessoria de profissionais com qualificação específica, os detalhes técnicos que permitam aferir a robustez dos programas de segurança implementados e o histórico de incidentes de segurança.

A análise dos documentos disponibilizados, em especial do mapeamento, deverá atentar para as bases legais que fundamentam as operações de tratamento realizadas pela empresa-alvo. Tratamentos baseados no consentimento dos titulares demandarão precauções do adquirente a depender da estrutura da operação, incluindo verificação sobre registros adequadso de gerenciamento de tais consentimentos pela empresa-alvo. Caso a operação seja estruturada como uma aquisição de ativos, ou de apenas parcela das unidades de negócio da empresa-alvo (*e.g.* por meio de cisão parcial da empresa-alvo, com versão das bases de dados para a adquirente), esta implicará alteração do controlador (para fins da LGPD)[11] e demandará comunicação aos titulares, que poderão revogar o consentimento inicialmente fornecido[12].

3. Impactos sobre os contratos da operação

Finalmente, as precauções referentes à proteção de dados pessoais derivadas da LGPD terão impacto também sobre os contratos que estruturam as operações de M&A, sejam contratos de compra e venda de participação societária (quotas ou ações), sejam contratos de compra e venda de ativos. O ponto central diz respeito à alocação dos riscos identificados no processo de

[11] Curiosamente, nesses casos não se verificaria alteração do controle *societário* da empresa-alvo, mas apenas do controlador dos dados. Aquisições de controle societário, por sua vez, tendem a não alterar (ao menos em princípio) o controlador dos dados, caso a personalidade jurídica da empresa-alvo seja preservada. Uma discussão interessante, que não é abordada neste artigo, diz respeito ao poder do novo controlador (societário) determinar as decisões administrativas da empresa adquirida. Para fins da LGPD, o controlador é definido como a pessoa jurídica a quem competem as decisões de tratamento de dados. É possível, portanto, a depender do grau de influência do novo controlador societário sobre as atividades da empresa adquirida, que o controlador societário possa também vir a ser considerado controlador de dados, ainda que a personalidade jurídica da adquirida seja preservada.

[12] O que pode, a depender da quantidade e da sensibilidade dos dados tratados, vir a impactar a própria estrutura da operação, cf. nota Pessoa (2019).

auditoria (que podem ser, inclusive, refletidos no preço final a ser pago pela adquirente, cf. Seção 1, acima) por meio da repartição contratual de responsabilidades. Destacam-se três dimensões principais: (i) declarações e garantias, (ii) indenização por eventual desconformidade da empresa-alvo em relação à LGPD ou por incidentes de segurança derivados, e (iii) eventual período de adequação da empresa-alvo à LGPD antes ou após a aquisição.

Cláusulas de declarações e garantias são usuais em contratos definitivos de operações de M&A e servem, essencialmente, para que a empresa-alvo e/ou os vendedores do ativo ou da participação societária atestem a veracidade e a completude das informações fornecidas ao adquirente ao longo do processo de auditoria. É relevante que o contrato da operação preveja declarações específicas dos vendedores e/ou da empresa-alvo sobre a aderência às exigências da LGPD, como forma de confirmar as informações fornecidas e dar conforto adicional ao adquirente. Exemplos[13] de declarações que podem ser previstas são (i) garantia de que a operação da empresa-alvo, ativo ou linha de negócios está em conformidade com as políticas escritas apresentadas ao adquirente, (ii) inexistência de investigações ou comunicações de autoridades (*e.g.* Ministério Público e, futuramente, ANPD) relativas a tratamentos de dados ilegais ou incidentes de segurança, (iii) inexistência de restrições legais à cessão e transferência das bases de dados objeto de aquisição, e (iv) inexistência de incidentes de segurança, perda, vazamento ou divulgação não autorizada de dados pessoais ou dados pessoais sensíveis. Eventuais exceções a tais declarações devem ser comunicadas previamente ao adquirente e, geralmente, listadas em documentos anexos ao contrato principal da operação.

Cláusulas de indenização também poderão exigir negociação estendida. É comum que os vendedores da empresa ou do ativo assumam a responsabilidade de indenizar o adquirente por contingências relacionadas a eventos ocorridos ou decisões tomadas antes da consumação da operação – não respondendo por eventos futuros, posteriores à venda da empresa ou do ativo. No entanto, especificamente no que diz respeito à proteção de dados, é possível, por exemplo, que vulnerabilidades em sistemas de segurança permaneçam não detectadas por um período razoável, estendendo-se pelo período anterior e posterior à operação[14]. Ainda, sobretudo para

[13] Cf. Shah, Bacal e Forester (2019).
[14] Como ocorrido no caso Marriott, referido na nota de rodapé 10 acima. Vale ressaltar que a definição ampla de "tratamento" da LGPD impõe dificuldade em precisar um momento preciso em que ocorre o tratamento. Assim,

empresas-alvo com baixo grau de adesão às exigências da LGPD, é de se esperar que a implementação das medidas de adequação fique a cargo do adquirente, após a operação.

Ambos os exemplos dizem respeito a situações de desconformidade com a LGPD que se estendem desde antes até após a operação, e podem gerar disputas sobre a repartição e limitação das responsabilidades entre as partes. Uma possibilidade de conciliação de interesses é a previsão de um período adicional de transição (*e.g.* 6 meses), posterior à operação, em que os vendedores permanecem obrigados a indenizar eventuais contingências da empresa-alvo relativas à proteção deficiente de dados. Nesse período, o adquirente estaria obrigado, já com o controle da empresa, a auditar em maior detalhe os sistemas de segurança e/ou implementar as medidas de adequação da empresa à LGPD.

Conclusão

As ainda recentes leis e regulações de proteção de dados pessoais vêm forçando advogados e outros profissionais que atuam em processos de M&A a ampliar seu leque de preocupações, tanto para os processos de setores econômicos ditos tradicionais como, e em especial, para os processos que envolvem empresas que atuam no ambiente digital e têm como núcleo de sua atividade o tratamento intensivo de dados pessoais. A LGPD não é exceção. Este artigo procurou apresentar uma primeira reflexão sobre os impactos mais evidentes da LGPD sobre as fases principais de processos de M&A no Brasil e apontar recomendações específicas, que exigem, em linhas gerais, que os profissionais envolvidos em tais processos "saiam do piloto automático" e revisem algumas práticas assentadas ao longo dos anos.

Em primeiro lugar, a LGPD deverá forçar analistas e assessores financeiros a incluir, nos modelos de *valuation*, premissas relativas ao grau de adequação da empresa-alvo às exigências referentes a proteção de dados. Essa tarefa, complexa *per se*, será ainda mais difícil nos primeiros anos de vigência da lei, quando a ANPD e o poder judiciário ainda começarão a assentar a sua interpretação e os montantes das penalidades aplicáveis a infrações.

---

ainda que um dado tenha sido coletado, irregularmente, em momento prévio à aquisição, o *uso* desse dado em momento posterior à aquisição será maculado pela irregularidade anterior.

Em segundo lugar e, acredita-se, como impacto principal, a necessidade de precaução relativa à proteção de dados forçará uma ampliação de escopo dos processos de auditoria jurídica. Será necessário que advogados e assessores se debrucem, dentre outros documentos, sobre as políticas de privacidade e proteção de dados e sobre os contratos que envolvem obrigações tratamento de dados pessoais, mas também sobre questões técnicas relativas à robustez dos sistemas de segurança de informação. A abordagem deverá abandonar um formalismo costumeiro (modelo "*check-box*") e buscar compreender a compatibilidade (ou não) do discurso e da prática das empresas-alvo.

Por fim, pela natureza das vulnerabilidades de sistemas informáticos de segurança e pela pouca idade da LGPD, questões envolvendo proteção de dados podem vir a exigir tratamento específico e negociação prolongada entre as partes envolvidas em um processo de M&A, dando margem para soluções inovadoras que permitam uma alocação justa dos riscos decorrentes nos contratos definitivos das operações.

Bibliografia

CARNEIRO, Isabelle da Nóbrega Rito, DEPS, Guilherme. "Na era dos dados, como ficam as operações de fusões e aquisições?" Portal JOTA, 04.05.2020, disponível em https://www.jota.info/opiniao-e-analise/colunas/regulacao-e-novas-tecnologias/na-era-dos-dados-como-ficam-as-operacoes-de-fusoes-e-aquisicoes-04052019 (último acesso em 13.12.2020)

DATA PROTECION WORKING PARTY, "Opinion 05/2014 on Anonymisation Techniques", disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (último acesso em 13.12.2020)

FACHINETTI, Aline Fuke, POGGIO, Gustavo Massaini. "Proteção de dados, due diligence e novos negócios". Portal JOTA, 06.08.2020, disponível em https://www.jota.info/opiniao-e-analise/artigos/protecao-de-dados-due-diligence-e-novos-negocios-06082020#_ftn2 (último acesso em 13.12.2020)

FRAJHOF, Isabella Z., SOMBRA, Thiago Luís. "A transferência internacional de dados pessoais" In MULHOLLAND, Caitlin (org.). ***A LGPD e o marco normativo no Brasil.*** **Porto Alegre: Arquipélago, 2020 (Edição do Kindle).**

LIBERMAN, Tania, EULÁLIO, Amanda. "A LGPD nas operações de M&A". Valor Econômico, 16.07.2020, disponível em https://valor.globo.com/legislacao/noticia/2020/07/16/a-lgpd-nas-operacoes-de-m-a.ghtml?GLBID=16320c8067984e2bbc4042331ff37eed5326d58795642736d67674f632d5f732d4e39735a4d42503257374654644e6151765643644c7643544d5542546953454a4f4c4545576c4e535248324469443043445971692d57436e44796178667941624 14b563039773d3d3a303a75676661776f6c6f7066646d71746977636f666d (último acesso em 13.12.2020).

MAIA, Roberta Mauro Medina. "O legítimo interesse do controlador e o término do tratamento de dados pessoais" In MULHOLLAND, Caitlin (org.). ***A LGPD e o marco normativo no Brasil.*** **Porto Alegre: Arquipélago, 2020 (Edição do Kindle).**

PESSOA, Daniel Tardelli. "Operações de Fusões em Aquisições e a Lei Geral de Proteção de Dados Pessoais. Levy & Salomão Advogados – Boletim Jurídico, Agosto 2019, disponível em https://www.levysalomao.com.br/publicacoes/boletim/operacoes-de-fusoes-e-aquisicoes-e-a-lei-geral-de-protecao-de-dados-pessoais (último acesso em 13.12.2020)

PIERI, José Eduardo. "Efeitos da Lei de Proteção de Dados em operações de M&A". Revista Capital Aberto, 18.01.2019, disponível em https://capitalaberto.com.br/secoes/artigos/efeitos-da-lei-de-protecao-de-dados-em-operacoes-de-ma/ (último acesso em 13.12.2020)

SHAH, Pritesh, BACAL, Matthew, FORESTER, Daniel. "Data Privacy and Cybersecurity in Global Dealmaking" in PEARCE, Will, BICK, John (Davis Polk & Wardwell LLP). ***Getting the Deal Through: Private M&A 2020.*** **Disponível em https://www.davispolk.com/files/ma2020data_privacy.pdf (último acesso em 13.12.2020)**

--*