UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
FACULDADE DE DIREITO
DEPARTAMENTO DE DIREITO PRIVADO E PROCESSO CIVIL

Yasmin Carolina do Amaral Pires Cannavo

A APLICAÇÃO DA NOVA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) EM OPERAÇÕES DE FUSÕES E AQUISIÇÕES

Porto Alegre
2023

Yasmin Carolina do Amaral Pires Cannavo

A APLICAÇÃO DA NOVA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) EM OPERAÇÕES DE FUSÕES E AQUISIÇÕES

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais na Universidade Federal do Rio Grande do Sul.

Orientador: Professor Doutor Fabiano Menke.

Porto Alegre
2023

FICHA CATALOGRÁFICA

CIP - Catalogação na Publicação

do Amaral Pires Cannavo, Yasmin Carolina
A APLICAÇÃO DA NOVA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) EM OPERAÇÕES DE FUSÕES E AQUISIÇÕES / Yasmin Carolina do Amaral Pires Cannavo. -- 2023.
73 f.
Orientador: Fabiano Menke.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Faculdade de Direito, Curso de Ciências Jurídicas e Sociais, Porto Alegre, BR-RS, 2023.

1. Lei Geral de Proteção de Dados. 2. Autoridade Nacional de Proteção de Dados. 3. Due Dilligence. 4. Mitigação de riscos. 5. LGPD. I. Menke, Fabiano, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

Yasmin Carolina do Amaral Pires Cannavo

A APLICAÇÃO DA NOVA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) EM OPERAÇÕES DE FUSÕES E AQUISIÇÕES

Trabalho de Conclusão de Curso apresentado como requisito parcial para a obtenção do grau de Bacharel em Ciências Jurídicas e Sociais na Universidade Federal do Rio Grande do Sul.

Orientador: Professor Doutor Fabiano Menke.

Aprovada em 11 de setembro de 2023

BANCA EXAMINADORA

Prof. Dr. Fabiano Menke

Orientador

Nome e titulação do membro da banca

Instituição do membro da banca

Nome e titulação do membro da banca

Instituição do membro da banca

RESUMO

O presente trabalho tem como objetivo principal descobrir quais principais pontos de atenção em processos de fusões e aquisições - F&A's de empresas de forma a facilitar as operações e promover segurança jurídica na aplicação da LGPD. Como um objetivo complementar, se analisa o momento atual da Autoridade Nacional de Proteção de Dados – ANPD, buscando explorar formas pelas quais a ANPD pode se fortalecer no cenário brasileiro, para uma eficaz proteção dos titulares de dados. Para tanto, dividiu-se o trabalho em três partes. Em primeiro momento, delimita-se o processo de F&A's em suas principais fases: pré-contratual e *duo dilligence;* negociação e aquisição; e integração e pós-aquisição. Em cada fase se explora os momentos de maior relevância quando se trata de conformidades com a LGPD. Na segunda parte, aborda-se os principais desafios para a proteção de dados em F&A's, tanto do lado empresarial como do lado regulatório. Na terceira e última parte, apresenta-se os principais elementos-chave para que uma fusão ou aquisição esteja em conformidade com as leis de proteção de dados. Esse estudo proporciona um entendimento aprofundado das implicações da LGPD nas F&A's e oferece orientações para que as empresas realizem essas operações com conformidade e respeito aos direitos dos titulares de dados. A pesquisa tem o potencial de contribuir significativamente para a prática de F&A no contexto das regulamentações de proteção de dados, além de oferecer sugestões para o fortalecimento da ANPD e a eficácia de suas atividades regulatórias.

Palavras-chave: Lei Geral de Proteção de Dados; Fusões e Aquisições; Autoridade Nacional de Proteção de Dados; *Due Dilligence*; Mitigação de riscos; LGPD.

ABSTRACT

The main objective of this work is to discover the main points of attention in mergers and acquisitions processes - M&A's of companies in order to facilitate operations and promote legal certainty in the application of the LGPD. As a complementary objective, the current situation of the National Data Protection Authority – ANPD is analyzed, seeking to explore ways in which the ANPD can strengthen itself in the Brazilian scenario, for effective protection of data subjects. To this end, the work was divided into three parts. Firstly, the M&A process is delimited into its main phases: pre-contractual and due diligence; negotiation and acquisition; and integration and post-acquisition. At each stage, the most relevant moments when it comes to compliance with the LGPD are explored. The second part addresses the main challenges for data protection in M&A's, both on the business and regulatory sides. The third and final part presents the main key elements for a merger or acquisition to comply with data protection laws. This study provides an in-depth understanding of the implications of the LGPD on M&A's and offers guidance for companies to carry out these operations with compliance and respect for the rights of data subjects. The research has the potential to contribute significantly to the practice of M&A in the context of data protection regulations, in addition to offering suggestions for strengthening the ANPD and the effectiveness of its regulatory activities.

Keywords: General Data Protection Law; Mergers and Acquisitions; National Data Protection Authority; Due Diligence; Risk Mitigation; LGPD.

AGRADECIMENTOS

Expresso meus sinceros agradecimentos a todas as pessoas que contribuíram para a realização deste trabalho e para meu crescimento profissional e acadêmico ao longo do curso de direito. O que aprendi durante os últimos anos como estudante nessa querida Universidade foi muito além do direito em si, formando muito de quem sou e de quem serei no futuro.

Meu mais profundo agradecimento é direcionado à minha mãe, Cintia Cristina do Amaral Pires Cannavo, ao meu pai, Telmo Bittencourt Cannavo, aos meus irmãos e a toda minha família. Seu constante incentivo, encorajamento e apoio foram a âncora que me sustentou durante minha jornada na faculdade. Ao crescer e evoluir como indivíduo ao longo dos anos, reconheço o privilégio de ter uma família que cresceu comigo, oferecendo força e coragem para superar os desafios que surgiram no caminho.

Devo muito aos meus orientadores de estágio, mentores e professores, cuja orientação e conhecimento foram fundamentais para moldar minha compreensão e aprofundamento no tema abordado nesta monografia. Agradeço também aos coordenadores de atividades extracurriculares, como o NEDEP, GDO e Competições, por proporcionarem oportunidades enriquecedoras que expandiram minha visão acadêmica e profissional. Espero que essa universidade tenha cada vez mais envolvidos na promoção do livre acesso ao conhecimento e de espaços mais inclusivos e acessíveis para indivíduos de todas as origens sociais.

Não posso deixar de expressar minha profunda apreciação por aqueles que compartilharam amizade e conselhos valiosos ao longo dessa jornada. Suas palavras e experiências moldaram minha perspectiva acadêmica e profissional, e essas lições serão carregadas comigo ao longo da vida.

Obrigada!

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Foi em outubro de 1972 a primeira bem-sucedida demonstração pública da ARPANET, predecessora da internet como a conhecemos. Mesmo ano em que o correio eletrônico foi introduzido, dando início aos princípios da nossa atual "World Wide Web"[1]. Com o desenvolvimento de pesquisa e avanços nos protocolos, em 1985 as tecnologias necessárias para popularização da internet já estavam estabelecidas.

No artigo publicado pela *Internet Society* em 2003, *"Uma breve história da internet"*, os autores falam de como o acesso público e gratuito a documentos básicos, pesquisas, dúvidas, especificações e protocolos, foi um dos motivos pelos quais a internet pôde se desenvolver de forma tão rápida e eficaz[2]. Pode-se dizer que, desde seu princípio, o sucesso da internet foi altamente impulsionado pela publicidade e acessibilidade à informação.

A criação da internet e sua extrema popularização no século XXI trouxeram consigo uma imensa quantidade de dados públicos e privados que se encontram a um clique de distância de seus agentes de coleta e/ou tratamento[3].

A internet, outrora uma mera plataforma para troca de informações, evoluiu para um verdadeiro universo paralelo no qual os cidadãos mergulham durante grande parte do seu dia a dia. Presente no trabalho, comunicação, entretenimento, educação, vida civil e em praticamente todas as esferas da vida moderna, a internet possibilita a coleta incessante de dados. O cidadão moderno, usuário dessa ferramenta quase indispensável, tem sua vida registrada e armazenada por centenas ou até milhares de entidades interessadas, por meio de caches, *cookies* e outras formas de armazenamento de dados.

Não há dúvidas de que o advento da digitalização na vida moderna trouxe à tona uma multiplicidade de redes sociais, aplicativos e websites que oferecem conteúdo, entretenimento, educação e diversos outros serviços aparentemente gratuitos, mas com uma contrapartida oculta. Em troca do acesso a esses recursos, as empresas por trás dessas plataformas têm o poder

---

[1] LEINER, Barry M. *et al*. A brief history of the Internet. **ACM SIGCOMM Computer Communication Review**, v. 39, n. 5, p. 22-31, 2009.

[2] "A key to the rapid growth of the Internet has been the free and open access to the basic documents, especially the specifications of the protocols.(...)" LEINER, Barry M. *et al*. A brief history of the Internet. **ACM SIGCOMM Computer Communication Review**, v. 39, n. 5, p. 22-31, 2009. p. 28.

[3] Tratamento de dados, segundo a LGPD, é "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" BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

de coletar e analisar minuciosamente os dados de seus usuários, utilizando essas informações para personalizar anúncios e publicidades de maneira a persuadir e influenciar cada usuário de forma individualizada.

As preocupações em relação à proteção dos dados pessoais, especialmente com a expansão da internet e a facilidade de acesso às informações, chamaram a atenção de organizações internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que em 1980 começou a desenvolver as "Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais"[4] (as "Diretrizes sobre a Privacidade"), buscando estabelecer princípios e padrões internacionais para garantir a privacidade e a segurança dos dados em uma era digital em rápido crescimento.

Essas diretrizes, adotadas em 1980 e revisadas posteriormente, foram e continuam sendo fundamentais para a proteção de dados pessoais em contextos globais, buscando promover a cooperação internacional e a harmonização das legislações sobre privacidade. Com base nesses preceitos, os países membros da OCDE buscam desenvolver suas próprias leis e regulamentações de proteção de dados, alinhando-se de maneira a facilitar o fluxo seguro de informações entre fronteiras.

O controle e a influência exercidos pelas denominadas "Big Techs" - como a Alphabet (controladora do Google), a Meta (proprietária do Facebook, Instagram e outras) e gigantes como Microsoft e Amazon - sobre o cidadão moderno são questões complexas que merecem uma análise mais aprofundada. O faturamento anual de algumas dessas empresas ultrapassa o Produto Interno Bruto (PIB) de muitos países, enquanto os termos de uso dessas plataformas são frequentemente alterados, deixando o usuário com pouco entendimento sobre o que está realmente consentindo. Além disso, indivíduos comuns têm sua carreira e subsistência cada vez mais vinculadas as suas identidades online e ao uso de redes e plataformas digitais, o que levanta importantes questões sobre competitividade, privacidade, transparência e proteção dos dados pessoais.

Segundo Bruno Miragem, o acesso e a utilização dos dados pessoais são considerados um dos principais ativos empresariais na sociedade contemporânea, mas também representam uma preocupação em relação aos riscos à privacidade do titular de dados (consumidor) diante das novas tecnologias da informação[5].

---

[4] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICOS. **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais.** [s.l.], 2002. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 02 jul. 2023.

[5] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, São Paulo, v. 108, n. 1009, p. 173-222, nov. 2019. p. 1.

Para enfrentar o desafio de salvaguardar esses dados, foi promulgada no Brasil, em 14 de agosto de 2018, a Lei 13.709, chamada Lei Geral de Proteção de Dados Pessoais (LGPD). Tal norma, amplamente inspirada na tradição europeia de dados, a qual deu origem à *General Data Protection Regulation* (GDPR), que entrou em vigor em 25 de maio de 2018[6], visa proporcionar um arcabouço legal robusto para a proteção dos dados pessoais no cenário brasileiro.

De acordo com o artigo 1º da LGPD, essa lei tem como objetivo proteger os dados de pessoas físicas. O inciso I do art. 5º define "dados pessoais" como "informação relacionada a pessoa natural identificada ou identificável". Sendo assim, as pessoas jurídicas não são as beneficiadas pelas proteções da LGPD[7]. A Lei concentra-se na proteção dos dados pessoais de indivíduos identificáveis, assegurando sua privacidade e segurança[8]. Segundo Sérgio Branco:

> Isso não significa dizer que os dados das pessoas jurídicas careçam de proteção. Afinal, se as pessoas jurídicas podem ser amparadas pelos direitos de personalidade, gozarão da proteção respectiva no que diz respeito, por exemplo, ao direito à privacidade. Além disso, dados de pessoas jurídicas encontram também tutela, por exemplo, na Lei nº 9.279/96, a lei de propriedade industrial, nos termos das regras de concorrência desleal quanto à proteção de segredos industriais e segredos de negócio". Ainda assim, a LGPD limita-se a proteger os dados pessoais de pessoas físicas, não de pessoas jurídicas.[9]

A lei engloba casos em que a operação de tratamento ocorra no território nacional, quando os dados pessoais em questão tenham sido coletados no território nacional, e situações em que a atividade de tratamento vise a oferecer bens ou serviços ou a tratar dados de indivíduos no território nacional. Vale ressaltar que a LGPD também alcança qualquer pessoa física que realize tratamento de dados pessoais de forma habitual e com fins econômicos.

Com o intuito de garantir a conformidade com a LGPD, as organizações são obrigadas a nomear um encarregado de proteção de dados[10], que atua como canal de comunicação entre

---

[6] Council Regulation 2016/679, 2016 O.J. (L 119/1); ver também EUROPEAN COMMISSION. **The GDPR:** new opportunities, new obligations. Luxemburgo, 2018. Disponível em: https://ec.europa.eulcommission/sites/beta-political/files/data-protection-factsheet-sme-obligations-en.pdf. Acesso em: 13 jul. 2023.

[7] "A proteção conferida pela LGPD não se estende às pessoas jurídicas, tendo em vista sua finalidade de proteger a pessoa natural" BRASIL. **IX Jornada de Direito Civil:** Enunciados aprovados. Brasília, 2022. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 22 ago. 2023.

[8] BRANCO, Sérgio. As hipóteses de aplicação da LGPD e as definições legais. In: MULHOLLAND, Caitlin (Ed**.). A LGPD e o novo marco normativo no Brasil.** [s.l.]: Arquipélago Editorial, 2020.

[9] *Ibidem.*

[10] Conforme o art. 5º da LGPD: VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados[11]. Essa figura desempenha um papel crucial na supervisão e no monitoramento das práticas de proteção de dados dentro das organizações. Esse cuidado preventivo será de suma importância para garantir a regularidade das práticas neste campo, evitando possíveis sanções legais.

Já no que se refere à proteção de dados em casos de Fusões e Aquisições (F&A ou M&A's, do inglês *Mergers and aquisitions*)[12], a aplicação dessa Lei apresenta vários desafios, entre eles o de entender quais são as obrigações institucionais do agente de tratamento[13] nessas operações, e a forma de fiscalização e regularização pelo Estado.

Ao falar em operações de M&A é muito comum que haja um foco maior na área financeira e negocial, desde a etapa de pré-aquisição até a integração pós aquisição. Todavia, à medida que avanços tecnológicos e regulatórios se tornam mais presentes, é essencial que os agentes envolvidos nessas operações compreendam suas limitações e responsabilidades em relação ao acesso e tratamento de dados.

As empresas envolvidas nessas operações frequentemente buscam adquirir não apenas a infraestrutura e os ativos de uma organização-alvo, mas também seus bancos de dados e participação no mercado, o dito *marketshare*. Isso torna imprescindível uma análise cuidadosa sobre como o compartilhamento, a transferência e a utilização desses dados podem ser conduzidas em conformidade com a LGPD, salvaguardando a proteção e a privacidade dos dados pessoais dos indivíduos.

Ao iniciar a pesquisa bibliográfica para essa monografia, o objetivo seria clarificar o processo de fusão e aquisição de empresas de forma a facilitar as operações e promover segurança jurídica na aplicação da LGPD.

No entanto, diante do cenário atual em matéria de proteção de dados, parece evidente que quem mais está precisando de segurança jurídica quando se trata de M&A's e outras operações entre *big-techs* são os titulares de dados, que estão mais vulneráveis nesse contexto.

11

12 Operações de M&A podem englobar diversas modalidades, como a aquisição de quotas ou ações, e a incorporação, a depender do formato societário em questão. Além disso, no âmbito das operações de M&A pode se estender para a aquisição de ativos específicos, representando um interesse por ativos tangíveis ou intangíveis que compõem o patrimônio de uma empresa. Além disso, reorganizações societárias como fusões e cisões também são cenários que merecem destaque, assim como as Joint Ventures. Na maioria das vezes em que se citar o termo M&A's ou F&A's nesse trabalho se estará referindo ao caso de uma transferência completa das operações da adquirida para a adquirente. No entanto, os fundamentos, princípios e conclusões podem ser aplicados em outros tipos de fusões e aquisições conforme as circunstâncias.

13 Conforme o artigo 5º da LGPD, o termo "agente de tratamento" se refere à junção da figura de controlador (VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais) e operador (VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador).

Dessa forma, além de mapear o processo de M&A conforme inicialmente planejado (seções 2 e 4), este trabalho também busca propor sugestões à ANPD em conjunto com outros órgãos para a efetiva fiscalização dessas operações (seção 3), o que envolve não apenas segurança e proteção de dados, mas também questões de direito concorrencial e consumerista. Através dessa abordagem, busca-se não somente facilitar a proteção de dados em operações de fusões e aquisições, mas também garantir que os direitos dos titulares de dados sejam respeitados e preservados em consonância com a legislação vigente.

É extremamente necessário diminuir a lacuna de conhecimento em relação à aplicação da nova Lei Geral de Proteção de Dados em casos de fusões e aquisições, com foco especial nas aquisições e incorporações entre empresas do setor de tecnologia. Essa missão envolve não apenas o entendimento das medidas que os agentes de tratamento devem tomar, como também as formas de fiscalização e punição que o Estado deve aplicar em casos de desobediência.

Para alcançar esse objetivo, serão estudadas as principais etapas do processo de aquisição e seus desafios quanto à aplicação da LGPD, utilizando pesquisas bibliográficas e análises de casos anteriores de fusões e aquisições, examinando a jurisprudência e a interpretação doutrinária. Com isso se responderá à pergunta de pesquisa: quais são os momentos mais importantes dentro do processo de fusões e aquisições para que haja o devido *compliance* em proteção de dados conforme a LGPD?

Ao final, espera-se oferecer contribuições para o aprimoramento das práticas de fusões e aquisições, apresentando recomendações práticas para as empresas envolvidas, de modo a assegurar a conformidade com a LGPD e preservar os direitos fundamentais dos indivíduos no contexto dessas transações. Para tanto, o trabalho percorrerá o processo de aquisição de forma a aprofundar o entendimento sobre a aplicação da legislação de proteção de dados em uma área tão dinâmica e relevante para o cenário atual.

2 CENÁRIO ATUAL: FUSÕES & AQUISIÇÕES E LGPD

O artigo 5º, inciso I, da LGPD, dispõe que dado pessoal é "informação relacionada a pessoa natural identificada ou identificável"[14]. A proteção de dados pessoais não se trata, portanto, da proteção de bens ou propriedades de uma ou outra organização, mas sim da proteção das pessoas naturais, que têm direito à tutela das informações a si relacionadas. No cenário atual, em que empresas coletam tantos dados quanto o setor público (senão mais), é importante que esses dados sejam cuidadosamente tratados, o que vai muito além de um *Non Disclosure Agreement* - NDA.

O processo de aquisição de empresas tem emergido como um meio de crescimento acelerado, proporcionando vantagens imediatas, como acesso a novos mercados e sinergias de custos, porém, a ascensão da economia de dados e a crescente digitalização oferecem desafios significativos para as práticas tradicionais de M&A.

As operações de fusões e aquisições abrangem uma ampla variedade de operações corporativas que vão além das fusões e aquisições tradicionais de participações societárias. Essas transações podem incluir fusões, onde duas ou mais empresas se unem para formar uma nova entidade legal que sucede todas as partes originais. Também podem envolver cisões, onde uma empresa é dividida em duas ou mais entidades separadas, cada uma assumindo parte dos ativos e obrigações. Outras formas de M&A incluem incorporações de ações, onde uma empresa incorpora as ações de outra, incorporações de empresas inteiras e aquisições de ativos isolados, onde uma empresa adquire ativos específicos de outra. Além disso, o trespasse refere-se à transferência de todo o estabelecimento comercial de uma empresa para outra

No contexto da legislação brasileira, a aquisição é a transferência, de forma total ou parcial, do controle ou capital de uma empresa de um ente adquirente para outro (Silva, 2015)[15]Essa definição abrange transações comerciais onde uma empresa adquire o domínio sobre outra, seja por meio da compra de ações ou ativos, buscando consolidar suas operações ou expandir sua presença no mercado. Já a incorporação, definida pelo Código Civil nos artigos 1.116 e 1.117[16], é a operação em que "uma ou várias sociedades são absorvidas por outra, que lhes sucede em todos os direitos e obrigações".

---

[14] BRASIL**. Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[15] SILVA, Eduardo Sá. **Fusões e Aquisições:** Abordagem Contabilística, Financeira e Fiscal. Porto: Vida Económica - Editorial AS, 2015.

[16] Art. 1.116. Na incorporação, uma ou várias sociedades são absorvidas por outra, que lhes sucede em todos os direitos e obrigações, devendo todas aprová-la, na forma estabelecida para os respectivos tipos.

Nas últimas décadas, os avanços na legislação antitruste buscaram evitar práticas anticompetitivas e monopolísticas resultantes de fusões e aquisições. O processo de aquisição, historicamente influenciado por avanços na legislação antitruste, viu sua natureza evoluir à medida que o acesso a grandes volumes de informações de usuário se tornou um ativo estratégico no mundo dos negócios.

As operações de M&A estão inseridas em estratégias para o crescimento de empresas de forma inorgânica, permitindo a uma corporação ter interesses satisfeitos de forma quase imediata, como o (i) rápido acesso a novos mercados e atividades; (ii) facilitação na internacionalização da atividade; (il) exploração de sinergias de custos e complementaridades; (iv) aumento do poder de mercado (redução da concorrência e aumento do poder de negociação)[17]. Segundo Cano (Cano, 2002, p. 164):

> Os processos de F&A's são inerentes à concorrência capitalista. Acumulação de capital, inovações, ganhos de produtividade e acirramento da competição, levando a pressões pela eliminação de concorrentes ou pela abertura de novos mercados, são processos que marcaram a história do capitalismo desde o seu início. Tais fatores foram potencializados pelo surgimento do capital financeiro monopolista organizado na forma de sociedade anônima, pelo aumento da intervenção estatal na economia e pelo desenvolvimento do mercado bancário de capitais, o que impulsionou as F&A's.[18]

A crescente digitalização e a economia baseada em dados têm impulsionado ainda mais a relevância do processo de aquisição de empresas. Afinal, adquirir uma empresa que já possui uma base sólida de usuários e dados estabelecidos pode fornecer uma vantagem significativa para a empresa adquirente, permitindo-lhe acelerar seu crescimento e aumentar sua influência no mercado.

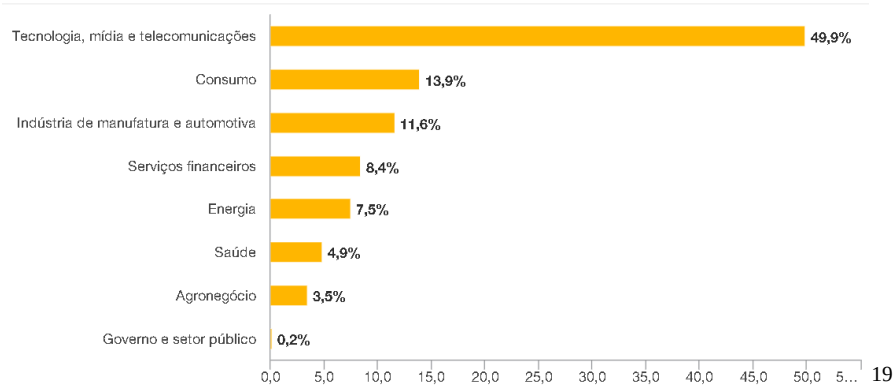
Atualmente, no Brasil há uma grande predominância do setor de tecnologia, mídia e telecomunicações quando se trata de fusões e aquisições, com esse setor realizando cerca 50% dessas operações em 2021, 2022 e 2023.

Art. 1.117. A deliberação dos sócios da sociedade incorporada deverá aprovar as bases da operação e o projeto de reforma do ato constitutivo.
§ 1 o A sociedade que houver de ser incorporada tomará conhecimento desse ato, e, se o aprovar, autorizará os administradores a praticar o necessário à incorporação, inclusive a subscrição em bens pelo valor da diferença que se verificar entre o ativo e o passivo.
§ 2 o A deliberação dos sócios da sociedade incorporadora compreenderá a nomeação dos peritos para a avaliação do patrimônio líquido da sociedade, que tenha de ser incorporada.

[17] COUTINHO, Sérgio Mendes Botrel. **Fusões e Aquisições**. 5. ed. São Paulo: Saraiva, 2016. p. 21.

[18] CANO, Marcelo. **O recente processo de fusões e aquisições na economia brasileira.** 2002. 16f. Dissertação (Mestrado em Economia) - Instituto de Economia, Universidade Estadual de Campinas, Campinas, 2002. p. 164.

Figura 1: Operações de M&A no Brasil: Transações anunciadas até maio de 2023 por setores da economia.



[19]

Fonte: PWC (2023)

A área de fusões e aquisições historicamente apresenta um vasto panorama de fontes normativas, envolvendo diferentes ramos do direito. O direito das sociedades desempenha um papel central, tanto na tomada de decisão das partes envolvidas quanto na execução do processo de transmissão ou integração empresarial[20]. Além do direito privado, especialmente o direito dos contratos, uma vez que essas operações são negócios realizados entre sociedades.

Com a entrada em vigor da LGPD, as empresas deparam com a complexa tarefa de garantir a conformidade durante as fusões e aquisições. A LGPD estabelece requisitos rigorosos para o tratamento de dados pessoais, incluindo a definição de uma base legal adequada e a implementação de medidas de segurança adequadas. Notavelmente, as sanções administrativas da LGPD, com multas de até 2% do faturamento bruto da empresa, acrescentam um elemento de risco substancial ao processo de M&A. A Autoridade Nacional de Proteção de Dados (ANPD), criada como autarquia de natureza especial, tem a atribuição de aplicar essas sanções.

A relevância histórica e atual das M&A, impulsionadas por fatores como a busca por novos mercados e sinergias de custos, é inegável. No entanto, o cenário contemporâneo é redefinido pela busca por conformidade com a LGPD, introduzindo deveres adicionais e penalidades significativas. À medida que avançamos, exploraremos em detalhes as várias fases das aquisições, examinando a intersecção complexa entre as estratégias de negócios e a proteção de dados pessoais.

---

[19] PWC. Operações de M&A no Brasil: Transações anunciadas até maio de 2023 por setores da economia. **PWC**, 2023. Disponível em https://www.pwc.com.br/pt/estudos/servicos/assessoria-tributaria-societaria/fusoes-aquisicoes/2023/operacoes-de-mea-no-brasil-maio-2023.html. Acesso em 18 de jul. de 2023.

[20] CÂMARA, Paulo; BASTOS, Miguel Brito. **O direito da aquisição de empresas: uma introdução. Aquisição de empresas.** Coimbra: Almedina, 2011, p. 15.

2.1 O Processo De Aquisição Entre Empresas

Para uma análise abrangente do processo de aquisição sob a perspectiva da proteção de dados, é fundamental que dividamos esse processo em etapas distintas.

Não existe uma estrutura única e rígida que se aplique a todas as operações de aquisição. Apesar de ser possível esboçar uma representação simplificada dos estágios desse tipo de operação, é imprescindível reconhecer a autonomia privada e a flexibilidade inerente às negociações, pois cada operação pode apresentar peculiaridades e particularidades próprias.

Buscando compreender a dinâmica do processo de aquisição entre empresas privadas em sua totalidade, este tópico abordará as três principais etapas do processo de aquisição: a fase pré-contratual e *due diligence* (2.1.1); a fase de negociações e Aquisição (2.1.2); e a etapa de integração pós-aquisição, voltada para a integração entre as empresas envolvidas (2.1.3).

Cada uma dessas fases demanda uma abordagem específica em relação à aplicação da Lei Geral de Proteção de Dados (LGPD), que se torna um elemento-chave para garantir a conformidade legal e a proteção dos direitos dos titulares de dados. Ao longo de cada fase será examinado como a LGPD se relaciona com cada estágio da operação de aquisição, identificando os desafios e as boas práticas para assegurar a segurança e o tratamento adequado das informações pessoais envolvidas no processo.

2.1.1 Fase Pre-Contratual e D*ue Diligence*

A etapa pré-contratual engloba várias atividades iniciais, desde a estratégia e triagem dos interessados até a *due diligence* e a elaboração de documentos preliminares, como acordos de confidencialidade e protocolos de intenção. Nesse estágio, as partes exploram a viabilidade da transação, avaliam os riscos e benefícios e buscam um acordo preliminar sobre como conduzir suas negociações. Essa fase tem seu início na formação da estratégia inicial da empresa a ser adquirida e da(s) potencial(is) adquirente(s), passando pela triagem das empresas que participarão do processo até o início da *due diligence.*

Durante o processo de pré-aquisição, é frequente que, na etapa de manifestação de interesse, seja firmado um acordo de confidencialidade, também conhecido como NDA (*Non-Disclosure Agreement)*, entre as partes envolvidas. Esse acordo estabelece as condições e obrigações de confidencialidade a serem seguidas pelas partes para garantir que as informações sensíveis não sejam divulgadas ou utilizadas de forma indevida.

Contudo, é importante observar que, em casos em que as informações sensíveis são especialmente confidenciais ou de alto risco, um NDA, por si só, pode não ser suficiente para

garantir a proteção adequada dos dados. Isso se dá porque o objetivo do NDA não gira em torno dos dados das pessoas naturais, e sim em torno das informações confidenciais relacionadas à atividade empresarial.

Para proteção dos dados pessoais, pode ser necessário estabelecer um acordo mais abrangente, com a especificidade para o compartilhamento de informações sensíveis ou um acordo que inclua cláusulas de restrição adicionais para mitigar os riscos de vazamento ou uso indevido das informações de pessoas naturais que as empresas envolvidas estejam coletando, tratando e/ou compartilhando entre si.

Quando se trata de empresa em que seu produto está intimamente relacionado à coleta e tratamento de dados, como seria o caso de uma empresa que desenvolve e emprega Inteligência Artificial ou uma rede social que fatura com base em anúncios direcionados ou segmentados, pode haver grande pressão da adquirente para ter acesso ao máximo possível de informações sobre dados acerca dos usuários ou bancos de dados pessoais que a empresa-alvo possui. É importante que a empresa a ser adquirida tome todas as providencias possíveis para evitar o vazamento de dados e fornecer apenas dados que estejam dentro do efetivo escopo da *due diligence*, evitando exposição desnecessária de dados pessoais.

A definição do que será incluído no *due diligence* é geralmente estipulada em documentos preliminares, como *Term Sheet*, MoU (Memorandum of Understanding) ou Carta de Intenções, de acordo com as necessidades específicas da operação de aquisição. Nesse estágio, a empresa alvo costuma disponibilizar uma "sala de dados" ou "*data room*", onde toda a documentação e informações relevantes relacionadas à aquisição estarão acessíveis aos envolvidos na operação.

Para Coutinho[21], a *Due diligence* é um procedimento investigativo essencial realizado durante o processo de aquisição ou fusão de empresas com o objetivo de obter uma compreensão abrangente do negócio a ser adquirido ou combinado. Além disso, visa a aumentar a probabilidade de uma decisão acertada, permitindo ajustes no preço e avaliando os riscos associados à operação e ao negócio em questão. Outra finalidade crucial é reduzir a exposição do vendedor a possíveis reclamações do comprador, especialmente em transações envolvendo venda de ativos empresariais ou participações societárias.

[21] COUTINHO, Sérgio Mendes Botrel. **Fusões e Aquisições.** 5. ed. São Paulo: Saraiva, 2016

Importante destacar que a doutrina entende o processo de *due diligence* em fusões e aquisições como um dos casos de tratamento de dados pessoais autorizado por "interesse legítimo" na LGPD[22]. Bruno Bioni explica que:

> (Um) exemplo claro de legítimo interesse de terceiros é a *due diligence* em processos de fusão e aquisição, em que terceiros que não têm nenhuma relação pré-estabelecida com os titulares de dados pessoais possuem o legítimo interesse de tratar esses dados para avaliar a viabilidade da operação societária; [23]

No entanto, é importante notar que o tratamento de dados na *due diligence* com a justificativa de legítimo interesse não pode quebrar a legítima expectativa do titular sobre o tratamento de seus dados pessoais, uma vez que tal conduta violaria o princípio da boa-fé objetiva.[24]

Apesar de não ser um requisito legal obrigatório[25], a realização da *due diligence* é uma prática amplamente adotada em operações de fusões e aquisições, devido ao fato de que os *insights* e informações obtidos nessa fase são de extrema importância para a tomada de decisões estratégicas, podendo influenciar diretamente no preço e nas estratégias pós-aquisição.

Também durante o *due diligence* pode ser realizada uma análise do perfil comportamental da companhia a ser adquirida e suas práticas de *compliance.* O *Compliance* se trata de um conjunto de normas regulatórias, tanto internas quanto externas, que os empregados e empresa devem seguir. Gustavo Justino de Oliveira e Gustavo Henrique Carvalho explicam a importância de aferir esses detalhes antes de uma F&A:

> Para além dos riscos relacionados aos comportamentos adotados pelos colaboradores da companhia alvo em momento anterior à operação de M&A, a baixa aderência ao seu programa de compliance pode colocar em risco a política de compliance da própria companhia sucessora. Ou seja, há o risco de que a atual cultura empresarial da companhia alvo seja inconciliável com a política de compliance da companhia adquirente, aumentando-se em demasia o risco de responsabilização por condutas a

---

[22] "Art. 7° O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;[...]." BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[23] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 3. ed. Rio de Janeiro: Forense, 2021.

[24] "ENUNCIADO 683 – A legítima expectativa do titular quanto ao tratamento de seus dados pessoais se relaciona diretamente com o princípio da boa-fé objetiva e é um dos parâmetros de legalidade e juridicidade do legítimo interesse". BRASIL. **IX Jornada de Direito Civil:** Enunciados aprovados. Brasília, 2022. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 22 ago. 2023.

[25] SAYDELLES, Rodrigo Salton Rotunno. A (in)existência de dever de realizar due diligence em operações de M&A à luz do direito brasileiro. **Res Severa Verum Gaudium**, Porto Alegre, v. 5, n. 2, p. 260-289, 2020.

> serem possivelmente adotadas por colaboradores da companhia adquirida após a operação de M&A.[26]

Verificando haver problemas de *compliance* de proteção de dados na companhia-alvo, a empresa adquirente pode tomar ações proativas para abordar esses problemas e garantir que a conformidade seja restabelecida. A inclusão de cláusulas específicas no contrato de compra e venda de ativos societários (Sales and Purchase Agreement - SPA), por exemplo, pode prever obrigações de correção e aprimoramento dos processos de compliance da empresa adquirida. Além disso, em algumas situações pode ser possível a celebração de um acordo de leniência com os órgãos de controle, uma alternativa para colaborar com investigações e reduzir as penalidades relacionadas às condutas passadas da companhia-alvo[27].

Aplicar mecanismos jurídicos como estes permite à empresa adquirente demonstrar seu compromisso com a integridade e a ética nos negócios, mitigando riscos legais e reputacionais associados à transação. Além disso, evidencia a responsabilidade corporativa e a preocupação em seguir padrões de compliance rigorosos.

O sucesso da *due diligence* está intrinsecamente ligado à cooperação das partes envolvidas. Tanto o vendedor quanto o comprador desempenham papéis fundamentais ao fornecer as informações necessárias, documentação e declarações pertinentes ao processo. No entanto, a colaboração do comprador vai além de simplesmente receber as informações; é essencial que ele conduza uma apuração minuciosa e ética do impacto desses dados na negociação.

No processo da *due diligence* o comprador deve buscar compreender profundamente as informações fornecidas pelo vendedor, verificando sua exatidão e relevância para a transação em questão. Parte disso é a realização de uma avaliação criteriosa dos riscos e oportunidades apresentados pelas informações coletadas, além da condução de todas as análises e investigações de maneira ética, em total consonância com os princípios de confidencialidade e proteção dos dados compartilhados.

Outro ponto a se considerar é que na etapa de *due diligence* podem ser descobertos vazamentos, práticas abusivas de tratamento de dados e riscos de compliance que tenham

---

[26] OLIVEIRA, Gustavo Justino de; SCHIEFLER, Gustavo Henrique Carvalho. **Compliance em Operações de Fusão e Aquisição (M&A):** intercorrências e inferências a partir dos acordos de leniência no Brasil. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4282044/mod_resource/content/0/COMPLIANCE%20EM%20OPERA%C3%87%C3%95ES%20DE%20FUS%C3%83O%20E%20AQUISI%C3%87%C3%83O%20%28pdf%29.pdf. Acesso em 05 de jun. 2023.

[27] OLIVEIRA, Gustavo Justino de; SCHIEFLER, Gustavo Henrique Carvalho. **Compliance em Operações de Fusão e Aquisição (M&A):** intercorrências e inferências a partir dos acordos de leniência no Brasil. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4282044/mod_resource/content/0/COMPLIANCE%20EM%20OPERA%C3%87%C3%95ES%20DE%20FUS%C3%83O%20E%20AQUISI%C3%87%C3%83O%20%28pdf%29.pdf. Acesso em: 05 jun. 2023.

ocorrido anteriormente ao processo de M&A, e que devem ser contabilizados no momento de negociação e aquisição.

Um exemplo ilustrativo ocorreu em 2017, quando a Uber estava em negociações para a venda de uma participação ao Softbank. Nesse momento, veio à tona que o Uber havia sido vítima de uma violação de dados que resultou na exposição das informações pessoais de 57 milhões de clientes. O executivo-chefe de segurança da Uber tentou minimizar os danos, negociando um pagamento de resgate de US$ 100.000 para os hackers. No entanto, a violação não foi divulgada publicamente por mais de um ano, uma decisão que foi posteriormente reconhecida como problemática pelo novo CEO da Uber. Embora esse incidente de segurança nos termos do acordo não tenha sido divulgado, causou danos significativos ao Uber, tanto em sua reputação quanto financeiramente. O contrato acabou por ser fechado em US$ 48 bilhões, o que representou um desconto de 30% em relação à avaliação inicial da Uber de US$ 68 bilhões.[28]

De maneira semelhante, em 2017, o preço da aquisição da Yahoo pela Verizon despencou US$ 350 milhões depois que o Yahoo divulgou três violações maciças de dados que comprometeram mais de 1 bilhão de contas de clientes[29].

Estes casos demonstram a necessidade de participação de profissionais como CISO's (*Chief Information Security Officers)*, DPOs (*Data Protection Officers*)[30], especialistas em cibersegurança e analistas de segurança da informação no processo de F&A's para que falhas de segurança e ilegalidades referentes à proteção de dados sejam identificadas cedo o suficiente para que os custos e consequências destas sejam contabilizados no valor de aquisição[31]. Durante

[28] MEYRICK, Julian*. et a*l. Assessing cyber risk in M&A. **IBM**, [s.l.], 3 maio 2021.Disponível em: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/cyber-risk-mergers-acquisitions. Acesso em: 20 jul. 2023.

[29] Kirk, Jeremy. "Yahoo Takes $350 Million Hit in Verizon Deal." **Bank Info Security**, 22 fev. 2017. Disponível em: https://www.bankinfosecurity.com/yahoo-takes-350-million-hit-in-verizon-deal-a-9736. Acesso em: 20 jun. 2023.

[30] Tanto o DPO quanto o Encarregado de Proteção de Dados têm a responsabilidade de garantir a conformidade com as leis de proteção de dados e promover a proteção da privacidade dos titulares de dados, mas as regulamentações específicas e os requisitos para essas funções podem variar de acordo com as leis aplicáveis em cada jurisdição. De forma geral, na maioria das vezes quando um profissional é o DPO de certa empresa, ele também será o EPD, de forma que nesse trabalho se utilizará o termo DPO como equivalente ao EPD.

[31] "When it comes to cyber in an M&A world—it's important to develop cyber threat profiles of prospective targets and portfolio companies to determine the risks each present," says Deborah Golden, a principal and U.S. Cyber & Strategic Risk leader at Deloitte Risk & Financial Advisory, Deloitte & Touche LLP. "Chief information security officers understand how a data breach can negatively impact the valuation and the underlying deal structure. Leaving cyber out of that risk picture may lead to not only brand and reputational risk, but also significant and unaccounted remediation costs." DELOITTE. M&A Alternatives Take Center Stage: Survey. **CFO JOURNAL**, [s.l.], 30 out. 2020.. Disponível em: https://deloitte.wsj.com/articles/m-a-alternatives-take-center-stage-survey-01604086979?tesla=y&tesla=y. Acesso em: 10 jul. 2023.

o processo de M&A, erros no que diz respeito à cibersegurança e proteção de dados podem causar resultados graves e imprevisíveis, como danos à reputação e marca da empresa, além de custos significativos para corrigir os problemas resultantes.

Nessa ordem de ideias, a cibersegurança é uma questão estratégica que pode afetar diretamente a viabilidade e o sucesso de uma transação. É crucial que as organizações envolvidas em M&A se concentrem em avaliar e mitigar os riscos cibernéticos de forma proativa, garantindo que todas as questões relacionadas à segurança da informação sejam tratadas antes da conclusão do negócio. Ademais, a adoção de práticas adequadas de cibersegurança pode ser um fator diferenciador para potenciais investidores, demonstrando um compromisso com a proteção dos dados e informações dos clientes e parceiros comerciais.

Em suma, a fase de *due diligence* em processos de fusões e aquisições desempenha um papel central na avaliação da viabilidade e dos riscos envolvidos em uma transação. Ela permite que as partes interessadas obtenham um entendimento abrangente do negócio em questão, desde suas práticas de compliance até os detalhes sensíveis de tratamento de dados. A cibersegurança e a conformidade com regulamentos, como a LGPD, emergem como pilares essenciais dessa avaliação, considerando os crescentes desafios de proteção de dados e a crescente importância da reputação e integridade corporativa.

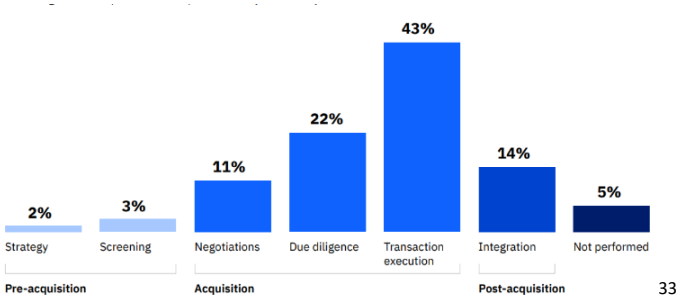
2.1.2 A Etapa de Negociação e Aquisição

Esse é o momento em que os termos do contrato são negociados e o contrato de compra e venda da empresa ou de participação é assinado. A empresa a ser adquirida deve, durante a negociação, fornecer informações sobre as operações de tratamento, sobre os sistemas empregados nessas operações de tratamento de dados pessoais bem como sobre as políticas de privacidade. Já a empresa adquirente deve obter uma compreensão completa das práticas de proteção de dados do alvo da aquisição para poder avaliar os riscos e responsabilidades potenciais relacionados à proteção de dados.

Ao longo dessa fase, o processo de *due diligence* também é crucial, e sua importância aumenta à medida que a expectativa de aquisição se consolida. A equipe de *due diligence* deve garantir que tenha havido a devida investigação de questões relacionadas à proteção de dados, incluindo a análise detalhada dos registros de segurança cibernética e histórico de incidentes de segurança do alvo. Isso permitirá identificar quaisquer vulnerabilidades existentes e garantir que medidas adequadas de segurança estejam sendo adotadas. Na maioria das vezes é nessa

fase que será envolvido o CISO ou DPO, conforme levantamento realizado pela IBM em 2019[32].

Figura 2: Em que momento organizações realizam uma avaliação de riscos de segurança cibernética:



[33]

Fonte: MEYRICK, Julian. *et al.* (2021)

No cenário brasileiro, é recomendável que as empresas estudem a possibilidade de estabelecer um fundo de contingência para acautelar possíveis exposições que possam surgir após o fechamento da aquisição. Assim como na fase pré-contratual, é crucial documentar toda a operação para evitar futuros questionamentos por órgãos fiscalizadores, como a ANPD.

No "*benchmarking* Internacional sobre as Instituições de Direito da Concorrência", estudo apresentado no fechamento do Acordo de Cooperação Técnica entre CADE e ANPD em 2021, ao falar um pouco sobre a visão do Departamento de Justiça (DoJ) dos Estados Unidos e da Comissão Europeia (CE) na aquisição da empresa FitBit pela Alphabet. Enquanto o DoJ expressava preocupação quanto ao acesso do Google a dados pessoais por meio da FitBit, a CE impôs condições à aprovação, como a restrição do uso desses dados para personalização de anúncios. O estudo trouxe que:

> Para o DoJ, a aquisição do Fitbit, que é uma empresa de produtos eletrônicos voltados para a saúde e a prática de atividades físicas dos usuários, **poderá conferir ao Google ainda mais acesso aos dados pessoais dos indivíduos.** Justamente por isso, **condições foram impostas pela CE para a aprovação da aquisição, como, por exemplo, o comprometimento do Google em não utilizar os dados coletados dos usuários, por meio dos aparelhos do Fitbit, para a personalização e o direcionamento de publicidades aos usuários.** (grifo próprio)[34]

[32] MEYRICK, Julian. et al. Assessing cyber risk in M&A. **IBM**, [s.l.], 3 maio 2021.Disponível em: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/cyber-risk-mergers-acquisitions. Acesso em: 20 jul. 2023.

[33]Figura 2: Quando organizações realizam uma avaliação de riscos de segurança cibernética MEYRICK, Julian. *et al.* Assessing cyber risk in M&A. **IBM**, [s.l.], 3 maio 2021.Disponível em: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/cyber-risk-mergers-acquisitions. Acesso em: 20 jul. 2023.

[34] CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. **Documento de Trabalho 002/2021**-Benchmarking internacional sobre as instituições de Defesa da Concorrência e de Proteção de Dados. Brasília, jun. 2021. p. 96.

Veja-se que há casos como esse, em que parte dos dados da empresa adquirida não serão de livre acesso pela empresa adquirente por conta de limitações impostas pelos órgãos regulatórios. Esse é um dos motivos pelos quais ter um DPO ou especialista LGPD envolvido desde a etapa pré-contratual não é apenas uma necessidade legal, como também estratégica.

Após a conclusão da negociação, é essencial garantir a adequada retenção e eliminação dos dados coletados durante a *due diligence*. O artigo 15 da LGPD estabelece o direito do titular de solicitar a exclusão de seus dados pessoais.

Em casos em que após a M&A haverá uma mudança na personalidade jurídica do controlador dos dados, como fusões ou incorporações, antes da integração pós-aquisição (normalmente o adquirente ou a PJ resultante da fusão), os titulares dos dados devem ser devidamente informados da iminência de terem seus dados acessados, transferidos e/ou tratados por um terceiro.

Consultorias empresariais também costumam sugerir, nessa fase, uma avaliação minuciosa dos custos de aquisição, abrangendo aspectos relacionados à segurança, como serviços essenciais de e-mail e compartilhamento de arquivos, bem como serviços mais complexos, incluindo ferramentas e métodos de desenvolvimento. Os custos associados ao gerenciamento de riscos e segurança cibernética durante a aquisição devem ser devidamente avaliados e considerados na negociação dos termos do negócio.

No contexto das fusões e aquisições (M&A), é fundamental considerar as implicações legais da Lei Geral de Proteção de Dados (LGPD) durante a fase contratual e após a aquisição. As disposições do Código Civil brasileiro e da Lei das Sociedades Anônimas também têm impacto nas operações de incorporação e fusão de empresas, visto que a sociedade incorporadora e a nova sociedade resultante da fusão assumem todos os direitos e obrigações da pessoa jurídica sucedida.

A utilização de cláusulas específicas em contratos de aquisição para lidar com irregularidades relacionadas à LGPD ou proteção de dados é uma prática importante e cada vez mais comum no contexto de fusões e aquisições. Após realizar a devida diligência prévia, que envolve a análise minuciosa da conformidade da empresa-alvo com as políticas de compliance, o adquirente pode identificar riscos relacionados à proteção de dados e buscar formas de mitigá-los.

Uma das formas de equilibrar os riscos identificados na due *diligence* é por meio de ajustes no preço da operação societária ou exigindo que o contrato de compra e venda contenha disposições que protejam o adquirente caso surjam problemas de proteção de dados no futuro.

Essas disposições podem ser estabelecidas na cláusula de "declarações e garantias", também conhecida como "*representations and warranties*"[35].

Nessa cláusula, ambas as partes descrevem aspectos relevantes da operação, incluindo informações sobre práticas de compliance e proteção de dados por parte do vendedor. Além disso, é possível vincular o conteúdo dessa cláusula a uma obrigação futura de indenização pelo vendedor caso as declarações fornecidas não estejam em conformidade com a realidade.

Isso garante que, caso o adquirente descubra após a aquisição que a empresa-alvo possui irregularidades com a LGPD ou que ocorreram vazamentos ou práticas inadequadas relacionadas à proteção de dados, ele tenha uma proteção contratual que lhe permita buscar compensação financeira perante o vendedor. Essa abordagem cria um incentivo para que o vendedor forneça informações precisas e transparentes durante o processo de negociação, além de dar ao adquirente maior segurança em relação aos riscos de compliance e proteção de dados envolvidos na transação.

A utilização de cláusulas específicas em contratos de aquisição para lidar com irregularidades relacionadas à LGPD ou proteção de dados é uma prática importante e cada vez mais comum no contexto de fusões e aquisições. Após realizar a devida diligência prévia, que envolve a análise minuciosa da conformidade da empresa-alvo com as políticas de compliance, o adquirente pode identificar riscos relacionados à proteção de dados e buscar formas de mitigá-los.

2.1.3 Integração Pós-Aquisição

A etapa de integração no contexto de fusões e aquisições (M&A) envolve a convergência das duas empresas em uma única entidade, seja por meio da absorção de uma delas pela outra ou por meio de uma reestruturação das empresas envolvidas. Independentemente do desfecho, o processo pós-fusão ou aquisição (PMI) é intrincado, demandando ajustes nos aspectos estruturais, recursos humanos e elementos técnicos da organização[36].

---

[35] PESSOA, Daniel Tardelli; SABADIN, Mariana Guerra. **Cláusulas de declarações e garantias e operações de fusão e aquisição**. 2012. Disponível em: http://www.levysalomao.com.br/files/publicacao/anexo/20120730185424_bj-julho-clausulas-de-declaracoese-garantias-e-operacoes-de-fusao-e-aquisicao.pdf. Acesso em: 10 maio 2023.

[36] EPSTEIN, Michael J. The determinants and evaluation of merger success. **Business Horizons**, v. 48, n. 1, p. 37–46, jan. 2005.

De acordo com o estudo conduzido pela IBM[37], 1 (um) a cada 3 (três) executivos relatou terem experenciado vazamentos de dados atribuídos a fusões e aquisições na fase de integração. Esse cenário crítico pode ser compreendido em virtude das mudanças substanciais que ocorrem na etapa pós-contratual, as quais representam momentos de ampla reconfiguração dos sistemas de tecnologia da organização.

Nesse contexto, a integração de sistemas e a etapa pós-contratual emergem como períodos de alta vulnerabilidade, pois frequentemente envolvem a convergência de infraestruturas tecnológicas distintas, sistemas de informação e fluxos de dados heterogêneos. Essa complexa interação muitas vezes acaba por expor brechas na segurança cibernética, permitindo que dados sensíveis sejam inadvertidamente comprometidos.

Diante desse cenário, o primeiro passo crucial para mitigar os riscos é conduzir uma análise detalhada dos sistemas que serão integrados, identificando os dados pessoais envolvidos em cada um deles. Isso permitirá uma compreensão clara dos riscos de privacidade associados a cada sistema e ajudará na definição de medidas adequadas de proteção de dados.

O caso da aquisição do Trustee Savings Bank (TSB) pelo Banco Sabadell em 2015[38] apresenta uma lição valiosa sobre a importância da integração pós-aquisição e a conformidade com regulamentos, como a LGPD, em processos de fusões e aquisições. Nesse caso, a migração de bancos de dados como parte do processo de integração pós-aquisição resultou em falhas graves no sistema online do TSB, afetando a acessibilidade aos serviços bancários e até permitindo que alguns clientes visualizassem as contas de outros usuários. O incidente resultou na saída do CEO da TSB e levou o banco a perder mais de 12.500 clientes. Isso veio junto com despesas de migração adicionais estimadas em cerca de £ 176 milhões e outros contratempos financeiros devido à renúncia de taxas bancárias. Além das perdas financeiras concretas, a migração malsucedida desencadeou várias investigações regulatórias e atraiu significativa atenção do público[39].

Esse episódio demonstra como uma integração inadequada dos sistemas pós-aquisição pode ter consequências significativas. No contexto da LGPD, o tratamento inadequado de dados pessoais durante essa migração teria implicações legais ainda mais sérias, considerando as

---

[37] MEYRICK, Julian. et al. Assessing cyber risk in M&A. **IBM**, [s.l.], 3 maio 2021.Disponível em: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/cyber-risk-mergers-acquisitions. Acesso em: 20 jul. 2023.

[38] BAILEY, Andrew. Re: TSB IT Migration. 2018. Disponível em <https://www.parliament.uk/globalassets/documents/commons-committees/treasury/Correspondence/2017-19/fca-to-chair-tsb-300518.pdf>. Acesso em: 20 jul. 2023.

[39] HENRICO DOLFING. Case Study 2: The Epic Meltdown of TSB Bank. **Henrico dolfing**, 13 mar. 2019. Disponível em <https://www.henricodolfing.com/2019/03/case-study-epic-meltdown-of-tsb-bank.html>. Acesso em 20 de jul. 2023.

multas substanciais e penalidades previstas pela legislação em casos de violações de proteção de dados.

Em operações de fusão e incorporação, a responsabilidade da empresa sucessora por atos e fatos ocorridos antes da operação societária está sujeita, ainda, às normas dos parágrafos 1º e 2º do artigo 4º da Lei Anticorrupção[40]. Em casos em que houver práticas corruptas ou antiéticas anteriormente à aquisição, a adquirente é obrigada a pagar multa e a reparar integralmente o dano causado até o limite do patrimônio transferido, exceto quando ocorre simulação ou evidente intuito de fraude.

Desta forma, se verifica a existência de responsabilidade solidária entre sociedades controladoras, controladas, coligadas ou consorciadas. Isso significa que essas empresas também podem ser responsabilizadas por atos de terceiros relacionados a elas que violem a Lei Anticorrupção. No entanto, essa responsabilidade solidária é restrita à obrigação de pagamento de multa e reparação integral do dano, conforme o parágrafo 2º do artigo 4º.

A descoberta de vazamentos, práticas antiéticas e ilegalidades no tratamento de dados após a integração é uma preocupação constante em F&A's. Em 2016, uma severa penalidade foi imposta a um provedor de telecomunicações com sede no Reino Unido quando um banco de dados de clientes adquirido anteriormente foi alvo de hackers[41].

No contexto de uma integração pós-aquisição, podem emergir desafios significativos, tais como garantir a segurança dos dados também e manter um armazenamento adequado durante o processo de integração. Após a aquisição, a segurança dos dados deve ser uma prioridade, com procedimentos de armazenamento adequados.

A falta de atualização dos consentimentos previamente obtidos para o tratamento de dados, quando essa consistir na base legal eleita pelo agente de tratamento, também se evidencia como uma lacuna crítica na integração pós-M&A. A revisão e atualização das políticas de privacidade se tornam mandatórias para assegurar a conformidade com as novas práticas de tratamento de dados decorrentes da integração.

---

[40] Art. 4º Subsiste a responsabilidade da pessoa jurídica na hipótese de alteração contratual, transformação, incorporação, fusão ou cisão societária.
§ 1º Nas hipóteses de fusão e incorporação, a responsabilidade da sucessora será restrita à obrigação de pagamento de multa e reparação integral do dano causado, até o limite do patrimônio transferido, não lhe sendo aplicáveis as demais sanções previstas nesta Lei decorrentes de atos e fatos ocorridos antes da data da fusão ou incorporação, exceto no caso de simulação ou evidente intuito de fraude, devidamente comprovados.
§ 2º As sociedades controladoras, controladas, coligadas ou, no âmbito do respectivo contrato, as consorciadas serão solidariamente responsáveis pela prática dos atos previstos nesta Lei, restringindo-se tal responsabilidade à obrigação de pagamento de multa e reparação integral do dano causado.

[41] MEYRICK, Julian. et al. Assessing cyber risk in M&A. **IBM**, [s.l.], 3 maio 2021.Disponível em: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/cyber-risk-mergers-acquisitions. Acesso em: 20 jul. 2023.

Uma das formas de a empresa adquirente manter parte dos dados de titulares que optarem por não consentir com a transferência e tratamento de dados pela empresa adquirente é por meio da anonimização. Dados anônimos são aqueles que perderam qualquer conexão com a identidade de uma pessoa, o que é alcançado através de técnicas como a supressão, generalização e randomização, que removem elementos identificadores dos dados originais.[42]

Dados são considerados anonimizados quando não é possível identificar o titular utilizando meios técnicos razoáveis disponíveis na ocasião do tratamento. O inciso XI da lei define "anonimização" como o uso de meios técnicos adequados durante o tratamento dos dados, de modo que eles percam a possibilidade de associação, direta ou indireta, a um indivíduo.

A integração de empresas por meio de fusões e aquisições pode desencadear uma série de desafios interconectados, cuja manifestação muitas vezes se inicia com problemas de compatibilidade e conflitos nas bases de dados. A convergência dos sistemas de TI de entidades distintas, apesar de visar uma harmonização operacional, pode inadvertidamente resultar na exposição inadequada de dados pessoais, constituindo um risco potencialmente grave.

Esse cenário é frequentemente exacerbado pela persistência desnecessária da retenção de dados após o processo de M&A, gerando um ambiente propício para vazamentos ou uso indevido. Além disso, a carência de treinamento em proteção de dados para os colaboradores, juntamente com a ausência de uma governança efetiva, pode culminar em violações inadvertidas e em uma falta geral de supervisão.

A complexidade da integração das diferentes culturas e processos organizacionais adiciona uma camada adicional de desafios, dificultando a implementação de práticas unificadas de proteção de dados. Diante dessa multiplicidade de questões, a identificação e a abordagem de brechas e lacunas na segurança destacam-se como aspectos críticos que precisam ser considerados.

Tendo em vista esse panorama, enfrentar esses problemas requer uma abordagem holística e proativa, especialmente para assegurar a proteção dos dados pessoais na etapa pós-aquisição no contexto de operações de M&A. Vale ressaltar que a integração de sistemas entre empresas pode acarretar a transferência internacional de dados, frequentemente sem a garantia dos níveis adequados de proteção requeridos pelas leis pertinentes.

Nesse sentido, é fundamental garantir não apenas a conformidade com as regulamentações, mas também os direitos dos titulares dos dados. Isto se estende tanto aos

[42] BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021. p. 311.

dados que serão transferidos à empresa adquirente quanto às mudanças que ocorrerão no tratamento desses dados após a integração.

Durante a etapa de integração dos sistemas, uma estreita colaboração entre a equipe de TI e especialistas em privacidade e segurança de dados é imperativa. Isso assegura que as práticas de tratamento de dados estejam perfeitamente alinhadas com os princípios estabelecidos pela legislação vigente, como a LGPD. Além disso, a implementação de medidas de segurança cibernética, tais como criptografia e controle de acesso, emerge como um requisito fundamental para proteger os dados pessoais contra acesso não autorizado ou potenciais vazamentos.

3. DESAFIOS PARA EFICÁCIA DA LGPD EM FUSÕES E AQUISIÇÕES

Nesta seção, abordaremos os principais desafios enfrentados pelas empresas que buscam efetivar a LGPD em operações de fusões e aquisições. Dividiremos a análise em duas perspectivas: os desafios enfrentados pelas próprias empresas envolvidas no processo de M&A, que precisam garantir a adequação dos processos de tratamento de dados de suas operações, e os desafios enfrentados pela ANPD e outros órgãos reguladores, que devem atuar de forma eficaz na fiscalização e aplicação da LGPD em operações de M&A.

Na primeira parte, exploraremos os desafios e dilemas que as empresas enfrentam ao incorporar a LGPD em todas as fases do processo de aquisição, desde a *due diligence* até a integração pós-aquisição. Serão analisados aspectos como a identificação e tratamento de dados sensíveis, a necessidade de ajustar políticas de privacidade e consentimento, bem como garantir a conformidade com a lei durante a transição dos dados da empresa adquirida.

Na segunda parte, voltaremos nossa atenção para os desafios enfrentados pelos órgãos reguladores, em especial a ANPD, no exercício de suas atribuições de fiscalização e aplicação da LGPD em operações de M&A. Será discutida a importância da cooperação entre a ANPD e outros órgãos reguladores, como o Conselho Administrativo de Defesa Econômica (CADE), para assegurar a devida proteção dos dados dos titulares e evitar concentração de mercado que possa comprometer a privacidade e a concorrência.

3.1 Necessidade de Aperfeiçoamento das Práticas Empresariais em Proteção de Dados

A crescente relevância da proteção de dados em fusões e aquisições torna imprescindível o aperfeiçoamento das práticas empresariais nesse contexto. A governança de dados deixou de ser uma opção para as organizações e se tornou uma necessidade essencial para manter a competitividade e a conformidade com as leis de privacidade de dados.

A LGPD dispõe, em seu artigo 5º, nos incisos VI, VII e VIII, os conceitos de controlador, operador e encarregado. Conforme a lei, o gênero agente de tratamento comporta as espécies da figura do controlador (“pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”) e do operador (“pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador”). Enquanto isso, o encarregado é a “pessoa indicada pelo

controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)"[43].

Esses conceitos foram inspirados no Regulamento Geral da União Europeia (GDPR), com base nos conceitos de *controler*, *processor* e *data protection officer* (DPO)[44]. Para entender o dever de cada um deles, torna-se importante a divisão dos deveres de cada figura dentro do processo de F&A para a proteção de dados conforme a LGPD, o que se fará a seguir.

3.1.1 Deveres do agente de tratamento: Controlador e Operador

Primeiramente, é importante entender que durante o processo de M&A haverá dois principais "agentes" no tratamento de dados: a adquirente e a adquirida. Ambas as empresas irão compor um time de trabalho que atuará na F&A durante o momento pré-contratual e contratual, isto é, na estratégia, no *due diligence*, nas formalidades, negociações, assinatura do contrato e tudo que isso envolve. Na ocorrência de irregularidades a responsabilidade recairá sobre os agentes de tratamento (e não sobre os indivíduos subordinados que compõem a operação de M&A)[45].

Desta forma teremos, em regra, sempre dois controladores (adquirente e adquirida), e por vezes a contratação de um operador (uma consultoria de M&A por exemplo), ambos trabalhando em cooperação para a mesma finalidade: Uma operação de F&A bem-sucedida. Essas duas figuras serão o que a LGPD define como "agentes de tratamento".

Neste sentido, as operações de tratamento de dados feitas dentro de uma operação de fusão ou aquisição serão, em sua maioria, casos de controladoria conjunta[46], respondendo a

---

[43] Art. 5º Para fins desta Lei, considera-se: VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[44] MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. 1. ed. Indaiatuba: Editora Foco, 2022. p. 11-37.

[45] Item "6. São agentes de tratamento o controlador e o operador de dados pessoais, os quais podem ser pessoas naturais ou jurídicas, de direito público ou privado. Ressalta-se que os agentes de tratamento devem ser definidos a partir de seu caráter institucional. Não são considerados controladores (autônomos ou conjuntos) ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento". AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS.
Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília: Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

[46] Apesar do conceito de controladoria conjunta não estar previsto formalmente na LGPD, pode ser inferido que este está contemplado no sistema jurídico de proteção de dados, como estabelecido pela ANPD. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS.

adquirida e a adquirente de forma solidária, conforme o inciso II do parágrafo 1º do art. 42 da LGPD[47] aponta. Apesar de o inciso II não utilizar o termo "controladoria conjunta", fica claro pela interpretação de sua redação a existência deste instituto no Brasil. Dessa forma, pode-se utilizar do regulamento europeu para dizer que a controladoria conjunta ocorre quando há "participação conjunta" na determinação de "finalidades e meios de tratamento", partindo as finalidades de tratamento de decisões conjuntas ou convergentes[48].

Assim, se as duas empresas estiverem tratando um conjunto de dados para os mesmos fins, como seria o caso da etapa de *due diligence, e* sendo as decisões tomadas no processo de F&A comuns, complementares ou convergentes, elas responderão solidariamente conforme o art. 42, §1º, II, da LGPD.

No entanto, não ocorrerá controladoria conjunta caso a finalidade do tratamento do mesmo conjunto de dados (ou de conjuntos de dados diferentes) diferirem entre as controladoras. Imaginemos, por exemplo, que um dos empregados da empresa a ser adquirida e membro da equipe operadora da F&A, logo antes da assinatura do contrato de aquisição, realiza a transferência ou tratamento de um conjunto de dados a mando de sua empregadora, para fins próprios dos sócios da adquirida e sem o conhecimento da adquirente. Este seria um caso de controladoria singular, afastando a incidência da solidariedade.

Percebe-se que um dos elementos essenciais na carta de intenções ou documento preliminar equivalente na etapa pré-contratual é o de determinação das finalidades do tratamento de dados durante o processo de aquisição, o que deve ser feito formalmente. Desta forma, caso haja decisões unilaterais de uma das controladoras no tratamento de dados, a identificação de casos em que não incidirá a solidariedade será facilitada, gerando mais segurança jurídica na operação.

Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília: Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

[47] Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados: (..)

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[48] 44. Nas **decisões comuns**, duas ou mais entidades possuem uma intenção comum sobre as finalidades e meios de tratamento e tomam decisões em conjunto. Em contrapartida, nas **decisões convergentes** existem decisões distintas sendo tomadas, porém elas se complementam de tal forma que o tratamento não seria possível sem a participação de ambos os controladores. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília, Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

É comumente recomendada a prática de contratar um terceiro *expert* em M&A‘s para a realização de tal operação, uma vez que esse processo é de alta complexidade. Cabe esclarecer que, sendo as finalidades e o poder de decisão ambos pertencentes à adquirida e à adquirente, não há que se falar em “terceirização” do papel de controlador, sendo a consultoria ou assessoria, quando for o caso, uma operadora no tratamento de dados relativo à operação, e não uma controladora.

Nota-se também que os conceitos de controlador e operador são funcionais, com responsabilidades de acordo com os papeis reais das partes[49]. A mera contratação de uma operadora em contrato firmado entre as partes não impede que as controladoras sejam responsabilizadas quando as decisões relativas ao tratamento dos dados estiverem em sua esfera de atuação.

Portanto, mesmo que haja um encarregado de proteção de dados (EPD) na equipe da empresa contratada para realizar a operação de M&A, o que se entende das recomendações da ANPD é que ainda é necessário que haja um encarregado de proteção de dados para cada controlador[50], de forma a fiscalizar se o operador está agindo conforme o objeto, a duração, a natureza e a finalidade do tratamento dos dados previamente definidos contratualmente[51].

Um dos principais deveres do controlador será o de determinar quem será o responsável pelo cumprimento das normas de proteção de dados[52] e fornecer os “recursos necessários ao desempenho (de suas) funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento[53]”, conforme o determinado pela ANPD

---

[49] De acordo com as orientações do *European Data Protection Board* - EDPB: “os conceitos de controlador e operador são funcionais: eles visam alocar responsabilidades de acordo com os papéis reais das partes. Isso implica que o status legal de um ator como ‘controlador’ ou ‘operador’ deve, em princípio, ser determinado por suas ações concretas em uma determinada situação, ao invés da designação formal como sendo um ‘controlador’ ou ‘operador’ (por exemplo, em um contrato).” (tradução livre). EUROPEAN DATA PROTECTION BOARD. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR**. [s.l.], set. 2020. Disponível em <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf>. Acesso em 05 ago. 2023. p. 9.

[50] 54. Cabe destacar, ainda, algumas das obrigações do operador: (i) seguir as instruções do controlador; (ii) firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador; (iii) dar ciência ao controlador em caso de contrato com suboperador.

[51]56. Os pontos que podem ser definidos contratualmente são o objeto, a duração, a natureza e a finalidade do tratamento dos dados, os tipos de dados pessoais envolvidos e os direitos e obrigações e responsabilidades relacionados ao cumprimento da LGPD. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília, Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

[52] MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. 1. ed. Indaiatuba: Editora Foco, 2022. p. 11-37.

[53] UNIÃO EUROPEIA. **REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504. Art. 38, n. 2.

nos itens 70 ao 77 do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais[54].

O artigo 38 da GDPR, visto como uma boa prática pela ANPD, proíbe que o agente de tratamento penalize ou destitua o encarregado pelo fato de exercer suas funções[55], dispondo o dever de que a organização apoie seu encarregado de dados (EPD) no exercício de suas funções e missão[56].

Não basta, portanto, que em uma operação de M&A o controlador e/ou operador contrate um profissional pouco experiente, o nomeie "DPO" ou "EPD" e se esqueça da existência desse profissional até o momento em que haja um questionamento pela ANPD. A responsabilidade pelas atividades de tratamento de dados continua sendo do agente de tratamento, de forma que o encarregado deve ser selecionado de forma cuidadosa e ter competência, capacidade e liberdade suficientes[57] na M&A para proteger a(s) controladora(s) de possíveis sanções e escândalos causados por irregularidades de forma preventiva.

Nesta direção, conforme anteriormente referido, a implementação de políticas e práticas robustas de proteção de dados desde o estágio anterior ao *due diligence* até a fase de pós-aquisição é fundamental para garantir a segurança dos dados e a preservação dos direitos dos titulares e das próprias controladoras. Para isso, o encarregado deve ser parte do processo desde seu início, ou ter fornecidos todos os recursos necessários para a perfeita condução da operação de acordo com a legislação.

Necessário é entender que o aperfeiçoamento das práticas empresariais em proteção de dados envolve a adoção de medidas proativas para identificar e mitigar riscos relacionados ao tratamento de informações sensíveis durante todo o processo de M&A. Além disso, é essencial promover a conscientização e a capacitação dos colaboradores, a fim de assegurar que todos os

---

[54] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília, Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

[55] "O responsável pelo tratamento e o subcontratante asseguram que da proteção de dados não recebe instruções relativamente ao exercício das suas funções. O encarregado não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções. O encarregado da proteção de dados informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante."

[56] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – UNIÃO EUROPEIA. **Orientações sobre os encarregados da proteção de dados (EPD).** Bruxelas, 2016. Disponível em: https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf. Acesso em: 12 jul. 2023.

[57] 77. Conquanto a LGPD não impeça que um mesmo encarregado atue em nome de diferentes organizações, é importante que ele seja capaz de realizar suas atribuições com eficiência. Assim, antes de indicar um encarregado, o controlador deve considerar se ele será mesmo capaz de atender às suas demandas e às de outras organizações concomitantemente. A responsabilidade pelas atividades de tratamento de dados pessoais continua sendo do controlador ou do operador de dados, conforme estabelece o art. 42 da LGPD.

envolvidos compreendam a importância da proteção de dados e respeitem as instruções e boas práticas elaboradas pelos encarregados de proteção de dados.

A reação dos empregados das operadoras e controladoras às políticas e sugestões que o EPD trouxer para a operação são, portanto, de responsabilidade da organização, de forma que esse profissional deve ser introduzido à equipe de trabalho de forma humanizada e que comande o devido respeito às suas funções. Os profissionais de recursos humanos ou de outros departamentos (jurídico, informático, segurança e etc.) podem e devem apoiar o EPD na promoção de uma cultura de proteção de dados[58].

Outro dever do controlador é o de implementar as ações necessárias para conformidade com a LGPD[59]. Esse dever não significa que todas as decisões terão de ser tomadas diretamente pelo controlador, podendo este contratar um operador, bastando que o primeiro "mantenha sob sua influência e controle as principais decisões, isto é, aquelas relativas aos elementos essenciais para o cumprimento das finalidades[60]. Um exemplo de elemento essencial é a escolha de quais softwares e equipamentos serão utilizados na F&A e o detalhamento de medidas de prevenção e segurança.

Por exemplo, o artigo 41 da LGPD determina que o controlador deve divulgar publicamente, de forma clara e objetiva, a identidade e as informações de contato do encarregado. Portanto, a empresa deve ter essas informações em seu *website.* Em uma F&A, esse dever de publicidade dos dados de contato do EPD pode ser traduzido em informar a equipe de trabalho da identidade do mesmo, colocando essa informação nos documentos de *onboarding* do projeto (ppt's, pdf's ou plataformas de comunicação interna) ou divulgação à interessados.

Tanto o operador quanto o controlador, enquanto agentes de tratamento de dados, têm o dever de "adotar medidas de segurança, técnicas e políticas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito"[61] (art. 46 da LGPD).

---

[58] GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – UNIÃO EUROPEIA. **Orientações sobre os encarregados da proteção de dados (EPD).** Bruxelas, 2016. Disponível em: https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf. Acesso em: 12 jul. 2023.

[59] De acordo com o art. 5º, VI, da LGPD, o controlador é o responsável por tomar as "decisões referentes ao tratamento de dados pessoais". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 jul. 2023.

[60] Item 36. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília, Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

[61] MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. 1. ed. Indaiatuba: Editora Foco, 2022. p. 20.

Também devem ser mantidos os registros das operações de tratamento de dados que realizarem dentro e fora da operação de F&A. Isso inclui, na condição de operadores, empresas de armazenamento físico ou em nuvem e software como serviço (*software as a service ou SAAS)* que sejam utilizadas na operação de M&A[62].

Torna-se indispensável contar com profissionais com competência em gestão de projetos e processos de fusões e aquisições que tenham também conhecimento em compliance e legislação de proteção de dados. Esta qualificação assegura que as transferências de dados aconteçam de maneira organizada e segura, minimizando riscos e definindo estratégias efetivas para sua mitigação.

3.1.2 Atuação do Encarregado de Proteção de Dados

A figura do encarregado foi criada pela necessidade de internalização, nas empresas, da "responsabilidade, *accountability* e diminuição da presença estatal nas atividades cotidianas de processamento, a fim de fomentar a cultura da privacidade no ambiente corporativo"[63]. O parágrafo 2º do artigo 41 da LGPD determina as atividades do encarregado, conforme o disposto:

> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A ANPD recomenda que o encarregado seja indicado por ato formal, como um contrato de trabalho ou de prestação de serviços[64].

Nem a LGPD nem a ANPD definiram a necessidade de o encarregado ser pessoa física ou jurídica, podendo o mesmo ser um funcionário interno ou um agente externo. Conforme o enunciado 680 da IX Jornada de Direito Civil, a LGPD "não exclui a possibilidade de nomeação

---

[62] MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. 1. ed. Indaiatuba: Editora Foco, 2022. p. 21-22.

[63] SOMBRA, Thiago Luís Santos. Fundamentos da regulação da privacidade e proteção de dados pessoais – pluralismo jurídico e transparência em perspectiva. São Paulo: Thomson Reuters Brasil, 2019. p. 179. Conforme citado por MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. 1. ed. Indaiatuba: Editora Foco, 2022. p. 17.

[64] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília, Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

pelo controlador de pessoa jurídica, ente despersonalizado ou de mais de uma pessoa natural para o exercício da função de encarregado pelo tratamento de dados pessoais"[65].

Dessa forma, não se excluí a possibilidade de contratação de terceiros para a atividade de EDP. A ANPD recomenda, em operações em que isso for necessário, a possibilidade de que o encarregado seja apoiado por uma equipe de proteção de dados[66].

Para uma atuação efetiva, o encarregado deve possuir *soft skills*, habilidades de negociação e empatia para negociar com outros profissionais e fazer entender a necessidade de modificar práticas comuns no processo de aquisição. Isso é o que se entende do Guia de Orientação para os Agentes de Tratamento, publicado pela ANPD, que recomenda que o EPD deve estar em posição hierárquica que lhe permita dar orientações isentas e com independência para que a organização possa alcançar conformidade com a legislação[67]. Também no guia é recomendado que o encarregado tenha conhecimentos demonstrados em proteção de dados e segurança da informação em nível que atenda às necessidades da operação da organização.

Pode se inferir, da análise da LGPD, da GDPR, dos guias da ANPD e das orientações do Grupo do artigo 29 Para Proteção de Dados, hoje conhecido como *"European Data Protection Board",* que a figura do encarregado deve possuir um posicionamento de liderança, uma vez que ele se reporta diretamente ao mais alto nível do controlador ou operador[68], atua como promotor da cultura de proteção de dados, e tem autonomia e liberdade ao exercer suas atividades. No entanto, é importante que não se confunda a figura de encarregado com a do CISO ou do diretor de privacidade, embora possa haver o acúmulo de funções quando houver qualificação, capacidade e disponibilidade destes. Já a cumulação de funções de encarregado e *compliance officer* é indesejada, uma vez que a autonomia do encarregado deve ser mais ampla,

---

[65] BRASIL. **IX Jornada de Direito Civil:** Enunciados aprovados. Brasília, 2022. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 22 ago. 2023.

[66] Item 73. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília, Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

[67] Item 75. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília, Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

[68] Art. 38 da GDPR: O responsável pelo tratamento e o subcontratante asseguram que da proteção de dados não recebe instruções relativamente ao exercício das suas funções. O encarregado não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções**. O encarregado da proteção de dados informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante**.

tendo também funções mais extremas, como o dever de reportar vazamentos de dados pessoais à ANPD[69].

Em M&A's, é preciso entender que a criação de uma cultura organizacional que valoriza a privacidade dos dados é um diferencial competitivo[70], aumentando a confiança dos clientes, parceiros e investidores, além de estar resguardando a reputação e a sustentabilidade dos negócios no longo prazo. Isso é um resultado secundário, mas altamente desejável, da nova regulamentação – o que os economistas frequentemente se referem como uma externalidade positiva[71].

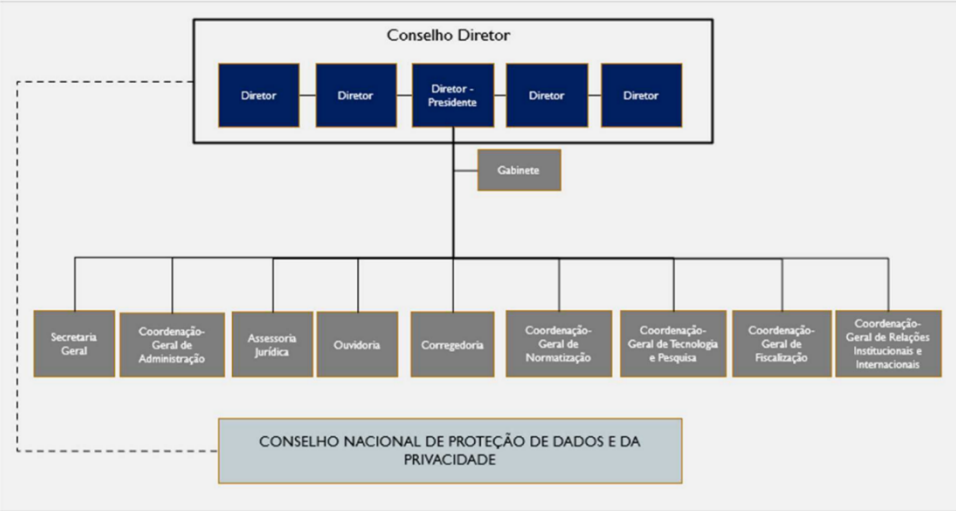
Os cuidados com a proteção de dados no ambiente corporativo antes, durante e após uma fusão ou aquisição são mais do que uma obrigação legal e moral, devendo ser encarados como um investimento necessário para evitar perdas astronômicas no valor e no sucesso da operação.

3.2 Necessidade de Fortalecimento e Reconhecimento da ANPD

Conforme o Decreto n. 10.474, de 26 de agosto de 2020, ANPD é composta por um Conselho Diretor, que é o órgão máximo da instituição e é integrado por cinco membros, com mandato de quatro anos, com possibilidade de prorrogação uma vez pelo mesmo prazo. A indicação dos membros é feita pelo Ministro de Estado Chefe da Casa Civil da Presidência da República, com aprovação pelo Senado Federal e nomeação pelo Presidente da República. Além disso, a ANPD possui uma estrutura organizacional que inclui outras áreas, como a Diretoria de Relações Internacionais e a Coordenação-Geral de Articulação Institucional.

[69] MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. 1. ed. Indaiatuba: Editora Foco, 2022. p. 22.
[70] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 72.
[71] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

Figura 3: Estrutura Organizacional da ANPD[72]



Fonte: ANPD (2022)

Dentro da ANPD, a Coordenação-Geral de Fiscalização (CGF) é responsável pela identificação de infrações à LGPD, refletindo o objetivo estratégico de fortalecer a cultura de proteção de dados pessoais. Conforme o Regimento Interno da ANPD, a CGF possui diversas competências, incluindo a promoção de ações de fiscalização sobre o tratamento de dados pessoais por agentes de tratamento, inclusive órgãos do Poder Público. Além disso, ela tem a atribuição de requisitar aos agentes de tratamento a apresentação do Relatório de Impacto à Proteção de Dados Pessoais.

A Resolução CD/ANPD nº 1, de 28/10/2021, desempenha um papel essencial na estruturação das atividades previstas no Regimento Interno da ANPD, determinando que a fiscalização tem como objetivo orientar, prevenir e reprimir infrações à LGPD. O Com essa abordagem, a ANPD busca proteger os direitos dos titulares de dados ao promover a implementação da legislação de proteção de dados pessoais.

Assim como observado com o recente Regulamento Europeu de Proteção de Dados Pessoais, o papel do órgão regulador também envolve o auxílio aos diversos atores reguladores para identificar suas obrigações e responsabilidades[73]. Nesse contexto, a ANPD desempenha um papel essencial ao desenvolver metodologias que facilitem o processo de conformidade (*compliance*) com as normas estabelecidas. Essas metodologias visam proporcionar orientações

[72] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Planejamento estratégico 2021-2023**. Brasília, 2023. Disponível em https://www.gov.br/anpd/pt-br/acesso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf. Acesso em 10 jun. 2023..

[73] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

claras e práticas para as organizações, permitindo que elas compreendam e cumpram adequadamente as exigências legais relacionadas à proteção de dados pessoais.

Veja-se que, embora o ônus de documentar e criar relatórios de impacto à proteção de dados pessoais seja da autoridade, há que se notar que até mesmo a mera análise de um relatório que trate dos impactos de uma aquisição envolvendo uma ou mais empresas de *Big Data* seria de altos custos para a ANPD[74], que atualmente, em 2023, teve um orçamento de apenas 42,3 milhões de reais, não possuindo quadro próprio de funcionários e reunindo, ao todo, cerca de 90 funcionários de diversos órgãos.

Atualmente a ANPD busca autorização para realizar concurso público para contratação de 215 profissionais próprios do órgão até 2024, o que trará um pouco mais de força para o órgão. Sem profissionais especializados e capacitados, a autoridade não consegue desempenhar suas funções de auditoria[75].

Uma das possíveis soluções para o problema de falta de orçamento da Autoridade seria a aplicação de multas, uma possibilidade com prós e contras a serem considerados. Entre as vantagens dessa abordagem está o fato de que a receita gerada pelas multas poderia ajudar a fortalecer as operações da ANPD, permitindo que ela desempenhe suas funções de fiscalização e regulação de forma mais efetiva. Além disso, a disponibilidade de recursos financeiros adicionais poderia impulsionar iniciativas educacionais e campanhas de conscientização sobre a proteção de dados, aumentando o nível de compreensão e conformidade com a Lei Geral de Proteção de Dados.

No entanto, a dependência de multas para financiar a ANPD também pode apresentar grandes riscos e desafios. Há o risco de que, ao buscar aumentar sua arrecadação por meio de multas, a ANPD possa se concentrar mais em punições do que em esforços educacionais e de conscientização. Isso poderia criar um ambiente onde o foco principal seja a aplicação de penalidades, em vez de promover uma cultura de proteção de dados de forma preventiva.

---

[74] Imaginando uma situação em que o CADE, atualmente responsável pela aprovação de operações de M&A, chamasse a ANPD para opinar acerca dessa matéria e a Autoridade visse a necessidade de solicitar um relatório.

[75] "Temos a construção de um PL, que nos coloca funções importantes para uma autarquia independente, como auditoria. Não temos auditoria no nosso quadro, não temos Ascom [Assessoria de Comunicação]. São funções importantes que eu preciso ter o chefe, o coordenador e a mão de obra necessária. Oficialmente lançamos a ideia de um concurso público, que foi bem aceita pelos órgãos competentes, como a própria Economia. Já entrou na PLOA 2023 esse acréscimo. Não é que vai resolver definitivamente os problemas da autoridade, mas vai nos aliviar bastante." GUIMARÃES, Arthur. Presidente da ANPD espera destravar concurso para contratar 215 funcionários em 2023. **JOTA**, 26 dez. 2022. Disponível em: https://www.jota.info/coberturas-especiais/protecao-de-dados/presidente-da-anpd-espera-destravar-concurso-para-contratar-215-funcionarios-em-2023-26122022. Acesso em: 5 jul. 2023.

Com a primeira sanção aplicada pela ANPD em julho de 2023 contra uma microempresa de telemarketing[76] ficou evidente que, enquanto a Autoridade se estrutura, é possível que haja maior atenção a empresas de menor porte em detrimento das entidades que lidam com maiores volumes de tratamento de dados, o que não parece ser o cenário ideal. Por outro lado, a decisão foi brilhante ao evidenciar a independência da autoridade na aplicação de sanções, reforçando a importância de todas as empresas, não importando o tamanho, cumprirem com as obrigações de proteção de dados.

É claro que a aplicação de sanções não tem apenas caráter punitivo como também educacional, mas em um cenário em que a ANPD ainda não tem capacidade estrutural para auditar transferências de grandes bancos de dados, esse tipo de estratégia poderia facilmente se tornar uma prática discriminatória, onde os mais vulneráveis são feridos, enquanto os mais poderosos (e que causam mais danos aos titulares de dados) escapam ilesos.

Dessa forma, considerando que buscar receitas por meio de punições poderia afetar negativamente a imagem e eficácia da ANPD como órgão regulador, no momento atual faz mais sentido que o orçamento seja conquistado através de alocação adequada de recursos governamentais e parcerias com órgãos, tendo-se o exemplo do Ministério da Justiça e do CADE, para atividades educacionais que visem o fortalecimento da cultura de proteção de dados no Brasil.

Nesse contexto, a ANPD poderia buscar arrecadar fundos de forma não punitiva através da oferta de selos de certificação de conformidade às empresas interessadas em demonstrar, de forma proativa, aos consumidores e titulares de dados que suas práticas estão em conformidade com a LGPD. De acordo com Luis Fernando Prado Chaves, a ideia do legislador brasileiro é que a ANPD aprove mecanismos como selos, certificados e códigos de conduta para comprovação de conformidade[77].

Os artigos 34 e 35 da LGPD dispõem algumas regulações sobre a transferência internacional de dados, as quais seriam permitidas (entre outros casos) pela comprovação de cumprimento dos princípios da LGPD por meio de “selos, certificados e códigos de conduta

[76] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Relatório de Instrução n/º 1/2023/CGF/ANPD**. Processo SEI/ANPD Processo nº 00261.000489/2022-62. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Coordenação-Geral de Fiscalização. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf. Acesso em: 25 jun. 2023.
[77] CHAVES, Luis Fernando Prado. Da transferência internacional de dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD:** Lei Geral de Proteção de Dados: comentada. 2. ed. São Paulo: Revista dos Tribunais, 2019.

regularmente emitidos"[78], que podem ser aprovados ou emitidos pela ANPD ou organismo de certificação fiscalizados por esta.

Pode parecer que a criação de uma iniciativa como essa traria mais custos do que ganhos à autoridade, mas é importante considerar que a ANPD enfrenta atualmente o desafio de possuir uma equipe limitada para conduzir auditorias de grande porte, o que pode comprometer a eficiência na fiscalização e eficácia da LGPD. Nesse sentido, uma iniciativa como a certificação por conformidade poderia justificar a contratação de uma equipe robusta de TI e auditoria, fornecendo à ANPD os recursos necessários para fortalecer suas capacidades e intensificar a supervisão de práticas de tratamento de dados em todo o país.

Inicialmente, é possível que apenas empresas que tratam dados de forma subsidiária busquem o selo, uma vez que seus processos de tratamento de dados seriam mais simples e facilmente regularizáveis. Com o amadurecimento dessa certificação e maior previsibilidade na forma de avaliação, empresas maiores estariam preparadas para submeter-se à avaliação da certificação, buscando os ganhos reputacionais que uma certificação de conformidade com a LGPD pode proporcionar. Esse sistema de certificação incentivaria as empresas a adotarem boas práticas de proteção de dados e transparência, beneficiando tanto os consumidores quanto a ANPD, que garantiria uma cultura de conformidade com a legislação de proteção de dados.

O quadro a seguir exemplifica um pouco dessa mentalidade de aplicação da LGPD por meio de fomentos e incentivos positivos.

Figura 4: Mentalidades de processos de conformidade à LGPD

[78] Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: (...)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: (...) d) selos, certificados e códigos de conduta regularmente emitidos;
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. (...) § 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento. § 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.
BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 jul. 2023.

Mentalidades de processos de conformidade à LGPD*	
Uma obrigação legal	**Uma janela de oportunidade**
Manutenção e revisão dos produtos existentes	Criação de novos produtos e revisão de modelo de negócio ou política pública
Análise estanque centrada no diagnóstico de riscos	Análise dinâmica centrada no que a organização pode gerar de valor
Gestão baseada em mitigação de risco	Gestão baseada em inovação
Reputação com base no medo de sanções	Reputação com base em dar mais transparência ao uso dos dados
- inovação - competividade - reputação	+ inovação + competividade + reputação

[79]

Fonte: Bioni (2021)

Um dos deveres da ANPD, segundo Bioni, seria o de auxiliar a formação de uma cultura de proteção de dados no Brasil[80]. Ao alinhar suas ações de governança com a missão institucional, as organizações que seguirem a LGPD demonstrarão um compromisso genuíno com a proteção dos dados de seus clientes e usuários. Em um contexto em que a privacidade e a segurança dos dados são cada vez mais valorizadas pelos consumidores, essas empresas se destacarão por oferecer uma experiência diferenciada, pautada na transparência, confiança e respeito à privacidade.

Além de fortalecerem sua reputação, essas organizações estarão melhor preparadas para enfrentar possíveis desafios regulatórios e evitar sanções decorrentes de não conformidades com a LGPD. A adoção de práticas humanizadas também contribui para a construção de relacionamentos mais sólidos com os clientes, permitindo uma maior fidelização e engajamento com a marca.

É importante que no futuro próximo a ANPD realmente possua estrutura para auditar processos de coleta e tratamento de dados com maior profundidade, pois sem isso a LGPD se torna intangível e vaga. Em matéria de fusões e aquisições, o ideal seria haver a participação da ANPD em operações de M&A que envolvam a concentração ou transferência de grandes volumes de dados pessoais, do que se trata o próximo tópico.

---

[79] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 78. Quadro elaborado em coautoria com Maria Cecilia Oliveira Gomes para o artigo de autoria dela intitulado: “Para além de uma obrigação legal: o que a metodologia de benefícios e riscos nos ensina sobre o papel dos relatórios de impacto à proteção de dados”.

[80] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 78.

A conformidade com as normas de proteção de dados não é apenas uma obrigação legal, mas também uma estratégia competitiva para manter a reputação e credibilidade no mercado. As empresas precisam compreender que infrações à LGPD podem resultar em sanções significativas, e a ANPD desempenha um papel crucial como fiscalizadora e orientadora nesse processo. À medida que a autoridade avança em processos administrativos sancionatórios, é esperado que empresas de todos os tamanhos também busquem adequação às normas de proteção de dados para garantir transparência, segurança e privacidade dos dados pessoais.

3.2.1 Cooperação entre a ANPD e Outros Órgãos

Uma das formas pelas quais a ANPD tem lidado com a falta de estrutura para fiscalizar vazamentos e infrações é pela cooperação com outros órgãos. O Presidente da ANPD, em 23 de fevereiro de 2021, durante o seminário Políticas de Telecomunicações, do portal Teletime, ressaltou que a Autoridade não tinha como, naquele momento, investigar vazamentos de dados de grande porte como os que estavam ocorrendo, mas ressaltou que:

> "Nossa relação com os demais órgãos se mostrou necessária e importante. Já estamos em reunião com Senacon, e com o Cert.br já temos um rascunho de acordo. Faremos isso com a Anatel, com a Polícia Federal. A ideia é estabelecer os limites do que cada órgão vai fazer e até mesmo auxílio entre os órgãos, usando a expertise de cada instituição. Não precisamos investir em software caríssimos de investigação se já existem quem faz[81]."

Essa abordagem faz muito sentido, na medida em que certas infrações e situações podem, por vezes, serem fiscalizadas em coordenação junto a outros órgãos, conforme os parágrafos 3º e 4º do artigo 55-j e artigo 55-k da LGPD, que trata das competências da ANPD. Embora as investigações específicas por suspeita de infração à LGPD em fusões e aquisições recaiam sobre a ANPD, está no melhor interesse do titular de dados pessoais que a Autoridade coopere com outros órgãos para cumprir seus deveres sempre que necessário e possível.

Nesta linha, o Brasil possui um órgão de suma importância no cenário das Fusões e Aquisições, bem como na proteção da livre concorrência: o CADE, conhecido como Conselho Administrativo de Defesa Econômica. O CADE é uma autarquia em regime especial com jurisdição em todo o território brasileiro e desempenha um papel importante na análise e

81 GROSSMANN, Luís Osvaldo. ANPD não tem poder de polícia para investigar vazamentos. **Convergencia Digital**, Brasília, 23 abr. 2021. Disponível em: https://www.convergenciadigital.com.br/Seguranca/ANPD-nao-tem-poder-de-policia-para-investigar-vazamentos-56185.html?UserActiveTemplate=mobile%2Csite. Acesso em: 13 de jul. 2023.

aprovação dessas transações, buscando preservar a competitividade e evitar concentrações excessivas de mercado que possam resultar em prejuízo aos consumidores[82].

No entanto, considerando que o CADE não é o órgão mais adequado para analisar a conformidade das coletas, tratamentos e transferências de dados em operações de M&A, pode surgir a necessidade de envolver a Autoridade Nacional de Proteção de Dados (ANPD). Assim, é recomendável que, quando necessário, o CADE possa consultar a ANPD para avaliar a necessidade ou não de fiscalização específica antes e/ou depois da conclusão do negócio.

Nessa direção, o CADE e a ANPD já perceberam a necessidade de atuação colaborativa e conjunta, tendo os órgãos assinado um Acordo de Cooperação Técnica em 02 de junho de 2021[83]. O acordo viabiliza ações conjuntas e coordenadas em situações em que haja interseccionalidade entre ambas as esferas de competência do CADE e ANPD.

Estando a LGPD baseada nos fundamentos da livre iniciativa, livre concorrência e defesa do consumidor[84], ela está alinhada com a missão do CADE e outros órgãos como a SENACON (Secretaria Nacional do Consumidor). A cooperação entre essas entidades é essencial para garantir a harmonização dos interesses e assegurar que as políticas de proteção de dados estejam em consonância com a defesa da concorrência e os direitos dos consumidores.

Veja-se que as F&A's são operações de concentração de mercado, e podem levar a monopólios. Por esse motivo, quando tratamos de LGPD aplicada a M&A's, não há como isolar a discussão entre leis de proteção de dados e direito concorrencial, pois surgem desafios tanto para a concorrência quanto para a proteção do titular de dados. Por exemplo, fusões entre empresas que possuem grande quantidade de dados do consumidor podem levantar preocupações relacionadas à privacidade e segurança dessas informações. Além disso, a falta de concorrência significativa pode limitar a escolha dos consumidores em relação a empresas que abusam de seu poder como agentes de coleta e tratamento de dados.

Questões de competição e proteção de dados estão se tornando cada vez mais interligadas[85]. Mudanças nas políticas de proteção do titular de dados em empresas de

---

[82] CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. **Cartilha do CADE.** [s.l.], maio 2016. Disponível em: https://cdn.cade.gov.br/Portal/acesso-a-informacao/perguntas-frequentes/cartilha-do-cade.pdf. Acesso em: 23 jul. 2023.

[83] Autoridade Nacional de Proteção de Dados. ANPD e CADE assinam Acordo de Cooperação Técnica. ANPD, [s.l.], 02 jun. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cade-assinam-acordo-de-cooperacao-tecnica. Acesso em 10 jun. 2023.

[84] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[85] "We are seeing more and more mergers and conduct matters with technology-related issues such as data collection, intellectual property, and network effects. And as consumers become data commodities themselves, the nature of competition has been evolving as well. What is most interesting to me is how concerns about competition and consumer protection no longer exist in isolation. Addressing a legal question

tecnologia podem ter implicações na concorrência, assim como questões de transferência de dados podem facilitar ou dificultar a entrada de novos competidores no mercado.

Em países como Austrália, Estados Unidos e Alemanha, a mesma instituição possui competência para tratar tanto de questões de proteção do consumidor quanto de defesa da concorrência[86]. Essa abordagem reflete uma compreensão clara da interligação entre os aspectos de proteção de dados, livre concorrência e bem-estar dos consumidores.

O caso *Bundeskartellamt* versus Facebook[87] é um exemplo de cooperação entre órgãos de concorrência e proteção de dados. Nesse caso, o Facebook foi alvo de restrições na coleta automatizada de dados, incluindo dados de aplicativos como Instagram e WhatsApp, bem como de outros sites por meio de interações dos usuários. A decisão exigiu o consentimento voluntário do usuário para essa coleta, garantindo o acesso à plataforma mesmo para aqueles que discordassem da coleta em outros aplicativos e sites.

Essa resolução decorreu de uma investigação sobre abuso de poder de mercado do Facebook pelo *Bundeskartellamt*, uma vez que a coleta automatizada prejudicava a autonomia dos usuários em relação ao uso de suas informações pessoais. A análise também levou em conta o impacto sobre os concorrentes do Facebook, considerando sua posição dominante e práticas abusivas de coleta de dados.

Assim, passou a ser requisito o consentimento voluntário do usuário para coletas realizadas em aplicativos, que deveria continuar autorizado a utilizar o Facebook normalmente caso discordasse das referidas coletas[88].

Apesar do foco da decisão do *Bundeskartellamt* ser em aspectos concorrenciais, o caso também possui relevância para a proteção de dados. A colaboração entre agências independentes fortalece as relações institucionais e garante o cumprimento das leis. Com o avanço tecnológico, as áreas jurídicas de concorrência e proteção de dados têm se aproximado,

---

on one side often has profound implications for the other. Consider a hypothetical merger between two companies that each control substantial consumer data; what are the privacy and security implications of that rollup? Consider also the consequences for consumers when limited competition means there is no meaningful choice about whether to patronize a company that may not prioritize user privacy." FEDERAL TRADE COMMISSION. **6th Bill Kovacic Antitrust Salon:** Where is Antitrust Policy Going?. Washington DC, 24 set. 2018. Disponível em: https://www.ftc.gov/system/files/documents/public_statements/1412806/slaughter__closing_remarks_for_6th_annual_bill_kovacic_antitrust_salon_9-24-18.pdf. Acesso em: 12 ago. 2023.

[86] CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. **Documento de Trabalho 002/2021**-Benchmarking internacional sobre as instituições de Defesa da Concorrência e de Proteção de Dados. Brasília, jun. 2021. Disponível em: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/documentos-de-trabalho/2021/Documento%20de%20Trabalho%20-%20Benchmarking-internacional-Defesa-da-Concorrecia-e-Proteacao-de-dados.pdf. Acesso em: 20 jun. 2023.

[87] BUNDESKARTELLAMT. **Implication of the German Facebook Decision**. Bruxelas, 17 abr. 2019. Disponível em: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Reden/L1/Andreas%20Mundt%20-%20%20Global%20Competition%20Law%20Centre.pdf?__blob=publicationFile&v=2. Acesso em: 20 jun. 2023.

[88] CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. *op. cit*. p. 36.

tornando a cooperação cada vez mais valorizada, permitindo que cada instituição contribua com sua expertise específica para abordar questões complexas relacionadas à livre concorrência e à privacidade dos dados pessoais.

Em futuros casos de fusões e aquisições em que uma empresa esteja adquirindo outra com a intenção de coletar e tratar dados da adquirida de forma anticompetitiva ou abusiva é possível antecipar colaborações entre a ANPD e o CADE para chegar a decisões semelhantes.

Esses e outros exemplos ocorridos na União Europeia têm mostrado que a proteção de dados não deve inviabilizar a atuação dos órgãos antitruste e investigados não podem usar a privacidade como justificativa para não colaborarem com as investigações em curso[89]. A premissa é de que ambas as áreas - proteção de dados e defesa da concorrência - possam coexistir e serem aplicadas de maneira complementar.

Um dos maiores desafios para a ANPD nas próximas décadas será aplicar as regras da LGPD aos grandes *players* da coleta e tratamento de dados, conhecidos como "*Big Data*" ou "*Big Techs*"[90]. Essas empresas detêm valiosos dados dos clientes, incluindo informações pessoais, histórico de compras, preferências de produtos e dados sensíveis, como informações de pagamento. A utilização desses dados permite a personalização da experiência de compra, o direcionamento de anúncios e o aprimoramento das operações e estratégias de marketing.

A concentração excessiva de dados nessas grandes empresas pode gerar consequências significativas tanto para a concorrência no mercado quanto para a privacidade dos usuários. Companhias dominantes, aproveitando seu poder de mercado, podem utilizar estratégias de aquisições predatórias para adquirir *marketplaces*[91] ou plataformas menores, visando alcançar os usuários das empresas adquiridas de forma não consensual. Esse tipo de prática anticompetitiva pode restringir a entrada de novos concorrentes, limitando a inovação e a oferta de opções para os consumidores[92].

---

[89] CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. **Documento de Trabalho 002/2021**-Benchmarking internacional sobre as instituições de Defesa da Concorrência e de Proteção de Dados. Brasília, jun. 2021. Disponível em: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/documentos-de-trabalho/2021/Documento%20de%20Trabalho%20-%20Benchmarking-internacional-Defesa-da-Concorrecia-e-Proteacao-de-dados.pdf. Acesso em: 20 jun. 2023. p.168.

[90] Esse termo se refere às poucas empresas que possuem a maioria dos dados em escala mundial, como Alphabet, Meta, Amazon, Alibaba e Tencent, entre outras.

[91] *Marketplaces* são ambientes digitais de varejo que concentram diversas marcas em um mesmo ambiente, em uma espécie de galeria digital. Além de coletar dados pessoais comuns ao varejo (como dados de cadastro do cliente ou histórico de compras), essas empresas podem adquirir dados muito mais específicos, como o tempo que o usuário passou visualizando uma categoria de produto ou a forma como ele interage com cada tipo de anúncio.

[92] CHIRITA, Anca D. Data-driven mergers under EU competition law. In: AKSELI, Orkun; LINARELLI, John (ed.). **The Future of Commercial Law:** Ways Forward for change and reform. 1. ed. Oxford: Hart Publishing, 2019. p. 147-183, 2018.

Além disso, a concentração de dados em poucas empresas aumenta significativamente o risco de violações de privacidade e mau uso das informações pessoais dos usuários. A ausência de alternativas viáveis no mercado pode restringir a escolha do consumidor, tornando mais difícil para eles exercerem o consentimento informado em relação ao tratamento de seus dados. Essa falta de controle sobre suas informações pessoais pode levar a um cenário preocupante de uso indevido, compartilhamento não autorizado e potencial exposição a violações de segurança.

Diante dessas questões, é fundamental que órgãos reguladores, como a ANPD, e autoridades de defesa da concorrência, como o CADE, atuem de forma proativa para garantir a proteção dos direitos dos titulares e consumidores e a promoção de um ambiente de negócios mais equilibrado. Uma cooperação efetiva entre essas entidades é essencial para lidar com os desafios impostos pela concentração de dados e assegurar que as práticas de coleta, tratamento e compartilhamento de informações respeitem as disposições da LGPD e os princípios do direito do consumidor. O equilíbrio entre inovação, competitividade e privacidade é fundamental para o avanço responsável da sociedade em um mundo cada vez mais conectado e orientado por dados.

4. ELEMENTOS-CHAVE PARA AQUISIÇÕES QUE RESPEITEM A LGPD

Realizar uma M&A é uma tarefa de alta complexidade que envolve inúmeros riscos para ambas as partes da transação. No momento de se planejar o modo como se realizará a F&A em questão, há que se levar em consideração diversos pontos, tanto na parte estrutural quanto na negocial, regulatória e formal como um todo. A falta de realizar ações preventivas nesse processo pode resultar em violações à LGPD e/ou outras normas, resultando em consequências negativas como multas, condenações, custos não-planejados e perda de parte da base de consumidores, entre outras.

Neste contexto, torna-se imprescindível que as empresas que estejam envolvidas em um processo de F&A tenham profissionais educados sobre o cenário jurídico brasileiro, e que estes estejam em posição para impactarem a forma como o processo será conduzido.

A ANPD já trouxe informações que deixam claras algumas das boas práticas que devem ser implementadas dentro de agentes de tratamento de dados[93], mas ainda se faz necessário explorar alguns dos principais pontos-chave para que a LGPD esteja sendo respeitada durante uma F&A.

Nesta seção, abordaremos uma série de etapas e considerações cruciais para assegurar que as transferências e tratamentos de dados realizados no processo de fusões e aquisições estejam em total alinhamento com a LGPD, garantindo, assim, a privacidade e proteção dos dados pessoais dos titulares. Na seção dois deste trabalho já se teceu considerações sobre alguns destes pontos, mas cabe explorá-los de forma mais aprofundada e jurídica.

Em primeiro lugar, discutiremos a importância de uma *due diligence* específica para a LGPD e segurança de dados, visando identificar potenciais riscos e vulnerabilidades no tratamento de dados pelas empresas envolvidas na operação. Em seguida, exploraremos a relevância da Documentação no processo de M&A, destacando a necessidade de registrar e documentar detalhadamente todas as decisões e ações relacionadas ao tratamento de dados, a fim de evitar futuros questionamentos legais.

Posteriormente, examinaremos a importância das Cláusulas Contratuais para transferência e Proteção de Dados, que desempenham um papel fundamental na definição de responsabilidades e obrigações das partes no que tange ao tratamento e transferência de dados pessoais durante e após a operação de M&A. Em seguida, abordaremos as Políticas de Privacidade e Consentimento dos Titulares de Dados pré-transferência, destacando a

[93] Alguns dos materiais lançados pela Autoridade Nacional incluem o" Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Enarregado" e o" Guia Orientativo para Aplicação da LGPD por agentes de tratamento no contexto eleitoral".

necessidade de obter o consentimento informado dos titulares de dados antes de qualquer transferência ou uso dos seus dados pessoais.

Por fim, exploraremos as etapas e procedimentos essenciais para a manifestação de consentimento do usuário pré-transferência de dados, bem como os processos de anonimização ou eliminação de dados pra quando o titular não opte por consentir com o tratamento de seus dados pelo novo agente de tratamento.

Com base nas estratégias abordadas anteriormente, esta seção tem como propósito oferecer uma visão completa e prática para orientar empresas que buscam realizar operações de fusões e aquisições alinhadas com a LGPD e outras regulamentações pertinentes.

4.1 Deveres para com a Proteção de Dados na *Due Diligence*

O *Due diligence* é um procedimento, como já explicado, em que a empresa interessada em adquirir outra realiza uma análise detalhada e minuciosa de diversos aspectos da empresa alvo, como suas finanças, infraestrutura, cultura e questões legais. No contexto da LGPD (Lei Geral de Proteção de Dados), a *due diligence* se torna ainda mais crucial, pois é necessário avaliar como a empresa alvo coleta, armazena, trata e compartilha dados pessoais.

Apesar de o *due diligence* não ser uma etapa obrigatória no processo de F&A's[94], a realização desse processo oferece ótimos benefícios à empresa adquirente[95]. Fica claro, a partir da análise de casos como os mencionados na seção 2, que os resultados obtidos nessa fase podem ter um impacto significativo na negociação do valor e nas cláusulas contratuais. Dessa forma, a condução minuciosa do *due diligence* é fundamental para uma tomada de decisão informada e para a identificação de potenciais riscos e oportunidades que possam afetar o sucesso da transação.

Durante o processo de *due diligence*, é essencial que a empresa adquirente avalie cuidadosamente a segurança e a proteção de dados da empresa a ser adquirida. Alguns aspectos cruciais a serem analisados incluem a adoção de medidas de segurança robustas, como criptografia de dados sensíveis, implementação de backups periódicos e armazenamento seguro, bem como a garantia de uma adequada remoção de dados pessoais de mídias físicas descartadas.

Para auxiliar nessa avaliação, a empresa adquirente pode utilizar materiais como o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do

[94] SAYDELLES, Rodrigo Salton Rotunno. A (in)existência de dever de realizar due diligence em operações de M&A à luz do direito brasileiro. **Res Severa Verum Gaudium**, Porto Alegre, v. 5, n. 2, p. 260-289, 2020.
[95] COUTINHO, Sérgio Mendes Botrel. **Fusões e Aquisições**. 5. ed. São Paulo: Saraiva, 2016.

Encarregado"[96], o "*Checklist* de medidas de segurança para agentes de pequeno porte"[97] ou o "Guia orientativo (de) aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral"[98], disponibilizados pela ANPD, que oferecem orientações práticas para garantir a segurança dos dados. É fundamental que a empresa adquirente estabeleça procedimentos claros e documentados para a condução do processo de *due diligence*, garantindo a identificação e o tratamento adequado de dados pessoais durante todas as etapas da avaliação.

Uma das principais recomendações para assegurar a conformidade com a LGPD durante o processo de aquisição é garantir que todos os envolvidos na due diligence estejam devidamente treinados e cientes das suas responsabilidades em relação à proteção de dados. Para isso, é essencial promover a conscientização dos funcionários por meio de treinamentos e campanhas, conforme orientado pela ANPD. Além disso, é importante informar e sensibilizar especialmente aqueles que estarão diretamente envolvidos no tratamento de dados, a fim de que compreendam as obrigações legais e adotem as medidas e precauções necessárias.

Durante o processo de aquisição, é comum ocorrer substituições do profissional responsável pelo tratamento de dados, liberação de acessos e integração entre sistemas. Por esse e outros motivos, a documentação detalhada de cada decisão relacionada ao acesso, coleta e tratamento de dados desde o início do processo é fundamental para evitar futuros questionamentos legais, conforme destacado pela ANPD

Em um levantamento conduzido pela IBM em 2019[99], descobriu-se que mais de metade das empresas não conduzem estudos de cibersegurança até após a conclusão da fase do *due diligence* em M&A's. O estudo trouxe 4 sugestões para executivos e empresas em F&A's para garantir a cibersegurança dos dados durante essas operações:

i) Inclusão de especialistas em risco cibernético e segurança cibernética como membros-chave da equipe de M&A, de preferência como parte de uma prática operacional

---

[96] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS.
Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

[97] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Checklist de medidas de segurança para agentes de pequeno porte**. Brasília, 4 out. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/checklist-vf.pdf/view>. Acesso em 10 de jul. 2023.

[98] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo:** aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes
de tratamento no contexto eleitoral. Brasília, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/guia_lgpd_final.pdf/view. Acesso em: 10 jul. 2023.

[99] MEYRICK, Julian. et al. Assessing cyber risk in M&A. **IBM**, [s.l.], 3 maio 2021.Disponível em: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/cyber-risk-mergers-acquisitions. Acesso em: 20 jul. 2023.

contínua, desde o *due diligence*, e não caso a caso. No caso brasileiro, além de especialistas de segurança digital, há a necessidade de ao menos um EPD;

ii) Ter em mente e entender como a segurança dos dados possibilita ou impede metas de negócios e objetivos da aquisição;

iii) Avaliação da resiliência de segurança cibernética da empresa a ser adquirida. Identificação de informações relevantes sobre ataques anteriores, incidentes e registros públicos para determinar possíveis riscos e responsabilidades comerciais;

iv) Avaliação dos requisitos regulamentares e de conformidade da empresa que está sendo adquirida com base nos impactos na tecnologia da organização adquirente e nos modelos operacionais de segurança e proteção de dados;

Além dessas ações, no caso brasileiro há de haver uma atenção especial à LGPD, indo além da cibersegurança para também englobar a proteção de dados e preparar a empresa para possíveis questionamentos da ANPD quando do momento da aquisição e/ou integração. Assim, para negociações que tenham essa característica de envolver transferências de dados, somam-se as seguintes sugestões:

i) Preparação de comprovantes, memorandos, atas de reuniões e quaisquer outros documentos que possam ser utilizados para compor o relatório de impacto à proteção dos dados pessoais caso solicitado pela ANPD;

ii) Avaliação e precificação de riscos de transferência internacional de dados: Caso a empresa a ser adquirida realize transferências internacionais de dados, é necessário avaliar se essas transferências estão em conformidade com as disposições da LGPD, e se existem cláusulas contratuais padrão ou outras medidas adequadas de proteção de dados em vigor para garantir a segurança das informações transferidas;

A condução diligente desse processo não apenas protege a empresa adquirente, mas também solidifica sua posição diante dos desafios inerentes à proteção de dados em um cenário de aquisição.

4.1.1 Documentação durante o processo de M&A como medida de prevenção

O dever de documentar as ações de tratamento de dados pessoais durante o processo de M&A está formalmente previsto no artigo 37 da LGPD[100], uma vez que a *due diligence* é hipótese de tratamento de dados pessoais justificado pelo legítimo interesse.

No contexto do processo de aquisição, a empresa adquirente pode elaborar, desde o estágio de pré-aquisição, um relatório de proteção de dados pessoais simplificado, semelhante ao definido no inciso XVII do art. 5º e no art. 38 da LGPD[101], contendo a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e segurança das informações, além da análise do controlador sobre as medidas e mecanismos de mitigação de risco adotados.

Importante notar que até mesmo antes do surgimento da LGPD já havia no Decreto de regulamentação do Marco Civil da Internet (Decreto Nº 8.711/2016) a obrigação de provedores de conexão e aplicações manterem certos registros das suas bases de dados, ainda que o objetivo fosse voltado à segurança da informação[102]. Visava-se, sobretudo, "a criação de uma estrutura de controle para gerenciar e auditar quem, quando e como era feito o acesso e a manipulação das bases de dados, a fim de se garantir a sua integridade"[103].

A LGPD amplia esse dever muito além da segurança da informação, obrigando os agentes de tratamento de dados a manter registros de todas as suas operações de processamento de dados pessoais.

Considerando que a definição de processamento de dados abrange tudo o que é feito com os dados, desde a coleta até o descarte, a extensão dessa obrigação de inventariar dados é

---

[100] Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[101] Art. 5º da LGPD: XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[102] Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: (...) III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; (...)

[103] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 269.

bem maior do que a que as empresas estavam costumadas a atender anteriormente. Para Bioni, ter uma "ficha corrida" dos eventos mais importantes relacionados aos dados seria o suficiente para que as partes envolvidas possam tomar decisões informadas, mitigar riscos e garantir que todas as obrigações e responsabilidades legais sejam cumpridas.

De fato, para aquisições entre empresas de pequeno porte, ter uma espécie de "livro contábil" dos fluxos e gestão de dados no processo pode ser suficiente para evitar irregularidades. O GDPR europeu estabelece, ainda, uma listagem das informações que devem constar nessa espécie de inventário de dados, resumidas por Bioni em[104]:

> a) finalidade do tratamento;
> b) descrição das categorias dos dados e dos titulares;
> c) o fluxo dos dados para fora da organização;
> d) as medidas de segurança;
> e) informações de identificação e contato do controlador;
> f) os períodos para a exclusão das diferentes categorias de dados.

No entanto, para empresas e aquisições maiores, que envolvem maior quantidade de dados e têm mais profissionais envolvidos nesse acesso, tratamento e transferência de dados, a tarefa de controlar e manter um "livro contábil" de forma manual se torna implausível. Dessa forma, uma solução é a gestão desses fluxos de dados por meio de softwares especializados em gestão de dados em F&A's[105]. Ter um software ou sistema que concentra toda a informação da operação pode ser ainda mais eficiente para fins de gestão dessas informações do que uma *data room* física.

Embora exista uma percepção inicial de que o acesso, coleta e tratamento de dados durante o processo de *due diligence* em uma aquisição seja em legítimo interesse do agente, é imprescindível que o compartilhamento de dados seja realizado de forma ética e em total conformidade com a LGPD e demais regulamentações aplicáveis.

A inclusão do legítimo interesse como hipótese de justificativa do tratamento de dados na LGPD foi um resultado de debates multissetoriais e reflexões sobre as melhores práticas internacionais em proteção de dados. Durante o processo legislativo, houve consenso sobre a necessidade de superar a hierarquia do consentimento como única base legal, reconhecendo que em certas situações, essa abordagem poderia se tornar onerosa e impraticável para os titulares

[104] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 269.

[105] Como um advento pós-pandemia, em 2023 já há vários desses softwares no mercado, normalmente oferecidos por consultorias especializadas, como o "Delloite DataMAAP" e diversos "Data Room Softwares" no mercado.

de dados[106]. Assim, a LGPD buscou equilibrar essa dinâmica ao estabelecer que o legítimo interesse deve ser baseado em finalidades legítimas, não sendo uma "carta coringa" que justificaria qualquer tratamento:

> "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
> I – apoio e promoção de atividades do controlador; e
> II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei."

Isso implica reconhecer a regularidade de situações em que os interesses legítimos do controlador podem justificar o tratamento de dados, desde que seja feito com transparência, respeitando as expectativas dos titulares e preservando seus direitos e liberdades fundamentais.

Como bem elabora Ana Frazão ao ponderar sobre empresas que lidam com decisões automatizadas sobre grandes bancos de dados: "até para demonstrar que determinada atividade não gera risco suficiente para justificar o relatório de impacto, será necessária a existência deste"[107].

Considerando-se que os processos de F&A são de alta complexidade e já têm um histórico de questionamentos e reprovações pelo CADE, a documentação de todas as ações relacionadas ao tratamento de dados desde o início da etapa pré-contratual é extremamente importante. Inclusive, isso já foi determinado pelo Enunciado 679 da IX Jornada de Direito Civil:

> ENUNCIADO 679 – O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser entendido como uma medida de prevenção e de accountability para qualquer operação de tratamento de dados considerada de alto risco, tendo sempre como parâmetro o risco aos direitos dos titulares".[108]

---

[106] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021. p. 78.

[107] FRAZÃO, Ana. **A nova Lei Geral de Proteção de Dados Pessoais:** Principais repercussões para a atividade empresarial: perspectivas a respeito da eficácia do direito à explicação e à oposição diante de decisões totalmente automatizadas. 28 out. 2019. Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2019-10-28-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_perspectivas_a_respeito_da_eficacia_do_direito_a_explicacao_e_a_oposicao_diante_de_decisoes_totalmente_automatizadas_Parte_XVII.pdf. Acesso em: 08 ago. 2023.

[108] BRASIL. **IX Jornada de Direito Civil:** Enunciados aprovados. Brasília, 2022. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 22 ago. 2023.

Um erro clássico nessa fase é adotar uma abordagem *laissez-fair*e no compartilhamento de informações, expondo dados confidenciais sem justificativa plausível. Nas palavras de Roberta Maia, pode não bastar que que haja legítimo interesse para o tratamento de dados no *due diligence*, sendo também importante que os agentes de tratamento consigam articular esse interesse e justificar suas decisões caso questionados pela ANPD:

> Deve, ainda, conforme se pode extrair da experiência prévia do Direito Europeu com o conceito, ser suficientemente articulado para que se possa permitir o adequado sopesamento com interesses do titular dos dados e, por fim, precisa representar um interesse real e atual, capaz de corresponder a benefício esperado em decorrência da atividade em virtude da qual se alega o legítimo interesse do controlador.[109]

Isso significa que as empresas envolvidas no processo devem assegurar que todas as etapas de tratamento dos dados sejam devidamente autorizadas, respeitando os princípios de finalidade, transparência, necessidade, proporcionalidade e segurança das informações. A adoção de medidas preventivas e um roteiro claro para garantir a conformidade com a LGPD durante o processo de *due diligence* são essenciais para evitar riscos e problemas legais relacionados à proteção de dados durante a aquisição.

4.2 Cuidados para Transferência e Proteção de Dados

Durante o processo de M&A, é essencial que a empresa adquirente implemente um plano de integração adequado que considere as questões de proteção de dados. Isso pode envolver revisar e ajustar as políticas e procedimentos de tratamento de dados, garantindo que eles estejam em conformidade com a LGPD. Além disso, é importante treinar os funcionários sobre as políticas de proteção de dados e conscientizá-los sobre a importância da privacidade e segurança dos dados.

Nesse cenário, a empresa adquirente também deve realizar uma análise minuciosa dos registros e práticas de tratamento de dados da empresa-alvo, identificando possíveis vulnerabilidades e riscos de não conformidade com a LGPD. Caso sejam encontradas irregularidades, é fundamental tomar medidas corretivas e estabelecer um plano de ação para garantir a adequação às exigências da LGPD.

Quando ocorre uma aquisição, é importante destacar que o consentimento previamente fornecido pelo titular dos dados à empresa adquirida pode não autorizar automaticamente a

---

[109] Maia, Roberta Mauro Medina. **O Legítimo interesse do controlador e término do tratamento de dados pessoais.** MULHOLLAND, Caitlin (Ed.). **A LGPD e o novo marco normativo no Brasil**. Arquipélago Editorial, 2020.

empresa adquirente a utilizar esses dados. Mesmo que o titular tenha dado consentimento por meio de um termo de usuário, cadastro em loja online, aceite de cookies ou qualquer outra forma de consentimento, essa autorização específica pode não se estender automaticamente à nova empresa adquirente.

A utilização dos dados requer uma análise cuidadosa da nova finalidade pretendida, adequação e do contexto da aquisição. Os princípios da finalidade e da adequação, conforme estabelecido pelo art. 6º, I e II da LGPD[110], está intrinsecamente ligado à realização do tratamento de dados com propósitos legítimos, específicos, explícitos e informados ao titular. Isso significa que os dados só podem ser coletados e utilizados para fins determinados e previamente informados ao titular, não sendo permitido o tratamento posterior dessas informações de forma incompatível com tais finalidades.

A LGPD fundamenta a restrição da transferência de dados pessoais a terceiros, e a análise do princípio da finalidade permite estruturar critérios para avaliar a razoabilidade da utilização de determinados dados para uma certa finalidade[111]. Em outras palavras, esse princípio orienta a adequação e a legalidade do tratamento de dados, garantindo que as informações sejam utilizadas apenas de maneira consentida e dentro dos limites estabelecidos.

Portanto, é fundamental que a empresa adquirente avalie a necessidade de obter um novo consentimento do titular para assegurar que o uso dos dados esteja de acordo com as bases legais e princípios estabelecidos pela LGPD. Essa abordagem proativa contribui para a proteção da privacidade e dos direitos dos titulares dos dados durante o processo de fusões e aquisições.

4.3 Políticas de Privacidade e Consentimento dos Titulares Pre-Integração

Com a chegada das *Guidelines da OCDE*[112] (que serviram como fundamentos para a LGPD) e a decisão do Tribunal Constitucional alemão que declarou a inconstitucionalidade parcial da Lei do Censo em 1980 e 1983, respectivamente, houve uma valorização do direito

---

[110] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[111] DONEDA, Danilo. **Direito fundamental à proteção de dados pessoais**, p. 45.
DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, 2011.

[112] ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. [s.l.], 10 jul. 2013. Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>. Acesso em: 20 jul. 2023.

do cidadão à autodeterminação informativa no cenário global. No Brasil, em 2020, tivemos a decisão da ADI 6387, pelo STF, que declarou a proteção de dados como um direito fundamental autônomo. Nas palavras do Ministro Luis Fux:

> a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, consectariamente, do princípio da dignidade da pessoa humana[113].

Hoje, o titular de dados está no centro da tutela de seus dados, tendo a garantia de liberdade de fornecer ou não seus dados pessoais[114]. A LGPD e a ANPD vieram com a missão de fazer com que esses direitos sejam efetivados. Nesta era digital, a proteção de dados não é uma reflexão tardia, é um necessário para os negócios. Isso faz com que seja necessário que os agentes de tratamento tomem medidas proativas para a aquisição de consentimento do usuário perante uma operação de M&A.

O consentimento representa o ato de manifestação de vontade que visa à produção de efeitos obrigacionais[115]. Há dois problemas centrais para a verificação de consentimento para o uso de dados pessoais: O problema cognitivo, no que tange à forma como o sujeito toma decisões sobre sua privacidade; e o problema estrutural, no que tange a como as decisões de consentimento são estruturadas[116]. Assim, caso a forma como o agente de tratamento obtém consentimento do titular possuir uma estrutura ou linguagem que leve à um consentimento meramente formal ou automático pelo usuário, tal aceite poderá ser desconsiderado.

Um exemplo de consentimento desconsiderável é quando o agente de tratamento tem uma política de cookies em que, pela mera utilização de um website, o usuário estaria consentindo. A mera utilização de um serviço não configura consentimento para mineração de dados pessoais do leitor de um blog, uma vez que a estrutura deste tipo de "contrato" não informa o titular sobre os dados que estão sendo coletados nem extrai um consentimento cognitivo deste.

Uma das formas como o consentimento pode fazer parte da experiência do titular de dados de forma proativa dentro de *websites*, softwares, redes sociais ou outros meios de coleta

---

[113] ADIn 6393 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO. DJe-270. DIVULG 11-11-2020. PUBLIC 12-11-2020.

[114] MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. 1. ed. Indaiatuba: Editora Foco, 2022. p. 42-43.

[115] MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**, n. 144, p. 47-53, 2019. p. 50.

[116] MATA, Camila Rosa da. JACQUES, Luísa Dresch da Silveira. BERNADINIS, Vitória do Prado. A Mudança da Finalidade do consentimento: do Consentimento aos limites ao tratamento posterior de dados no contexto de intenso fluxo informacional. In: MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. Indaiatuba: Editora Foco, 2022. p. 44.

de dados, é pela *privacy by design*, uma técnica que combina design e proteção de dados para chegar a uma experiência do cliente que realmente extraia o consentimento do usuário de produtos e serviços digitais ou físicos.

Após uma fusão ou aquisição entre duas empresas controladoras e/ou operadoras de dados pessoais, é fundamental realizar alterações e atualizações nas Políticas de Privacidade e Consentimento dos Titulares de Dados anteriormente à transferência para garantir a conformidade com a LGPD. Essas mudanças são necessárias para que a nova empresa adquirente possa utilizar os dados de forma legítima, e devem ser claramente informadas aos titulares.

Conforme o art. 5º, XII da LGPD, o consentimento é "a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[117]. Dessa forma, na fase de pós-aquisição e integração, para a transferência de dados da adquirida para a adquirente será necessário que o agente de tratamento extraia o consentimento de forma cognitiva e estrutural do titular de dados especificamente para a finalidade transferência de seus dados pessoais à adquirente.

É importante notar que há diversos tipos de M&A's, sendo possível que uma empresa A adquira participação majoritária de uma empresa B sem que haja modificação da personalidade jurídica e das finalidades de tratamento de dados pessoais da última. Nesses casos, até mesmo a atualização da política de privacidade do usuário pode ser dispensável, uma vez que tanto a finalidade quanto o agente de tratamento não terão sofrido mudança alguma.

No entanto, em fusões ou aquisições em que a personalidade jurídica da empresa estará sendo alterada, ou em que após a aquisição a empresa adquirente pretende utilizar dos dados pessoais coletados pela empresa adquirida para novas finalidades, o consentimento para a transferência de dados pós-aquisição, em observância ao que já foi dito e também a princípios como o da boa-fé, não deve ser adquirido por mera "atualização" cotidiana de política de privacidade ou de política de usuário.

Nesses casos, a fusão ou aquisição se trata de um evento, uma mudança significativa na finalidade da coleta e tratamento de dados e também do recipiente destes dados. Sem o eficaz consentimento do titular específico para transferência dos dados à nova controladora não se pode afirmar que houve respeito aos requisitos de tratamento de dados, conforme estabelece o

[117] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

artigo 16 da LGPD[118]. Como elaborado pelas autoras do capítulo "A Mudança da Finalidade do consentimento: do Consentimento aos limites ao tratamento posterior de dados no contexto de intenso fluxo informacional":

> O consentimento que autoriza a coleta e o processamento do dado para determinada finalidade não se estende a outros ambientes diferentes daquele, sendo nulo, (...) quando formulado de forma genérica ou a partir de informações enganosas, conforme determinam respectivamente os art. 8º, §4 e 9º da LGPD[119].

Também se nota que o consentimento tem eficácia *ex nunc*, podendo ser revogado a qualquer momento pelo titular. Dessa forma, o agente de tratamento tem o dever de disponibilizar meios pelos quais esse direito possa ser materializado antes da aquisição ou fusão.

Os passos e procedimentos para essa atualização podem incluir:

i) Análise da Política de Privacidade existente: O primeiro passo é revisar a Política de Privacidade da empresa adquirida e entender como os dados são coletados, utilizados, compartilhados e armazenados. Essa análise é crucial para identificar qualquer inconformidade com a LGPD e determinar as alterações necessárias;

ii) Identificação de novas finalidades, além da transferência de dados entre adquirente e adquirida: Com a fusão ou aquisição, é provável que a nova empresa adquirente tenha novos propósitos para a utilização dos dados pessoais. É fundamental identificar essas novas finalidades e informá-las de forma clara e específica aos titulares;

iii) Obtenção de novos consentimentos: Para as novas finalidades de tratamento de dados, a empresa adquirente deve obter novos consentimentos dos titulares. Esses consentimentos devem ser específicos, informados, livremente concedidos e documentados de acordo com os requisitos da LGPD;

iv) Comunicação com os titulares de dados: É importante comunicar aos titulares sobre a fusão ou aquisição e as mudanças na Política de Privacidade e Consentimento. Essa comunicação deve ser transparente, destacando as alterações relevantes e fornecendo

---

[118] Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: (...)
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei;
BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[119] MATA, Camila Rosa da. JACQUES, Luísa Dresch da Silveira. BERNADINIS, Vitória do Prado. A Mudança da Finalidade do consentimento: do Consentimento aos limites ao tratamento posterior de dados no contexto de intenso fluxo informacional. In: MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. Indaiatuba: Editora Foco, 2022. p. 53.

informações claras sobre como os titulares podem exercer seus direitos em relação aos seus dados;

v) Atualização da Política de Privacidade: Com base na análise realizada e nas novas finalidades identificadas, a Política de Privacidade deve ser atualizada para refletir as mudanças decorrentes da fusão ou aquisição. A nova Política deve estar acessível e facilmente disponível para os titulares;

vi) Oferecimento de alternativas reais ao consentimento, como procedimentos para a eliminação de dados pessoais e/ou a anonimização dos dados anteriormente à transferência;

Novamente, caso a adquirente opte pela aquisição sem a integração das atividades, sistemas e bancos de dados entre as duas, o novo consentimento do titular para transferência de dados pode ser desnecessário. No entanto, para que isso seja possível, a identidade do controlador e a finalidade de tratamento devem restar inalteradas, e não haver livre comunicabilidade de acesso e tratamento dos dados entre as duas empresas. Também, no futuro, caso a adquirente opte pela integração e transferência de dados, haverá necessidade de nova coleta de consentimento do titular com a devida clareza, sob risco de ir contra a expectativa do titular de dados, violando o princípio da boa-fé objetiva[120].

A realização desses passos e procedimentos ajudará a nova empresa adquirente a assegurar a proteção dos direitos dos titulares de dados e a promover um ambiente de negócios mais seguro e confiável, em total conformidade com a LGPD e demais legislações pertinentes. Além disso, demonstrará o compromisso da organização em respeitar a privacidade e os dados pessoais de seus usuários.

Quando se trata da formação de bancos de dados de consumidores e da utilização das informações para fins comerciais, a LGPD deve ser compreendida à luz dos princípios que norteiam a coleta e tratamento de dados, bem como dos direitos dos titulares e dos procedimentos adequados para a regular coleta e tratamento dos dados[121]. É essencial que as empresas estejam em conformidade com essa legislação para garantir a privacidade e a segurança dos dados pessoais dos usuários.

---

[120] "ENUNCIADO 683 – A legítima expectativa do titular quanto ao tratamento de seus dados pessoais se relaciona diretamente com o princípio da boa-fé objetiva e é um dos parâmetros de legalidade e juridicidade do legítimo interesse". BRASIL. **IX Jornada de Direito Civil:** Enunciados aprovados. Brasília, 2022. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 22 ago. 2023.

[121] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, São Paulo, v. 108, n. 1009, p. 173-222, nov. 2019. p. 4.

Será necessário, portanto, adicionar uma opção de eliminação de dados pessoais e sensíveis no aplicativo, website ou plataforma da empresa adquirida, o que requererá mudanças no *front* e *backend*[122] da programação da plataforma, e implementação de políticas reais de retenção de dados e a adoção de procedimentos para atender a solicitações de exclusão.

Ao atualizar minuciosamente os consentimentos e reestruturar o tratamento de dados após uma aquisição, as empresas aumentam a confiança e garantem que seus usuários se sintam seguros e respeitados em seu âmbito digital.

4.3.2 Importância do procedimento para anonimização ou eliminação de dados

A Lei Geral de Proteção de Dados (LGPD) foi concebida com base na criação de um ciclo que se inicia com a etapa de coleta e define a "vida" ou existência dos dados pessoais. Esse ciclo percorre as fases de retenção, processamento, compartilhamento e culmina no término do tratamento dos dados, onde ocorre a anonimização ou eliminação dos dados.

O artigo 15º da LGPD dispõe as hipóteses de término do tratamento de dados[123], os quais devem ser eliminados após o término de tratamento, salvo quando autorizada a conservação para as finalidades de cumprimento de obrigação legal, estudo por órgão de pesquisa, transferência a terceiro (desde que respeitados os requisitos de tratamento) ou uso exclusivo do controlador desde que anonimizados os dados e vedado seu acesso por terceiros[124].

---

[122] De forma simplificada, o *front-end* (parte frontal) é tudo que o usuário visualiza durante a utilização regular do aplicativo, website, plataforma, software e etc. Já o back-*end* é a parte que o usuário não visualiza, como os bastidores de um espetáculo, onde está a estrutura do mesmo.

[123] Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
II - fim do período de tratamento;
III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.
BRASIL. **Lei nº 13.709, de 14 de agosto de 201.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

[124] Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
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, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.
BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

Esse processo pode ser realizado manualmente ou por uma inteligência artificial treinada para eliminar elementos identificadores, mantendo-se parte dos dados para fins de legítimo interesse.

A eliminação de dados também é objeto da LGPD no inciso XIV do artigo 5º, sendo definida como a "exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado". O tema também aparece no Marco Civil da Internet no art. 7º, X, que dispõe que os usuários da internet têm direito à "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais".

Para realizar a eliminação adequada dos dados quando o titular requerer a eliminação dos mesmos, a empresa adquirente pode seguir os seguintes passos, adaptando-os às suas necessidades:

i) Identificação dos titulares não consentidores: É fundamental identificar os titulares que optaram por não conceder consentimento para o uso de seus dados pessoais. Essa identificação pode ser feita por meio de registros de consentimento, sistemas de gerenciamento de dados e demais fontes que contenham informações sobre as preferências dos titulares;

ii) Revisão dos dados coletados: Após identificar os titulares não consentidores, é importante revisar os dados pessoais anteriormente coletados pela empresa adquirida. Nessa etapa, a empresa deve garantir que todos os dados relacionados aos titulares que optaram por não consentir sejam encontrados e devidamente registrados;

iii) Eliminação dos dados: A empresa deve proceder à exclusão dos dados pessoais dos titulares não consentidores. Isso implica a remoção completa e definitiva dessas informações dos bancos de dados e sistemas de armazenamento da empresa, de forma que não seja possível recuperá-los posteriormente;

iv) Anonimização dos dados (opcional): Caso a eliminação dos dados não seja viável devido a obrigações legais ou outros motivos legítimos, a empresa pode optar por anonimizar os dados pessoais dos titulares não consentidores. A anonimização consiste em tornar os dados irreversivelmente impossíveis de serem associados a um indivíduo identificável, garantindo que não haja qualquer risco de identificação do titular;

v) Registros de conformidade: A empresa adquirente deve manter registros detalhados de todo o processo de eliminação ou anonimização dos dados pessoais dos titulares não consentidores. Esses registros servirão como prova de conformidade com a LGPD caso sejam necessários para futuras auditorias ou investigações;

vi) Comunicação aos titulares: A empresa deve informar os titulares não consentidores sobre a eliminação ou anonimização de seus dados pessoais, garantindo a transparência e a clareza na comunicação sobre o tratamento de suas informações;

vii) Revisão das políticas e processos internos: A empresa deve revisar suas políticas internas de privacidade e processos de coleta e tratamento de dados para assegurar que a eliminação ou anonimização dos dados seja realizada de forma eficaz e em conformidade com a LGPD;

viii) Notificação aos agentes de tratamento com os quais o controlador tenha compartilhado dados acerca da exclusão dos dados do titular, conforme o artigo 15 e 18, §6º da LGPD[125].

A anonimização, prevista no artigo 16, §4, é um recurso que pode ser empenhado para conservação de dados após o término do tratamento, contanto que os dados sejam utilizados apenas pelo controlador, sem acesso de terceiros.

De acordo com o princípio da transparência previsto no artigo 6º, inciso VI, caso os dados sejam conservados após o término do tratamento isso deverá ser expressamente comunicado ao titular. Embora a LGPD não especifique um prazo máximo para mantimento dos dados após o término do tratamento, o artigo 47 da LGPD (que prevê o dever de garantir a segurança da informação) aliado ao exemplo do Considerando 39 da GDPR ("a fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica") levam a entender pela existência de um tempo limite. Uma solução adotad por diversos doutrinadores seria a de aplicar o prazo previsto no Marco Civil da Internet, o qual determina a guarda de registros de acesso a aplicações de internet na provisão de aplicações, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses ou de acordo com regulamento específico[126].

Em contextos de fusões e aquisições, é crucial que as empresas tomem medidas para garantir a proteção adequada dos dados pessoais, especialmente quando o consentimento prévio não foi obtido para a continuação do tratamento desses dados. A decisão entre a anonimização e a eliminação depende da necessidade de reter certos dados para cumprir obrigações legais ou de negócios. No entanto, independentemente do caminho escolhido, a empresa deve considerar a eficácia dessas técnicas em garantir a privacidade dos titulares de dados, evitando a possibilidade de reidentificação e protegendo-os contra qualquer uso indevido ou exposição

[125] *MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. 1. ed. Indaiatuba: Editora Foco, 2022. p. 75.*

[126] O Término do Tratamento de Dados Pessoais na LGPD. In: MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. Indaiatuba: Editora Foco, 2022, p. 76.

indesejada. Ao realizar esses procedimentos de forma transparente e eficiente, a empresa demonstra seu compromisso com a proteção dos dados e a conformidade com as regulamentações de privacidade.

5. CONCLUSÕES E PERSPECTIVAS

Ao longo desse trabalho foi explorada a complexidade da aplicação da Lei Geral de Proteção de Dados (LGPD) em cenários de fusões e aquisições, considerando o contexto brasileiro. A intersecção entre a proteção de dados e as transações corporativas têm gerado desafios significativos, que vão desde a avaliação da conformidade da empresa adquirente com as exigências da LGPD até a garantia da privacidade dos titulares de dados em meio às mudanças organizacionais.

A proteção dos dados pessoais em fusões e aquisições é uma preocupação emergente, visto que a aquisição de grandes conjuntos de dados é considerada estratégica para a geração de insights valiosos. No entanto, o consentimento prévio dos titulares para a utilização desses dados não pode ser presumido, o que gera a necessidade de uma análise minuciosa sobre como lidar com esses dados antes e após transações que afetem a personalidade do agente de tratamento ou a finalidade da coleta e tratamento dos dados.

A avaliação da LGPD no contexto de fusões e aquisições revela desafios para as empresas adquirentes e também para a Autoridade Nacional de Proteção de Dados (ANPD). As empresas devem considerar a proteção de dados durante todas as fases da operação de M&A. Também é importante frisar a necessidade de atualizarem suas políticas de privacidade, obter novos consentimentos dos titulares e, em alguns casos, proceder com a anonimização ou eliminação dos dados não consentidos.

A ANPD, por sua vez, enfrenta a tarefa de garantir a conformidade dessas operações com as regulamentações da LGPD e de promover a conscientização sobre a importância da proteção de dados nesses cenários. Para isso, é necessário que a Autoridade conquiste um amior orçamento e estrutura, e que reúna uma equipe que possa proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade das pessoas naturais[127].

A abordagem para anonimização ou eliminação de dados após uma aquisição depende das obrigações legais e da necessidade de manter certas informações para cumprir as operações de negócios. A decisão entre anonimizar ou eliminar deve ser guiada pela proteção da privacidade dos titulares de dados, evitando riscos de desnonimização e uso indevido das informações.

[127] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. BRASIL**. Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 de jul. 2023.

Em última análise, o sucesso na aplicação da LGPD em fusões e aquisições requer um equilíbrio cuidadoso entre os interesses de negócios e a proteção dos direitos dos titulares de dados. A colaboração entre as empresas adquirentes, os titulares de dados, a ANPD e outras autoridades regulatórias é essencial para criar um ambiente onde as transações corporativas possam ocorrer de maneira ética, legal e transparente, ao mesmo tempo em que se respeita a privacidade dos indivíduos e os princípios da LGPD.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD e CADE assinam Acordo de Cooperação Técnica. **ANPD**, [s.l.], 02 jun. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cade-assinam-acordo-de-cooperacao-tecnica. Acesso em: 10 jun. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado.** Brasília: Abr. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 12 jul. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Planejamento estratégico 2021-2023**. Brasília, 2023. Disponível em https://www.gov.br/anpd/pt-br/acesso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf. Acesso em: 10 jun. 2023

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Relatório de Instrução n/º 1/2023/CGF/ANPD**. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf. Acesso em: 25 jun. 2023.

BAILEY, Andrew. **Re: TSB IT Migration**. 2018. Disponível em https://www.parliament.uk/globalassets/documents/commons-committees/treasury/Correspondence/2017-19/fca-to-chair-tsb-300518.pdf. Acesso em: 20 jul. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021.
BRANCO, Sérgio. As hipóteses de aplicação da LGPD e as definições legais. In: MULHOLLAND, Caitlin (Ed.). **A LGPD e o novo marco normativo no Brasil**. [s.l.]: Arquipélago Editorial, 2020.

BRASIL. **IX Jornada de Direito Civil:** Enunciados aprovados. Brasília, 2022. Disponível em: https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf. Acesso em: 22 ago. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 201.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 12 jul. 2023.

BUNDESKARTELLAMT. **Implication of the German Facebook Decision**. Bruxelas, 17 abr. 2019. Disponível em: https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Reden/L1/Andreas%20Mundt%20-%20%20Global%20Competition%20Law%20Centre.pdf?__blob=publicationFile&v=2. Acesso em: 20 jun. 2023.

CÂMARA, Paulo; BASTOS, Miguel Brito. **O direito da aquisição de empresas:** uma introdução. Aquisição de empresas. Coimbra: Almedina, 2011.
CANO, Marcelo. **O recente processo de fusões e aquisições na economia brasileira**. 2002. 16f. Dissertação (Mestrado em Economia) - Instituto de Economia, Universidade Estadual de Campinas, Campinas, 2002.

CHAVES, Luis Fernando Prado. Da transferência internacional de dados. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD:** Lei Geral de Proteção de Dados: comentada. 2. ed. São Paulo: Revista dos Tribunais, 2019.

CHIRITA, Anca D. Data-driven mergers under EU competition law. In: AKSELI, Orkun; LINARELLI, John (ed.). **The Future of Commercial Law:** Ways Forward for change and reform. 1. ed. Oxford: Hart Publishing, 2019.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. **Cartilha do CADE.** [s.l.], maio 2016. Disponível em: https://cdn.cade.gov.br/Portal/acesso-a-informacao/perguntas-frequentes/cartilha-do-cade.pdf. Acesso em: 23 jul. 2023.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA. **Documento de Trabalho 002/2021**-Benchmarking internacional sobre as instituições de Defesa da Concorrência e de Proteção de Dados. Brasília, jun. 2021. Disponível em: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/documentos-de-trabalho/2021/Documento%20de%20Trabalho%20-%20Benchmarking-internacional-Defesa-da-Concorrecia-e-Proteacao-de-dados.pdf. Acesso em: 20 jun. 2023.

COUTINHO, Sérgio Mendes Botrel. **Fusões e Aquisições**. 5. ed. São Paulo: Saraiva, 2016.

DELOITTE. **M&A Alternatives Take Center Stage: Survey**. CFO JOURNAL, [s.l.], 30 out. 2020.. Disponível em: https://deloitte.wsj.com/articles/m-a-alternatives-take-center-stage-survey-01604086979?tesla=y&tesla=y. Acesso em: 10 jul. De 2023.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico,** Joaçaba, v. 12, n. 2, p. 91-108, 2011.

DONEDA, Danilo. **Direito fundamental à proteção de dados pessoais**, p. 45.
EPSTEIN, Michael J. The determinants and evaluation of merger success. **Business Horizons**, v. 48, n. 1, p. 37–46, jan. 2005.

EUROPEAN COMMISSION. **The GDPR: new opportunities, new obligations.** Luxemburgo, 2018. Disponível em: https://ec.europa.eulcommission/sites/beta-political/files/data-protection-factsheet-sme-obligations-en.pdf. Acesso em: 13 jul. 2023.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 07/2020 on the concepts of controller and processor in the GDPR**. [s.l.], set. 2020. Disponível em <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf>. Acesso em 05 ago. 2023.

FRAZÃO, Ana. **A nova Lei Geral de Proteção de Dados Pessoais:** Principais repercussões para a atividade empresarial: perspectivas a respeito da eficácia do direito à explicação e à oposição diante de decisões totalmente automatizadas. 28 out. 2019. Disponível em: http://www.professoraanafrazao.com.br/files/publicacoes/2019-10-28-A_nova_Lei_Geral_de_Protecao_de_Dados_Pessoais_Principais_repercussoes_para_a_atividade_empresarial_perspectivas_a_respeito_da_eficacia_do_direito_a_explicacao_e_a_oposicao_diante_de_decisoes_totalmente_automatizadas_Parte_XVII.pdf. Acesso em: 08 ago. 2023

GROSSMANN, Luís Osvaldo. ANPD não tem poder de polícia para investigar vazamentos. Convergencia Digital, Brasília, 23 abr. 2021. Disponível em: https://www.convergenciadigital.com.br/Seguranca/ANPD-nao-tem-poder-de-policia-para-investigar-vazamentos-56185.html?UserActiveTemplate=mobile%2Csite. Acesso em: 13 jul. 2023.

GRUPO DO ARTIGO 29.º PARA A PROTEÇÃO DE DADOS – UNIÃO EUROPEIA. **Orientações sobre os encarregados da proteção de dados (EPD).** Bruxelas, 2016. Disponível em: https://www.cnpd.pt/media/meplvdie/wp243rev01_pt.pdf. Acesso em: 12 jul. 2023.

GUIMARÃES, Arthur. Presidente da ANPD espera destravar concurso para contratar 215 funcionários em 2023. **JOTA**, 26 dez. 2022. Disponível em: https://www.jota.info/coberturas-especiais/protecao-de-dados/presidente-da-anpd-espera-destravar-concurso-para-contratar-215-funcionarios-em-2023-26122022. Acesso em: 5 jul. 2023.

HENRICO DOLFING. Case Study 2: The Epic Meltdown of TSB Bank. **Henrico dolfing**, 13 mar. 2019. Disponível em <https://www.henricodolfing.com/2019/03/case-study-epic-meltdown-of-tsb-bank.html>. Acesso em 20 de jul. de 2023.
Julian. et al. Assessing cyber risk in M&A. **IBM**, [s.l.], 3 maio 2021.Disponível em: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/cyber-risk-mergers-acquisitions. Acesso em: 20 jul. 2023.

KIRK, Jeremy. "Yahoo Takes $350 Million Hit in Verizon Deal." **Bank Info Security,** 22 fev. 2017. Disponível em: https://www.bankinfosecurity.com/yahoo-takes-350-million-hit-in-verizon-deal-a-9736. Acesso em: 20 jun. 2023.

LEINER, Barry M. *et al.* A brief history of the Internet. **ACM SIGCOMM Computer Communication Review**, v. 39, n. 5, p. 22-31, 2009.
Maia, Roberta Mauro Medina. O Legítimo interesse do controlador e término do tratamento de dados pessoais. MULHOLLAND, Caitlin (Ed.). **A LGPD e o novo marco normativo no Brasil**. Arquipélago Editorial, 2020.

MATA, Camila Rosa da. JACQUES, Luísa Dresch da Silveira. BERNADINIS, Vitória do Prado. A Mudança da Finalidade do consentimento: do Consentimento aos limites ao tratamento posterior de dados no contexto de intenso fluxo informacional. In: MENKE, Fabiano (Org.). **Lei Geral de Proteção de Dados:** subsídios teóricos à aplicação prática. Indaiatuba: Editora Foco, 2022.

MENKE, Fabiano (Org.). Lei Geral de Proteção de Dados: subsídios teóricos à aplicação prática. 1. ed. Indaiatuba: Editora Foco, 2022. p. 11-37

MEYRICK, Julian. et al. Assessing cyber risk in M&A. **IBM**, [s.l.], 3 maio 2021.Disponível em: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/cyber-risk-mergers-acquisitions. Acesso em: 20 jul. 2023.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, São Paulo, v. 108, n. 1009, p. 173-222, nov. 2019.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**, n. 144, p. 47-53, 2019.

OLIVEIRA, Gustavo Justino de; SCHIEFLER, Gustavo Henrique Carvalho. **Compliance em Operações de Fusão e Aquisição (M&A):** intercorrências e inferências a partir dos acordos de leniência no Brasil. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4282044/mod_resource/content/0/COMPLIANCE%20EM%20OPERA%C3%87%C3%95ES%20DE%20FUS%C3%83O%20E%20AQUISI%C3%87%C3%83O%20%28pdf%29.pdf. Acesso em: 05 jun. 2023.

OLIVEIRA, Gustavo Justino de; SCHIEFLER, Gustavo Henrique Carvalho. **Compliance em Operações de Fusão e Aquisição (M&A):** intercorrências e inferências a partir dos acordos de leniência no Brasil. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4282044/mod_resource/content/0/compliance%20em%20opera%c3%87%c3%95es%20de%20fus%c3%83o%20e%20aquisi%c3%87%c3%83o%20%28pdf%29.pdf. Acesso em 05 de jun. 2023.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICOS. **Diretrizes da OCDE para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais.** [s.l.], 2002. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 02 jul. 2023.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. [s.l.], 10 jul. 2013. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188. Acesso em: 20 jul. 2023.

PESSOA, Daniel Tardelli; SABADIN, Mariana Guerra. Cláusulas de declarações e garantias e operações de fusão e aquisição. Levy & Salomão Advogados, Boletim – Julho 2012. Disponível em: http://www.levysalomao.com.br/files/publicacao/anexo/20120730185424_bj-julho-clausulas-de-declaracoese-garantias-e-operacoes-de-fusao-e-aquisicao.pdf. Acesso em 10 maio 2023.

PWC. Operações de M&A no Brasil: Transações anunciadas até maio de 2023 por setores da economia. **PWC**, 2023. Disponível em https://www.pwc.com.br/pt/estudos/servicos/assessoria-tributaria-societaria/fusoes-aquisicoes/2023/operacoes-de-mea-no-brasil-maio-2023.html. Acesso em: 18 de jul. 2023.

SAYDELLES, Rodrigo Salton Rotunno. A (in)existência de dever de realizar due diligence em operações de M&A à luz do direito brasileiro. **Res Severa Verum Gaudium**, Porto Alegre, v. 5, n. 2, p. 260-289, 2020.

SILVA, Eduardo Sá. **Fusões e Aquisições:** Abordagem Contabilística, Financeira e Fiscal. Porto: Vida Económica - Editorial AS, 2015.

SOMBRA, Thiago Luís Santos. Fundamentos da regulação da privacidade e proteção de dados pessoais – pluralismo jurídico e transparência em perspectiva. São Paulo: **Thomson Reuters Brasil**, 2019. p. 179.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 Do Parlamento Europeu E Do Conselho de 27 de Abril de 2016**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02016R0679-20160504. Acesso em: 18 jul. 2023;