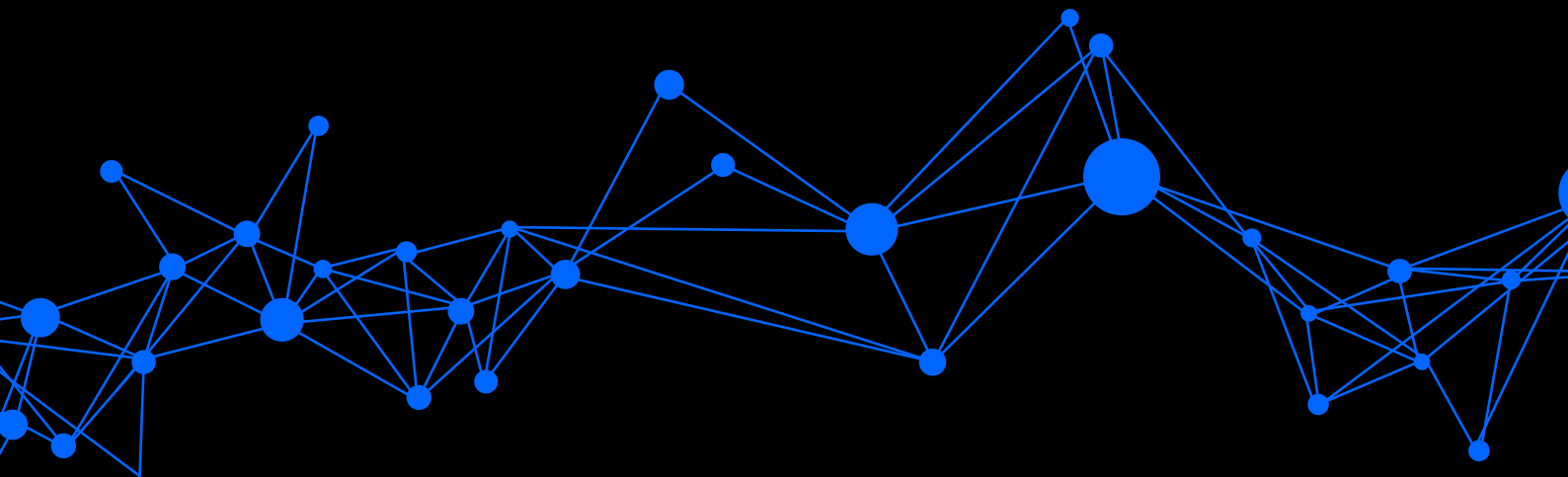


LOGO

MBSA

DUE DILIGENCE | 2026





# INTRO

A intersecção entre o Direito Societário e a Proteção de Dados Pessoais transcendeu a mera burocracia para tornar-se um pilar estratégico na estruturação de operações de Fusões e Aquisições (M&A).

No cenário atual, a validação de premissas de negócio e a própria formação do preço (valuation) dependem de processos de due diligence que envolvam o compartilhamento massivo de informações.

Entretanto, a entrada em vigor da LGPD impõe que esta circulação de ativos informacionais seja pautada por uma conformidade técnica rigorosa, sob pena de inviabilizar a transação ou gerar passivos ocultos de magnitude imprevista.



Este texto informativo tem por objeto analisar o regime jurídico aplicável ao compartilhamento de dados pessoais entre controladores — especificamente o vendedor/sociedade alvo e o potencial comprador.

É imperativo desafiar a premissa de que o **consentimento** seria a base legal absoluta em transações que exigem estrito sigilo.

Importante frisar que, desde logo, a desqualificação técnica dos agentes de tratamento e a escolha equivocada da base legal podem atrair uma responsabilidade solidária indesejada, elevando drasticamente o risco financeiro do adquirente antes mesmo do fechamento (closing).

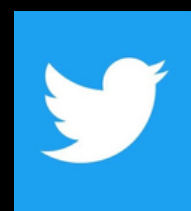
A segurança jurídica da operação não é apenas um objetivo; é o único mecanismo capaz de garantir que a liberdade de se informar do comprador não se transforme em um ônus indenizatório intransponível.



# ANÁLISE CRÍTICA DE PRECEDENTES DE MERCADO

Casos paradigmáticos, tanto no âmbito nacional quanto internacional, servem de advertência sobre os riscos de privacidade que podem corroer o valor de um ativo.

# CASO TWITTER/MUSK



À época da tentativa de aquisição da Twitter, Inc. por Elon Musk expôs as entranhas da "firehose" de dados.

É vital notar que a própria Twitter, Inc. reconheceu ter fornecido um volume de informações que ultrapassava o estritamente necessário para consumir o negócio.

Tal excesso configura violação direta ao princípio da Necessidade (Art. 6º, III, LGPD).

O acesso irrestrito a dados granulares e sensíveis, caso a operação fosse frustrada, criaria um passivo de privacidade imenso, demonstrando que o compartilhamento indiscriminado é um vetor de litígio e risco reputacional.



# CASO PETZ/ZEE.DOG

Na aquisição da Zee.Dog pela Petz, a política de privacidade da sociedade alvo previa que o compartilhamento com terceiros exigiria consentimento expresso.

Contudo, a análise técnica revelou um detalhe crucial: a PwC atuou como operadora no processo.

Este caso ilustra que a segregação de funções em contrato é a única salvaguarda eficaz para evitar que consultorias e assessores arrastem o cliente para uma responsabilidade solidária por falhas no processamento de dados.

A comunicação prévia a milhares de clientes em transações sigilosas é operacionalmente inviável, reforçando a necessidade de enquadramentos legais que não dependam da manifestação volitiva do titular.



A lição extraída é clara: o compartilhamento impróprio não é apenas um erro de conformidade, mas um fator de depreciação do ativo.

Lacunas de privacidade detectadas na auditoria devem ser tratadas como redutores de preço ou gatilhos para cláusulas de indenização específicas.





# DESAFIANDO A TESE DO CONSENTIMENTO

## BASES LEGAIS NO M&A



Deve-se desconstruir a ideia de que o tratamento de dados em M&A gravita em torno do consentimento (Art. 7º, I).

Em operações massivas, o consentimento apresenta uma inviabilidade operacional de rastreamento de revogação que compromete a estabilidade do negócio.



# BASES LEGAIS ESTRATÉGICAS

1. **Legítimo Interesse (Art. 7º, IX):** Esta é a base precípua para a due diligence. Fundamenta-se no apoio e promoção das atividades do controlador (venda do ativo) e na necessidade do comprador em validar seu investimento.

2. **Execução de Contrato e Procedimentos Preliminares (Art. 7º, V):** Aplicável quando o compartilhamento é intrínseco à continuidade dos serviços ou à sucessão empresarial, onde o adquirente assume a posição contratual frente aos titulares.

3. **Exercício Regular de Direitos (Art. 7º, VI):** Justifica a manutenção de dados para salvaguardar as partes em futuras disputas contratuais ou arbitrais decorrentes da própria transação.



# DADOS SENSÍVEIS

**Dados Sensíveis (Art. 11):** Adverte-se que o Legítimo Interesse não se aplica ao tratamento de dados sensíveis (saúde, biometria, etc.), recorrentes em auditorias de empresas como Mater Dei (saúde) ou Alper (seguros).

Nestes casos, o enquadramento deve ocorrer obrigatoriamente no "Exercício Regular de Direitos" ou na "Prevenção à Fraude", exigindo medidas de segurança e governança ainda mais robustas.

# MATRIZ DE RISCO OPERACIONAL



CRITÉRIO

CONSENTIMENTO

LEGÍTIMO INTERESSE

SIGILO

Inexistente (exige notificação)

Elevado (dispensa comunicação imediata)

ESTABILIDADE

Precária (revogabilidade *ad nutum*)

Sólida (fundada na finalidade do negócio)

GESTÃO

Inviável em bases massivas

Gerida via Relatório de Impacto (RIPD)



# LIMITAÇÕES DA DUE DÍLIGENCE E ESTRATÉGIAS DE MITIGAÇÃO

O compartilhamento de dados encontra limites intransponíveis nos princípios da Finalidade, Necessidade e Adequação.

Com base na Boa-fé Objetiva (Art. 113, CC), o vendedor que omite riscos de privacidade ou o comprador que abusa do acesso à informação agem à margem da lei.



Propõem-se as seguintes técnicas de mitigação:

- **Anonimização:** Deve ser a regra para dados de clientes e empregados que não ocupem cargos-chave. O comprador não necessita da identidade do consumidor para auditar o *churn rate* ou o faturamento.
- **Clean Teams:** Esta prática, embora consolidada no antitruste (CADE), é a única salvaguarda eficaz para o tratamento de dados sensíveis ou competitivamente sensíveis. Ao utilizar comitês independentes que entregam apenas relatórios agregados aos tomadores de decisão, as partes cumprem o dever de se informar sem violar a privacidade individual ou o segredo de negócio.



# QUALIFICAÇÃO DOS AGENTES E REGIME DE RESPONSABILIDADE

A correta alocação dos papéis de Controlador e Operador não é uma escolha estética, mas uma definição de risco financeiro.

Apoiamos a tese da Controladoria Conjunta (*Joint Controllershhip*) entre comprador e vendedor durante a *due diligence*. No ambiente do *Virtual Data Room* (VDR), o comprador não é um mero convidado; ele decide a finalidade (validação do preço) e os meios (quais dados analisar) do tratamento.

Ao assumir essa posição, o adquirente atrai para si a incidência do [Art. 42, §1º, II, da LGPD](#). Isso significa que o comprador responde solidariamente por qualquer vazamento ou incidente no VDR, independentemente de o negócio ser concluído ou frustrado. A liberdade de se informar traz consigo o ônus da responsabilidade objetiva sobre a segurança daquela base de dados compartilhada.



# CICLO DE VIDA DO DADO

## RETENÇÃO E ELIMINAÇÃO (O FATOR STJ)

O término do tratamento deve observar os limites da segurança jurídica pós-fechamento (Arts. 15 e 16, LGPD).

- **Operação Concretizada:** A retenção de documentos da auditoria é legítima para fins de defesa em disputas contratuais. O prazo é o decenal (10 anos), conforme fixado pelo STJ no EREsp 1.281.594/SP, referente à prescrição contratual.
- **Operação Frustrada:** Recomenda-se a eliminação imediata, salvo para fins de defesa contra alegações de *culpa in contrahendo* (responsabilidade pré-contratual). Para tanto, deve-se manter uma "cópia de arquivo" (*cold storage*) estritamente limitada ao prazo de 3 anos (reparação civil). O NDA deve prever expressamente este protocolo de destruição ou devolução.



# CONCLUSÕES E RECOMENDAÇÕES DE BOAS PRÁTICAS

A adequação à LGPD em processos de M&A deve ser interpretada como um mecanismo de eficiência e transparência, e não como um entrave. A negligência neste campo resulta em destruição de valor.



# RECOMENDAÇÕES IMPERATIVAS

1. **Auditoria de Conformidade como Redutor de Preço:** Lacunas graves de LGPD na *target* devem ensejar a redução direta do *valuation* ou a retenção de valores em *Escrow Account* para cobrir eventuais multas da ANPD.

2. **Privacy by Design no VDR:** Implementar níveis de acesso granulares, liberando dados identificáveis apenas na fase de *signing*, e somente se estritamente necessário.

3. **Cláusulas de Indemnity:** Incluir declarações e garantias específicas (R&Ws) sobre a inexistência de incidentes prévios e a conformidade total da base de dados.

4. **NDA e Acordos de Transferência:** Explicitar contratualmente quem é o controlador e quem é o operador em cada fase da operação, delimitando a responsabilidade de cada agente.

Em conclusão, o mercado brasileiro de M&A exige uma abordagem proativa: a conformidade com a LGPD é hoje o *caveat emptor* da era digital. Aqueles que ignoram o regime de responsabilidade solidária em auditorias estão, na prática, assumindo um passivo sem o devido desconto no preço.



# ESTRATÉGIA JURÍDICA



[rm@mastropasqua.com.br](mailto:rm@mastropasqua.com.br)  
[www.mastropasqua.com.br](http://www.mastropasqua.com.br)

